Secure deletion of digital data
INDEX

1. Introduction p.3
2. Protecting data, the true challenge of our time p.4
3. What is secure deletion of data? p.5
4. To adhere to legal requirements and industry standards, the secure erasure of data is not a choice but a need p.6
5. Data recovery and data protection p.7
   Some key terminology under the DPA p.7
   What is required to stay compliant? p.7
   What is the current situation? p.8
   What’s next? p.8
6. Technical measures for secure erasure p.9
   Erasure software p.9
   Low level formatting p.9
   Degaussing p.9
   Punching or mechanical deformation p.10
   Physical destruction or disintegration p.10
   High-intensity Demagnetisation p.10
7. Devices subject to deletion or cancellation p.11
8. Professional tools to perform secure data deletion p.12
   Software overwrite p.12
   Hardware demagnetisation p.13
   Services p.14
9. Conclusion p.15
Glossary p.16
1. Introduction

Digital data security is a high priority nowadays, and it’s even more relevant when referring to the security of personal data and confidential data. Lawmakers around the globe are joining a broader debate related to the protection of privacy and personal data. The UK Information Commissioner’s Office (ICO) enforces the law against organisations that process personal data. Such a role is ever expanding given the nature of our world and dependency on computers and devices that store data including personal data.

In order to prevent the possibility of unauthorised access to data, it is necessary to ensure that the information stored within legacy or redundant IT infrastructure has the appropriate and rigorous level of protection when its life cycles comes to an end.

Most organisations invest in security but these efforts are usually focused on the protection of IT systems whilst they are still in use. However now, in light of new risks regarding the privacy of individuals, something else is required. The fundamental question that arises is how companies can protect data even when the computer systems containing them are eventually decommissioned, disposed of, reused or recycled. This problem deserves special attention, as due to the increasing speed of technological obsolescence, the replacement of IT equipment is happening on a regular basis within most organisations.

Fortunately, there is a solution for secure data deletion. With ad hoc tools, you can protect your data by eliminating it permanently from computers and other electronic devices, upon the expiry of device lease agreements, the termination of the life cycle of hardware, or whenever the organisation decides to reuse or dispose of its IT assets.

As we will discuss in the following pages, secure data erasure is also required by the current regulatory framework on privacy, represented in the UK by the Data Protection Act 1998 (DPA) and additional guidance on destruction of data as issued by the ICO.

In addition, secure deletion is an important part of the forthcoming European General Data Protection Regulation (GDPR) which will replace the EU Data Protection Directive 95/46/EC (the Directive). Details of the draft GDPR have now been agreed between the appropriate EU institutions, and once adopted, member states will have a two year window to prepare for the GDPR before it comes into force. At this stage organisations will be aware that the GDPR will amongst other things impose much stronger penalties of up to 4% of total annual turnover and will require data breach notifications to be made.

The GDPR is on track to be formally adopted in the first few weeks of 2016. The UK will be enacting legislation to replace the DPA once the GDPR is adopted within the two year window referred to earlier. The GDPR will provide, as far as is possible, for uniform protection of personal data within all the member states of the European Union. Now is the time for organisations to prepare for a much stronger privacy regime.

In this ebook, readers will find an overview of the main operational and regulatory aspects concerning the secure deletion of data. For your convenience, at the end of the ebook, we’ll also provide you with a useful glossary of terms that are most frequently used, when discussing the different concepts of privacy.

Phil Bridge
Managing Director, Western Europe, Data Storage Technologies

*Please note all content featured in this ebook is valid at date of publication, January 2016.
2. Protecting data, the true challenge of our time

The protection of electronic information and the continuous protection of privacy is the real challenge of our time for all businesses; a challenge that digital technology complicates even further.

For business leaders making decisions or for IT departments on an operational level, data protection requires a separate effort. As previously mentioned, we must ensure we safeguard our computer systems at all times, even when they get to the end of their life cycle within a particular organisation.

Nowadays all types of data, not just personal information, are at a greater risk than in the past. They represent an intangible asset that can cause a more unlawful kind of interest. High profile cyber attacks on large multinational companies are becoming more and more common.

