bsia
british security industry association

GDPR ready?

Procuring compliant data destruction services

Form No 336
Issue 2
August 2018

Contents

What is data destruction?

Secure data destruction is the process of destroying confidential materials to the point that the data cannot be reconstituted. These materials can take many forms, including paper documents, computer hard-drives, branded products and uniforms, but crucially, they all hold the potential to cause problems for your business, your employees or your customers if they fall into the wrong hands.

Information Destruction companies provide a range of services to help businesses of all sizes to protect themselves from the risks associated with data loss or theft. Shredding of materials can take place at your business premises using a mobile shredding vehicle, or materials can be collected and shredded at a high-security shredding facility.

Whether confidential materials are shredded on-site or at a high-security shredding facility, businesses that outsource their shredding to a professional service provider, (such as a BSIA member company), can be assured that the data will be completely destroyed.

Additionally, the services provided by an information destruction company extend far beyond the actual destruction of confidential material. These services can also include secure document storage, data security advice and guidance, office clearance and recycling.

What are my data security obligations?

Every business will collect and generate confidential information relating to its operations, its employees or its customers. When this information is no longer required, there can be severe consequences for the data subjects if the information is not correctly disposed of and subsequently falls into the wrong hands.

Therefore, any business that collects, holds, processes or disposes of a person's personal information has a responsibility to ensure that it is protected from loss or theft.

The data protection rules have changed as of 25th May 2018, when the **General Data Protection Regulation (GDPR)** came into effect and is supported by the new Data Protection Act 2018 which was introduced on **23rd May 2018** and replaces the previous Data Protection Act 1998. The GDPR has potentially significant impacts on the ways in which UK businesses collect and process the personal data of individuals.

25th May 2018, the General Data Protection Regulation (GDPR) came into effect in the UK

What has changed?

- ✔ GDPR allows the Information Commissioner's Office (ICO), and other European data protection authorities, to impose substantially bigger fines for non-compliance. There is a two-tier system, with fines from £8m (2% of global annual turnover), to fines of up to £16m (4% of global annual turnover) depending upon the severity of the data breach.
- ✔ GDPR has heightened security requirements for businesses that control the data and their data processors. Businesses are now required to notify the relevant national data protection authority (for UK-based businesses this is the ICO) and the affected individuals of data breaches within 72 hours of being made aware of the breach, unless it is unlikely to result in risk to the rights and freedoms of individuals.
- ✔ Individuals are given the opportunity to make an informed decision on the use of their data through more robust consent requirements. Consent must be given unambiguously with affirmative action, i.e. it is no longer possible to use data through "presumed consent". The GDPR introduces a default consent age threshold for minors in relation to online and other information society services set at 16, below which parental consent is required. EU member states are given the ability to lower that threshold from 16 to 13.
- ✔ Individuals now gain more extensive rights under GDPR such as erasure, objection, portability and access.
- ✔ Under GDPR is no longer possible to transfer data to non-EU countries that are not officially recognised as "adequate" by the EU. For non-EU countries to be considered "adequate" they now have stricter conditions applying to them. New mechanisms, such as privacy seals, will be considered and binding corporate rules endorsed.
- ✔ The previous requirements to notify the ICO of data processing activities have been largely replaced with new requirements to maintain internal documentation on a business's processing activities and controls, both to record what processing they do and how they achieve compliance. In certain cases, businesses will need to conduct privacy impact assessments of their data processing activities.
- ✔ Businesses that process large quantities of sensitive personal data or that process personal data and engage in systematic monitoring on a large scale will have to appoint a 'Data Protection Officer'.
- ✔ Member states will have the ability to enhance specific rules around employee data processing.

How should I comply with GDPR?

The ICO have published the following 12 steps to help businesses of all sizes to prepare

AWARENESS
Ensure decision makers and key people are aware that the law is changing. It is important to understand the impact that this will have and begin to identify areas that could cause compliance issues.

INFORMATION YOU HOLD
Begin to document what personal data you currently hold, where it came from and who you share it with. It may be necessary to organise an information audit across the organisation.

