ADISA
ASSET DISPOSAL & INFORMATION
SECURITY ALLIANCE

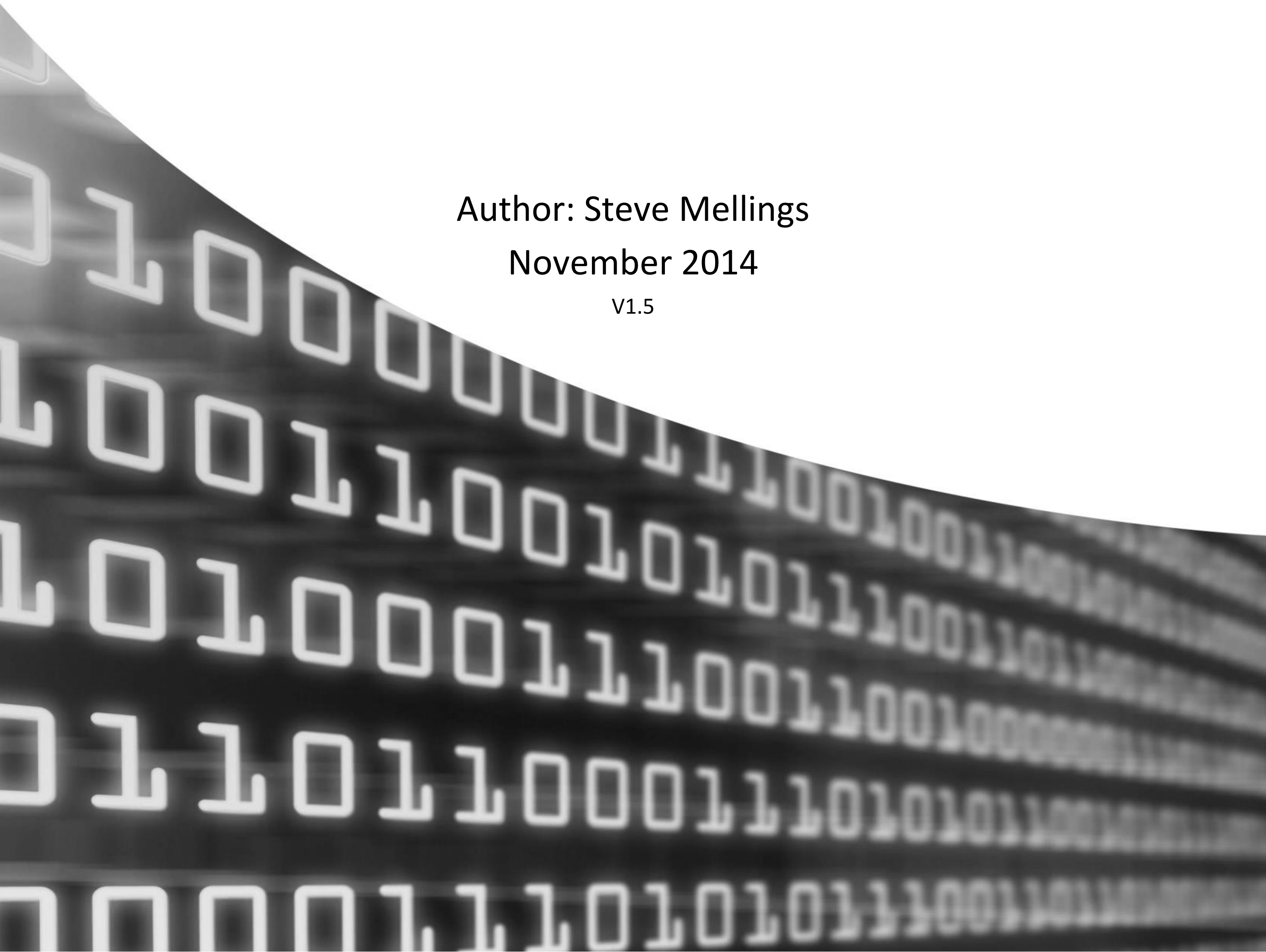
ADISA WHITE PAPER

Complying with current, and potential future changes to EU Data Protection Law when disposing of ICT Assets

Author: Steve Mellings

November 2014

V1.5



Abstract.

With many companies already struggling to comply with existing legislation, the spectre of a new and significantly amended EU Data Protection Law is quickly coming into view. This re-write is the most significant change in Data Protection within the EU since the EU Data Protection Directive (officially Directive 95/46/EC) was introduced in 1995. This review comes at a time when the pace of change in technology and most importantly attitudes to hardware ownership and privacy, are evolving at an even quicker rate.

So whilst businesses are aware of the need to protect the data held relating to individuals, as well as their own corporate information, many are unsure precisely what would be viewed as acceptable in the eyes of the regulators and lawyers.