For company data and particularly personal data, protection must be prioritised as a legal obligation towards the protection of the business itself and all parties with which the company operates including customers, suppliers and employees. Christopher Graham, the Information Commissioner stated earlier this year that “We are set for a new data protection framework in the next three years, but there are still basic things that organisations can be doing today, not only to comply with the current legislation, but also to prepare for the future regulatory landscape. Businesses should address consumers’ concerns and provide clearer information to explain when people’s details will be shared and with whom. Getting these basics right today will not only improve consumer trust, but also help a business along the road to future compliance.”

Gartner, the world leader in strategic consulting, research and analysis in the field of IT, has placed the issue of security and data protection within the top 10 technology trends of 2015.

There is no doubt that the proliferation of storage devices has complicated the management and control of information. It is precisely for this reason that today it is globally requested that there be greater attention and sensitivity on this subject. In this regard, the EU also has proposed to upgrade the protection of privacy to integrate new scenarios.

The European Commission describes personal data as “any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, your posts on social networking websites, your medical information, or your computer’s IP address.”

The European General Data Protection Regulation (GDPR) will, as far as is possible, unify the laws of personal data protection to meet the challenges of the digital age and, in particular, to reinforce its protection online. By adopting the regulation, it will oblige all companies that handle personal data of EU citizens to eliminate such information upon request, or when it is no longer required for the organisation; as well as introducing other defences and safeguards.

The constraints over the protection of privacy are destined to be further reinforced, with security requirements being continuously upgraded. Businesses are recommended to start assessing their situation as soon as possible, either internally or with the help of a third-party expert, to remedy any shortfalls.
3. What is secure deletion of data?

As previously mentioned at the beginning of this ebook, the decommissioning, disposal or reusing of your IT assets currently represents one of the most vulnerable moments for your data. Most companies don’t take appropriate precautions for the retirement of each PC, mobile device, server system or other electronic devices. At best, IT departments ensure the partial deletion of some of the content by launching the erase command provided by the operating system itself.

In the case of retiring legacy IT infrastructure, all information (including personal data) will remain completely visible and accessible to anyone who has access to that hardware. As computers are often given away to charity or sold as second-hand, simple data recovery software can be used in many cases to easily restore files that were supposedly eliminated.

Many people believe that native deletion options, such as the use of the Delete command on a selection of files, choosing to Empty Trash or Formatting the drive are all secure erasure solutions, capable of eliminating all traces of deleted files quickly and permanently. Many IT departments believe that this resolves the technical dilemma of how to dispose of storage devices without having the data previously saved on them be recoverable. Unfortunately, the fact that the content is no longer visible does not necessarily mean that it is no longer present on the storage media system, and the data previously stored there will still be recoverable.

This type of deletion, that seemingly is a simple task by just deleting pointers to the operating system where your files are located, is not accompanied by the definitive elimination of the contents of the files themselves.

Imagine you are browsing through a book. At the beginning there will be an index indicating the location of chapters through page numbers. If you get rid of this index, you would be mistaken in imagining that it equates to the deletion of the contents of the book. You will not be able to know what position a particular chapter is, but the book content nevertheless remains there and if you ‘search’ through it you will not have any trouble in finding what you are looking for.

Secure erasure is important; it’s different from the simple act of deleting file pointers and the contents of the files themselves, in fact none of the original information on your device is recoverable once it’s been securely deleted. Returning to the example of the book, it is as if by removing the index, all the pages of the chapters in the book are also deleted.

Secure erasure is important; it’s different from the simple act of deleting file pointers and the contents of the files themselves, in fact none of the original information on your device is recoverable once it’s been securely deleted. Returning to the example of the book, it is as if by removing the index, all the pages of the chapters in the book are also deleted.

Overwriting, of which we will talk more about in section 6, is a technical measure for the secure deletion of data. It eliminates not only the pointers to the files but also the files themselves. Securely deleted data is no longer present on the media itself, and cannot be retrieved, not only with the use of specific software but also by data recovery specialists.