COMMUNICATING PRIVACY INFORMATION
Review your current privacy notices and put a plan in place for making the necessary changes.

INDIVIDUALS' RIGHTS
Check existing procedures to ensure they cover individuals' rights, including how you delete personal data or provide data electronically.

SUBJECT ACCESS REQUESTS
Update your procedures and plan how you will handle requests within the new timescales and provide additional information. The rules for dealing with subject access requests will change.

LEGAL BASIS FOR PROCESSING PERSONAL DATA
Review the current types of data processing you carry out, identify the legal basis for carrying it out and document it.

CONSENT
Review how you seek, obtain and record consent and whether you need to make changes.

CHILDREN
Think about putting systems in place now to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

DATA BREACHES
Ensure you have the right procedures in place to detect, report and investigate a personal data breach. The GDPR will bring in a breach notification duty across the board.

DATA PROTECTION BY DESIGN & DATA PROTECTION IMPACT ASSESSMENTS (PIAs)
Familiarise yourself with the PIAs, and look at how to implement them in your organisation. These processes help businesses and organisations anticipate and address likely privacy impacts of projects and actions that involve exchanging personal information.

DATA PROTECTION OFFICERS
Designate a Data Protection Officer now, if required, and assess where the role will sit within your organisation's structure and governance arrangements.

INTERNATIONAL
If you operate internationally you should determine now which data protection supervisory authority you fall under. The GDPR contains complex arrangements for working out which data protection supervisory authority takes the lead when investigating a complaint with an international aspect.

Getting your house in order

The ICO has also designed a self-assessment tool to help you get your house in order, ready for the new data protection reform. It includes getting to grips with the new rights of individuals, handling subject access requests, consent, data breaches, and designating a data protection officer.
Take the test here: https://ico.org.uk/for-organisations/register/self-assessment

What are the risks to my business?

A data breach can pose some significant risks to your business or organisation. These can include reputational damage leading to lost business, financial penalties being issued by the ICO, or even prosecution of those who commit criminal offences under the Act.

Under GDPR regulations, the ICO can fine a business or organisation up to £16.7m or 4% of global annual turnover. These are far greater penalties than under the former 1998 Data Protection Act and these have been introduced to protect the EU including UK citizens' personal data by encouraging compliance.

Not only can the ICO issue these increased fines but, for the first time, individuals have the right to claim compensation for material and non-material harm.

A national estate agent found itself in breach of the data protection act for continuing to leave papers containing personal information on the street. The papers were stored in transparent bags and contained copies of passports and tax credit awards which could have been used for the purposes of identity fraud. Despite a previous warning the company were subject to actions taken by the ICO.

A key principle of GDPR stipulates that a business must take appropriate measures against accidental loss, destruction or damage to personal data and against unlawful processing of the data.

But it's not just the penalties issued by the ICO that can cause significant damage to your business. Data breaches can also cause a huge amount of damage to business reputation. Customers are becoming increasingly aware and concerned about how businesses collect and use their personal information. Businesses run the risk of losing customer confidence in the brand where they feel that their privacy is not being protected or respected. Of course, a loss in customer confidence can ultimately lead to lost business.

The risk for business does not stop here. As important will be the loss of company reputation which potentially will lead to lower orders, reduction in profit and for international companies damage to global brand awareness.

"Under GDPR regulations, the ICO can fine a business or organisation up to £16.7m or 4% of global annual turnover."

How can I mitigate the risks?

GDPR regulations cover all personal data on all EU individual persons saved on all data systems, paper or digital, including cloud computing platforms.

All Data Controllers and Data Processors are responsible for ensuring they are handling data on a lawful basis.

The collection and processing of personal data is lawful if at least one of the legal bases below are met:

- Consent
- Legitimate Interest
- Contractual Necessity
- Legal Obligations
- Vital Interests.