It should now be clearer why using a secure data deletion solution is the only form of erasure that you can confidently use to eliminate personal data that complies with the data protection legislation.
4. To adhere to legal requirements and industry standards, the secure erasure of data is not a choice but a need

The final elimination of data is not a choice left to each individual company. However, rather than being perceived as required by law, secure data erasure should be adopted as best practice for the protection of data held by the company, regardless of the type of business.

Protecting the personal information of customers, suppliers, and employees is ultimately a common-sense rule; as is protecting confidential data related to the business such as intellectual property rights, development projects for new products, and accounting information, etc.

According to MarketsandMarkets, the global cyber security market is currently worth $106.32 billion and expected to grow to $170.21 billion by 2020. However, it is evident that all investments and information stored within protected IT systems become insecure if you neglect to apply adequate security as soon as hardware is discarded; leaving the existing data vulnerable.

Protecting your personal data and digital information doesn’t mean it has to be a burden on your existing IT procedures but rather an investment in security for the benefit of the company and to protect those who interact with it.

In order to fulfil the so-called quantum leap, it is important to initially begin to think about security as a process and not as a product. Safety is first and foremost a cultural approach: you need a greater awareness of the problems related to the incorrect handling of data, and use appropriate IT tools to achieve defined security objectives.

More specifically, because secure erasure will become a part of corporate culture and grow to be more effective, it should not be left to the goodwill of individual users or even to the initiative of IT departments.

Nowadays many larger businesses follow IT frameworks such as TOGAF and ITIL security management process, which provide guidelines for IT architecture compliance as well as how to incorporate security in the management of the organisation. Having these in place helps corporations continue to develop their IT infrastructure within a secure framework.

The importance of secure deletion has to be acknowledged throughout the company. As a policy it should be circulated amongst the employees so they have a clear understanding. As a logical consequence, the IT departments should be equipped with adequate tools and instruments in order to perform all new procedures correctly.

As you’ll see in the subsequent sections, it is not even necessary for the deletion process to be completed directly by the company’s IT staff. This further simplifies compliance with data protection obligations, as you can delegate the task to third-parties.
Under the Data Protection Act (1998) ("DPA"), any individual or business handling or “processing” personal information needs to ensure that it is properly protected. It is essential that any and all devices being sent for destruction or resale are completely clear of data.

If anyone, criminal or otherwise, manages to recover data from an old device, your business, as the owner of such a device, is in breach of the DPA and will be held legally responsible. This could mean that enforcement action will be taken by the Information Commissioner and that your organisation will receive a substantial fine.

Some key terminology under the DPA

It is the data controller that will face enforcement action against it, or possibly a fine under the DPA. It is the role of a data controller to protect the personal information belonging to data subjects and to therefore ensure anyone acting on its behalf as a data processor complies with the DPA’s strict provisions.

A data controller can be a person, but usually is an organisation. The data controller determines the purpose for processing of personal data and may appoint a data processor to carry out certain functions such as data destruction on its behalf.

Data processors often are external contractors, who may be appointed to handle the personal data belonging to your clients for specific tasks. In the guidance provided by the Information Commissioner, it is recommended that strong contractual provisions are put in place to ensure data processors also adhere to the provisions of the DPA principles.

It is the Information Commissioner who has the legal powers to enforce the provisions of the Data Protection Act. These powers may be used as a result of a complaint by a data subject. A data subject is the living individual to whom personal data relates. The data subject will have given consent to the data controller for processing of his or her personal data in accordance with specific instructions which have been provided to him/her.

What is required to stay compliant?

The Data Protection Act outlines 8 key principles by which all data controllers are bound. However it is Principle 7 that is of key interest in the case of data destruction and device disposal:

“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.”

The DPA does not actually specify what deletion means within the ambit of ‘appropriate technical measures’, but the Information Commissioner has issued guidance to say that personal data must be unrecoverable when disposing of hard drives and other data storage media. Archiving data is therefore not considered as deletion.

The suitable approach to data deletion will depend on how the device is being disposed of.