Follow the data protection principles

GDPR sets out strict rules governing the use of personal information by organisations, businesses or the government. Following these six rules – or 'data protection principles' – will help to ensure that you comply with the GDPR

The principles call for:

- Lawfulness, fairness and transparency
- Retention for legal purpose
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

"One of the most vulnerable periods of the data processing cycle is the point at which data is no longer required and needs to be disposed of. If data is not adequately disposed of at the end of its life cycle, it can fall into the wrong hands and be unlawfully processed."

In addition, GDPR is much more specific than the former 1998 Data Protection Act in requiring auditable technical and organisational measures.
In the event of a data breach, these measures will need to be demonstrated.

These should include:

- Identifying all personal data held and on what grounds.
- Restricting and controlling access to personal data.
- Keeping data policies updated which should include privacy, information security and data retention.
- Having a detailed service agreement with the data processor i.e. the information destruction/shredding service provider.

The fifth principle of GDPR relating to storage limitation stipulates that appropriate measures must be taken against accidental loss, destruction or damage to personal data and against unlawful processing of the data.

One of the most vulnerable periods of the data processing cycle is the point at which data is no longer required and needs to be disposed of. If data is not adequately disposed of at the end of its life cycle, it can fall into the wrong hands and be unlawfully processed.

Outsourcing the destruction of confidential materials to a professional information destruction service provider has a number of benefits, not least the assurance that your information is being destroyed securely. Selecting a BSIA Information Destruction member will ensure guarantees in terms of expert knowledge and ability to deliver a secure and competent service, including appropriate technical and organisational measures.

Shredding confidential material in-house is a costly exercise. Whilst office shredders are one option, a shredder capable of processing large volumes of material is still a sizeable investment. Then of course there is the cost of electricity, maintenance and having someone employed to operate it. There are also the practical implications such as the office space taken up by the shredder and the subsequent disposal of the shredded material.

Probably most importantly, when shredding in-house, the responsibility remains in-house. This means that it is up to the business to ensure that confidential material is stored securely prior to destruction, is destroyed in a timely manner and to a degree that it can't be reconstituted. For materials other than paper, i.e. DVDs or hard drives, this can involve different levels of destruction needing a variety of destruction equipment. To ensure customer compliance with GDPR audit requirements it is recommended that a destruction certificate is obtained as an approved control document to demonstrate compliance.

Therefore, it is usually impractical and time consuming to rely on in-house shredding, particularly when large amounts of data are being generated. An outsourced professional service provider will always advise and agree the destruction level required to ensure you are complying with your obligations.

Most professional service providers will be able to destroy your data at your premises using a mobile shredder, or can collect it from your premises and destroy it at a high-security shredding facility, both of which are equally secure.

They are able to destroy large volumes of material with powerful shredding machines that utilise cross-cut shredding technology. In addition, the shredded material is then mixed with tonnes of other particles from other sources, which means that confidential data is irretrievable following destruction.

Once material has been destroyed, a professional service provider will issue you with a certificate of destruction which enables you to prove that you have disposed of confidential material responsibly.

A professional data destruction service provider will also be able to securely destroy all manner of materials that could pose a threat to your business if they fell into the wrong hands. This could include electronic storage devices such as hard-drives, DVDs, uniforms, identification badges or access passes. Securely destroying these types of materials in-house would be very difficult, time-consuming and expensive.

Assess your compliance

The ICO has a range of resources available to help you assess how well prepared you are to comply with GDPR, and to help you identify areas that you can improve in.

These include a range of self-assessment tools aimed at particular elements of GDPR, including data protection assurance, information security and records management.

Visit www.ico.org.uk/for-organisations for more information.

What should I should be looking for in a data destruction service provider?

When outsourcing your data destruction to an external service provider, there are a number of key considerations to look out for to ensure that you are receiving the best possible service. Any provider you choose must be able to demonstrate that they are certified to BS EN 15713 – the European standard for data destruction. This standard sets out the measures that information destruction service providers should take to maintain the security of confidential data, and provides recommendations relating to the management and control of collection, transportation and destruction of confidential material to ensure such material is disposed of safely and securely.

The standard has the following requirements which a BSIA approved Information Destruction member will be able to assure you that they comply with:

1. Confidential destruction premises

All premises carrying out information destruction should:

- Have an administration office where necessary records and documentation is kept for conducting business.
- Be separated from other business or activities on the same site.
- Have an intruder alarm, installed to PD 6662 / EN 50131-1, monitored by an Alarm Receiving Centre.
- Have a CCTV system with recording facilities that monitors the unloading, storage and processing areas. The images should be retained for a minimum of 31 days unless otherwise agreed with the client.

2. Contracts and documentation

The following legal agreements regarding responsibility should be in place:

- A written contract covering all transactions should exist between the client and the organisation.
- Sub-contracted work should only be allocated to companies complying with BS EN 15713, incorporated within UKAS approved ISO 9001 or ISO 27001 Quality Management System.
- In every case, clients should be informed if sub-contractors are used.
- The client, as data controller, should:
  - Choose a data processor providing guarantees in respect of technical and organisational security measures.
  - Take reasonable steps to ensure compliance with these measures.
- A Waste Transfer Note should be issued when the material is collected from your site.
- A Certificate of Destruction should be issued to you following destruction of the data, confidential information or product.

3. Personnel

All personnel involved in the destruction of confidential data should:

- Be security vetted in accordance with BS7858, which includes a Disclosure and Barring Service (DBS) check.
- Have signed a deed of confidentiality prior to commencement of employment.

4. Collection and retention of confidential material

Information destruction companies should employ the following measures when collecting confidential material:

- Confidential material to be collected should remain protected from unauthorised access from the point of collection to complete destruction.
- Collection should be made by uniformed and suitably trained staff carrying photographic identification.
- The destruction of confidential material should take place within one working day from arrival at the destruction centre, where shredding is taking place at the destruction company's premises.

5. Vehicles (off site shredding and destruction services)

Vehicles collecting confidential data for destruction off site should:

- Be either box bodied or have a demountable container.
- Where a curtain side vehicle is used, material should be transported within a suitable secure container.
- Be able to communicate with home base by radio or telephone.
- Be fitted with electro-mechanical immobiliser or alarm system.
- Be closed and locked / or sealed during transit.
- Be immobilised or alarmed when left unattended.
- Use Satellite tracked vehicles

6. Vehicles (on site shredding and destruction services)

Vehicles destroying confidential data at the customer's premises should:

- Be box bodied.
- Be fitted with lockable and / or sealable doors.
- Be able to communicate with the home base by radio or telephone.
- Not be left unattended when unprocessed material is onboard.
- Use Satellite tracked vehicles
- Be in possession of a valid Trading Standards certificate if charging by weight

7. Environmental issues

The following environmental measures need to be taken when destroying confidential waste:

- Where practicable, end products should be recycled.
- If recycling is not practicable, the cost and convenience of other methods should be taken into account, e.g. Waste to Energy disposal.
- Landfill should only be used where no other method of disposal is practical.
- Waste Transfer Notes should be issued for each consignment, or annually for regular scheduled collections.

Finding an information destruction service in your area

All members of the BSIA's Information Destruction section are required to meet all of the criteria outlined in this guide. As well as having ISO 9001 or ISO 27001 quality management system certificate incorporating the information standard BS EN 15713, the Association carries out due diligence to validate member companies.

BSIA members cover the length and breadth of the UK and are able to provide services nationally, regionally and locally. A validation certificate for each member can be downloaded from the BSIA website.

To find a reputable supplier that meets with all of the criteria that should be expected of an information destruction company and to download our compliance checklist, visit **www.bsia.co.uk/sections/information-destruction/members**

Compliance checklist for procuring information destruction services

The BSIA has written this guide to aid you in selecting an information destruction service provider.