Resale

Any storage media that is resold must have been completely wiped. This means that all data must be erased, completely overwritten and formatted again to prevent any recovery. All Blanco erasure software
solutions from Kroll Ontrack offer 100% secure data erasure whilst leaving the device fully functioning.

Recycling/Disposal

If the device is being recycled or otherwise disposed of, there is a wider choice of erasure options. Software deletion can be used, although it is relatively slow and cumbersome – particularly if there is a lot of hardware to be processed.

For devices that store data magnetically, the alternative is to use a tool like the Ontrack Eraser Degausser which physically destroys each disk or piece of media by altering the magnetic fields that govern data storage in each disk platter, rendering the device completely unusable. The process takes around 4 seconds per unit, and the results are irreversible. It has the added benefit that it is also more cost efficient than other physical destruction options (such as shredding) as it can not only quickly process a much larger number of devices. Additionally, it is CESG certified so there is certainty of complying with regulatory demands.

One other thing—ICO registration

As a data controller, you are expected to register with the Information Commissioner’s Office (ICO). Registration costs £35 per year and is a legal requirement.

You are also expected to report breaches of the DPA direct to the ICO as soon as they are discovered.

What’s next?

Despite being less than 20 years old, the DPA (which is based on the EU Data Protection Directive 95/46/EC) has struggled to cope with the technological changes and challenges of the 21st Century. As a result, the new EU General Data Protection Regulation (“GDPR”) and additional associated data protection laws will be formally adopted in 2016. The GDPR itself will come into effect two years later in EU member states.

The DPA will be replaced with more stringent data protection legislation and requirements as a result. Importantly, the GDPR is designed to tackle the challenges of personal data security and privacy in the age of the global, data-driven marketplace. The basic principle of protecting subjects’ data from loss or breach will remain unchanged although data processors as well as data controllers will also have liability under the new law.

Expect to see greater emphasis on transparency, so that data subjects have a better understanding of how their information is stored, processed and deleted. The penalties for non-compliance will be increased to up to 4% of total annual turnover for breaches. Such strong enforcement acts as a key incentive to businesses to ensure that data storage hardware is disposed of responsibly.

With significant legislative changes like this on the horizon, it is critical that businesses ensure that their hardware disposal and data erasure routines are compliant with current legislation and that they audit their processes, increase rigour and prepare for a stricter regime. Such preparatory work will then mean that much less effort and cost will be needed if organisations are required to raise standards when the new legislation comes into force.

In the UK, the ICO issued £1,078,500 in fines for legislative breaches during the 2014/2015 period, a contraction from previous periods.
6. Technical measures for secure erasure

In its guide for small and medium-sized businesses, the ICO explains that “An organisation that processes personal data is required to handle personal data in accordance with the data protection principles. A data controller may choose to use another organisation to process personal data on its behalf – a data processor. The data controller remains responsible for ensuring its processing complies with the DPA, whether it processes in-house or engages a data processor.” In other words, it is not necessary that companies take on the physical, secure erasure procedures themselves. Where there is a lack of appropriate skills, resources, and/or time allocation, you have the option to outsource this activity to competent suppliers, available in your area—but bear in mind the responsibility for the effectiveness of the process remains with you.

The technical measures for the secure deletion of data applicable to electronic devices are identified according to the following table:

<table>
<thead>
<tr>
<th>If the device is intended for re-use and recycling, the actual data deletion can be completed with:</th>
<th>If the device is intended for disposal, you can also achieve secure deletion of optical storage or magneto-optical with the following procedures:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erasure software</td>
<td>Degaussing</td>
</tr>
<tr>
<td>Low level formatting</td>
<td>magnetic devices</td>
</tr>
<tr>
<td></td>
<td>Punching or mechanical deformation</td>
</tr>
<tr>
<td></td>
<td>Physical destruction or disintegration</td>
</tr>
<tr>
<td></td>
<td>High intensity demagnetisation</td>
</tr>
</tbody>
</table>

Next we’ll take a more in-depth look at the pros and cons of each solution.

**Erasure software**

As the term suggests, this software overwrites random sequences of binary digits (ones and zeros) onto the existing data. The overwriting operation is to ensure greater protection; it is repeated several times in order to minimise the possibility of recovering original information through software or of a higher technical data recovery intervention.

It is important to consider that different media types (such as HDDs, SSDs and flash) will require different overwriting techniques to ensure the secure deletion of the data. The number of passes each type requires affects the time it takes for the erasure to complete, which can be a few hours or a few days depending on the type of media and write speed.

**Low level formatting**

A particular type of formatting applied to the hard drive by following the instructions and using any erasure software provided directly by the manufacturer.

**Degaussing**

A special technique of permanent deletion of data applicable to memory devices based on a magnetic or magneto-optical (hard disk, floppy disk, magnetic tapes on open reels or cassette). It is able to ensure the rapid deletion of information from media to which you cannot apply overwriting erasure software.

The physical principle underlying the degaussing relies on the polarisation of the Weiss domains.
The data is stored on magnetic media, such as hard disks and tapes, whereby a magnetic field is applied to very small areas called magnetic domains, specifically Weiss domains. This process is based on the theory developed by French physicist Pierre Weiss. The magnetic field whilst in the writing phase of the information impresses a verse, which orients the magnetisation of a certain number of Weiss domains. These verses of the magnetisation are associated with the bit values 0 and 1.

By subjecting magnetic media to degaussing, the magnetisation within the Weiss domains is disturbed resulting in the arrangement of the fields being no longer in one direction but rather randomised, therefore the data is no longer accessible nor recoverable.

The demagnetisation process employs the use of an adequately powered hardware tool called a degausser. In contrast to overwriting software programmes, the time taken to complete an erasure through degaussing can be standardised, no matter what type of media or its data capacity. Another difference from overwriting erasure software is that a device subjected to demagnetisation is no longer reusable, so long as the degausser used is powerful enough.

Punching or mechanical deformation

Punching refers to a drilling procedure obtained by pressing or hitting a punch on the surface of the device to be drilled. The mechanical deformation obtained by distorting the storage media or by modifying its geometry, dimensions or its form makes the data inaccessible.

Physical destruction or disintegration

This process is mainly used to reduce to fragments the storage media through the use of specific apparatuses equipped with suitable cutting blades.

High-intensity Demagnetisation

Applicable to magnetic storage media as discussed in point 6.3 Degaussing. It is also usable on failed devices that cannot be subjected to overwriting erasure software procedures.

Figure 3—A graphical representation of Weiss domains in a material subjected to a magnetic field.
7. Devices subject to deletion or cancellation

The devices subject to deletion include computers, desktops, laptops and servers as well as external storage media. The law speaks in general of supporting the legal obligation that exists in relation to the type of data contained therein. Any type of storage media containing personal data should be subject to safe erasure procedures and should include any device that contains information you want to keep private and confidential. Hard drives, SSDs, flash media of various types and formats, USB drives and magnetic tapes represent only a small sample of media to consider. A relatively new category of storage but one that is especially critical is mobile devices.

Smartphones and tablets, despite their small size, now offer considerable storage space and are now considered standard equipment for most employees. According to data obtained by Smart Insights, mobile devices are now more popular than desktops globally.

It is therefore very important when business mobile devices are withdrawn, to include them in the secure deletion process. It is important to note that smartphones and tablets contain the same information that you can find on devices such as desktop and laptop computers (e.g. email and documents) and even more data if we consider SMSs, phonebook and call logs.

The issue is far more complicated in businesses where BYOD (Bring Your Own Device) is implemented in which case the employee uses their own personal device for work activities. Since you cannot usually distinguish between professional and private data, secure deletion could potentially also remove the personal information of the device owner.

It is appropriate then that companies carefully evaluate all legal aspects before deciding on implementing a BYOD policy.
8. Professional tools to perform secure data deletion

The choice of software or hardware tools each company uses to perform a secure erasure process needs to be considered in detail. Not all tools on the market are effective and have the suitable features to ensure business compliance with the current privacy legislation. It is also best to avoid do-it-yourself solutions as they are very risky in terms of effectiveness; and completely inadequate in providing a company with a professional and verifiable deletion certification or audit trail.