A provider that meets industry standards, works to best practice and promotes excellent staff working conditions can ensure that the service you require meets and exceeds your expectations and ensures that your data is reliably and securely destroyed.

bsia
british security industry association

Information Destruction Service Provider Name and Address:

Question	Yes	No	Details	Expiry Date	Additional Requirements	Docs Supplied
1) Is your information destruction provider certified to ISO 9001 or ISO 27001 and inspected by a UKAS accredited inspectorate as per BSIA Information Destruction company requirements?	☐	☐	Registration No.: Certification No.:		Please attach a copy of their certificate, showing BS EN 15713 compliance on the certificate.	☐
2) Does your information destruction provider follow the BS 7858 Code of Practice for security screening of personnel employed in a security environment?	☐	☐			Please attach a copy of their certificate showing where this standard has been embedded into the third party inspection regime.	☐
3) Does your information destruction provider follow the EN 15713 Code of Practice for Secure destruction of confidential material?	☐	☐			Please attach a copy of their certificate showing where this standard has been embedded into the third party	☐
4) Does your information destruction provider have 2 years audited accounts?	☐	☐				☐
5) Is your information destruction provider VAT registered?	☐	☐	Registration No.: Date of Registration:		Please provide copy of VAT registration document or evidence of VAT registration.	☐
6) Does your information destruction provider have Public and Products Liability Insurance with a minimum of £5m?	☐	☐	Insurer: Certification No.:		Please attach proof of insurance	☐
7) Does your information destruction provider have Employer's Liability Insurance with a minimum of £10m?	☐	☐	Insurer: Certification No.:		Please attach a copy of their insurance certificate.	☐
8) Does your information destruction provider have Professional Indemnity Insurance with a minimum of £1m?	☐	☐	Insurer:		Please attach evidence of Professional Indemnity insurance	☐
9) Is your information destruction provider registered with the Environment Agency or SEPA as a waste carrier/broker under the Control of Pollution (amendment) Act 1989?	☐	☐	Registration No.:		Please attach a copy of their registration certificate.	☐
10) Does your information destruction provider have Environmental Permits/Exemptions for all of their your sites where you conduct off-site secure destruction of confidential materials?	☐	☐	Licence No's:		Please attached copies of all Environmental Permits or Exemptions	☐
11) Does your service provider complete destruction within agreed time scale? The destruction of confidential material should take place within one working day of arrival at the Destruction Centre.	☐	☐				☐
12) Does your information destruction provider issue a Duty of Care Waste Transfer Notes	☐	☐			Please attach an example of Duty of Care Waste Transfer Note.	☐
13) Does your information destruction provider hold any Trade Association Memberships?	☐	☐	Association: Membership No.:		Please attach a copy of any membership certificates.	☐

Question	Yes	No	Details	Expiry Date	Additional Requirements	Docs
14) Does your information destruction provider's premises have:						
An administration office?	☐	☐				☐
Remote monitored intruder alarm, installed to PD 6669/EN 50131-1?	☐	☐				☐
CCTV coverage of unloading, storage and processing areas?	☐	☐				☐
15) Does your information destruction provider's collection or mobile shredding vehicles meet the following criteria:						
Box bodied or demountable container	☐	☐				☐
Radio or telephone comms link to home base	☐	☐				☐
Fitted with immobiliser or alarm	☐	☐				☐
Lockable / sealable doors	☐	☐				☐

References: when procuring a data destruction service it is recommended you obtain references from prospective service providers in order to ensure that they are suitable to undertake the work.

Security Duty of Care Validation, signed off yearly.

Signature: _____ **Comments:**

Name (capitals): _____

Position: _____

Company: _____

Date: _____

Next Review Date: _____

To find an approved BSIA member

www.bsia.co.uk/sections/information-destruction/members

About the BSIA

The British Security Industry Association (BSIA) is the trade association representing over 70% of the UK's private security industry. Its membership includes companies specialising in all sectors of security. For security buyers, BSIA membership is an assurance of quality, with all member companies required to adhere to strict quality standards.

www.bsia.co.uk/sections/information-destruction

Form No 336
Issue 2
August 2018

bsia
british security industry association