With the right tools you can create an effective deletion process that is easy, compliant and has a low cost per device. Professional products are characterised by:

- Independent certification
- Use of standard international algorithms
- Technical characteristics suitable for this purpose
- Detailed reports
- Traceability of deletion that has been carried out

It should also ensure full compliance with your company’s rules and regulations.

Kroll Ontrack solutions meet every requirement in the field of secure deletion and include:

- Software overwriting
- Hardware demagnetisation
- Services performed by specialised technicians

Software overwrite

Kroll Ontrack’s expertise in data recovery and erasing hardware and services, partnered with the market leading eraser software solutions from Blancco Technology Group, offer a portfolio of software solutions for the secure elimination of data. The erasure software suite is the most complete end-to-end solution for erasing all of your organisation’s IT assets, including PCs and laptops, servers and storage environments, LUNs, virtual drives, virtual machines, smartphones and tablets, flash media devices and even individual files and folders.

Each device can, therefore, have a unique software solution that is best suited to its characteristics:

- **Blancco 5**—A high speed, efficient and flexible total erasure solution for PCs, laptops, servers and storage environments that enables safe disposal and reuse
- **Blancco Management Console**—Designed to help manage IT asset disposal processes, including erasure software distribution, hardware asset management, and erasure reporting for auditing purposes
- **Blancco 5 Mobile**—Secure mass erasure of Android, iOS and Windows smartphones and tablets
- **Blancco Flash**—Erase flash media storage devices stored within smartphones, tablets, network routers, and cameras etc
- **Blancco File**—Erase files and folders on active PCs, servers and virtual machines to prevent data breach
- **Blancco LUN**—Centrally erase logical drives like LUNs and virtual machines in an active storage environment
The erasure software suite offers:

- **Detailed reporting** of any erasure or cancellation, required to confirm the task execution
- Possibility to choose between different erasure algorithms, all compliant with international standards
- **Numerous certifications and recommendations** from independent third parties
- The manageability of this product platform is provided by a hosted web console or property through which it is possible to centralise the administration of permits and reports of the deletion. The company can then view and manage in one place the erasure processes of all their IT assets

Hardware demagnetisation

**Ontrack Eraser Degausser** is a professional hardware device for secure deletion through a demagnetisation (degaussing) process. It is one of the most powerful degaussers in the market, able to generate peak magnetic field strengths of up to 18,000 gauss (1.8 tesla), with 10,000 gauss (1 tesla) hitting the core of the device.

A magnetic field of such power not only offers the guarantee of successful elimination of data from newer hard disks, but also to safeguard the investment of the future with the use of disks that have a high recording density and coercivity factor.

Not all degaussers, in fact, are able to permanently delete data from hard drives and tapes. You must bear in mind that a magnet opposes some resistance to demagnetisation called magnetic coercivity. Coercivity is the intensity of the reversed magnetic field that must be applied to a material to cancel its magnetisation. For a degausser to be effective, it is necessary that it is able to generate a magnetic field of at least equal to 1.5 times the coercivity of the support that needs to be deleted.

What follows is that the higher the power of the degaussser, the greater its effectiveness and the possibility to use it on future technology hard disks and other magnetic media. The degaussing procedure lasts only a few seconds; simply place the device in the compartment and push a button to initiate the demagnetisation. The media will not be reusable after this procedure.

Ontrack Eraser Degausser is effective and safe to use around people as well as other equipment and objects. The low-frequency magnetic field is concentrated to one area, where the action is well below the limits currently recommended by the ICNIRP—International Commission on Non-Ionising Radiation Protection—to the overall exposure of the general public.

Ontrack Eraser Degausser is certified by CESG (The National Technical Authority for Information Assurance) and is suitable for the safe erasure of media with classified information. The unit also has international accreditations including:

- **NATO | OTAN approved to NATO Confidential**
- Approved by the [Norwegian Security Authority](#)
- [CSA](#) approved (CSA test and certify products in the US and Canada)
- Approved by the [BSI](#)—German Federal Office for Information Security
- Accredited in Norway under test 033
Services

For companies that prefer to rely on a skilled third-party provider to fulfil their legal obligations or need to confirm the deletion process has been successful, Kroll Ontrack offers two types of services:

**Services for secure data erasure**

Technical personnel can perform erasure operations with the Ontrack Eraser Degausser tool directly at the customer premises (on-site) or on the devices submitted to the Kroll Ontrack laboratory (in-house). The process is subsequently attested through an appropriate report, confirming the successful execution of the erasure process on the devices, which are then processed for disposal.

**Erasure reporting services for audits/verification (Erasure Verification Services)**

*Erasure Verification Services* are necessary to guarantee sanitisation of data on media intended for reuse or disposal. Organisations that do not verify the expunging of data on their media leave themselves open to accidental exposure or theft of sensitive data.

Devices are analysed by our technicians in our laboratories using sophisticated data recovery tools in order to identify any traces of user data. In the case of success (no trace data found), Kroll Ontrack will release a report as per the customer’s request confirming that it has been checked and the data erasure process used was adequate.

If instead we find traces of data it will be immediately communicated to the customer so that they can make the necessary adjustments to their deletion process.

**Managed end of life services**

Other complementary services available for devices at this stage of their life cycle worth mentioning include onsite infrastructure decommissioning and the secure disposal of IT assets. It is important to ensure the full lifecycle of the device is covered as even at this stage it is possible to incur in fines should this not be done properly.
9. Conclusion

The Information Commissioner’s Office guidance on how businesses can protect individuals’ information access and unauthorised distribution is nowadays even more relevant due to the ever increasing amount of personal data collected and processed by all types of businesses.

The ICO’s Guide to Deleting personal data provides details for companies on the appropriate measures that need to be taken to ensure the proper sanitisation of devices that contain personal data, including violations to these guidelines and related penalties. It is also worth noting that it is necessary to put erasure processes in place for end-of-life media that is due to be decommissioned / recycled, but also for through-life data during the regular lifecycle of devices.

The new General Data Protection Regulation (GDPR) will aim to standardise and will update the protection of personal data so as to face the new challenges of the digital era.

In this scenario, the solution to the problems discussed takes the name of ‘secure deletion’; a safe form of erasure that utilises special techniques which ensure the permanent deletion of data from computers and other electronic devices beyond any possible recovery.

For businesses, the easiest way to implement this is to set budget aside at the time of purchasing any new hardware, and then utilise the service when the device needs to be disposed of or reused. Companies may also decide to outsource this service to qualified third parties.

To overlook and ignore this stage of the data lifecycle can be a very high risk and expensive option. Overlooking end-of-life data and the incorrect management of data procedures, including the disposal of computers and IT assets containing personal data can become a serious threat to the security of company information; it also opens the company up a potential risk for penalties and breaches of privacy legislation, which can cause irreparable damage to the businesses image and reputation.

THE AUTHOR

Phil has been at the helm of UK activity for the world’s foremost data recovery company since 2006. In addition to leading the UK business, Phil manages Western Europe operations with facilities in UK, France, Spain, Portugal, Ireland and Belgium.

He has been with Kroll Ontrack for over 18 years, moving from sales to global channel manager to business development manager to managing director. This has led to Phil having an extremely well rounded view of the company and an in-depth knowledge of the industry.
Glossary

The definitions below correspond to the terms used in the Data Protection Act as explained by the ICO.

**Personal data** means data which relate to a living individual who can be identified:
- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

**Sensitive personal data** means personal data consisting of information as to:
- Racial or ethnic origin of the data subject
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Whether the data subject is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission by the data subject of any offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

**Data controller:** 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:** 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:** 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:
- Organisation, adaptation or alteration of the information or data
- Retrieval, consultation or use of the information or data
- Disclosure of the information or data by transmission, dissemination or otherwise making available
- Alignment, combination, blocking, erasure or destruction of the information or data

**Inaccurate data:** for the purposes of this Act data is inaccurate if it is incorrect or misleading as to any matter of fact.

**Recipient:** in relation to personal data, means any person to whom the data is disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom it is disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.

**Data subject:** an individual who is the subject of personal data.