This paper reviews one critical area, ICT disposal, and relates it to current UK Data Protection requirements based on the 1998 law. It then introduces some of the proposed changes happening to the EU Data Protection legislation and concludes with recommendations for businesses to follow in order to not only comply with current UK Data Protection Law, but also hypothesises on steps to take to future proof against changes to the law and technology.

The target audience for this paper is compliance and in-house legal experts and it is therefore assumed that the reader has an understanding of the current UK Data Protection Law. The objective is to bridge the gap between legal requirements and operational non-compliance, to help create an internal demand to review and correct areas of known operational risk.

Author Note.

I feel it is important to emphasise that in my opinion the most crucial step in improving organisational data protection is by changing company culture. Business leaders must acknowledge the importance of data protection and empower their staff through training, budget and resource, in order to create an environment where data protection is second nature. Without this cultural empowerment, the road to improvement will be long and extremely challenging and those involved in data protection and information security will be viewed in many instances as business inhibitors or simply as custodians of the burden of regulatory compliance.

In such a challenging environment how can they be expected to perform without support and direction from the business as a whole? Data breaches can, and do, happen from the most embarrassing of oversights and technology alone cannot win this battle. Just ask the office of Oliver Letwin MP[1].

Steve Mellings
September 2014

What is ICT asset disposal?

As individuals we have a nature to consume resources at an alarming rate. For ICT equipment, not only has there been a predisposition to demand the latest and greatest technology, but there has also been refresh catalysts driven by the manufacturers, resellers and software developers. This has created a “use and lose” approach to hardware. Within the wider world of ICT, the perception is that once infrastructure has finished its life with them, then it is simply waste and those who remove it are the “ICT Dustmen”. However, a failure to understand that disposal includes three assets – data, software as well as hardware – leads to poor policy, poor operational process and most of all, to uncontrolled risk taking.

This often-maligned process continues to allow data to leak from business unabated. Within the last 12 months there has been a second significant fine[8] in regard to data breached as a result of improper IT asset disposal. This has taken the total fines issued to over £500,000 in the past 18 months, all due to this business process. In the US, Coca Cola suffered a significant breach[5] when a staff member stole redundant equipment, rather than place it into the disposal route. So how can such a seemingly innocent process go so badly wrong?

To understand this let us first define asset disposal. ADISA’s definition is as follows:

“Any situation where the data controller transfers custody of an ICT asset to a third party for management or processing, whether on a temporary or permanent basis”.

Diagram one, whilst not exhaustive, shows that there are many opportunities for hardware to leave the control of the data controller. Most of these processes are managed behind the scenes often with little management oversight and generally are viewed as troublesome.

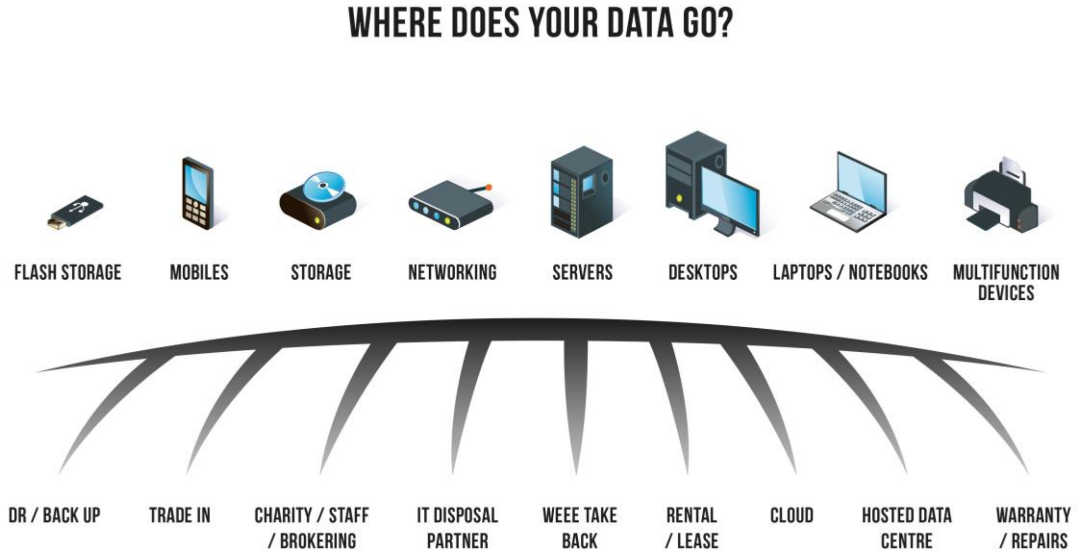


Diagram 1. Sample of business processes and product sets which are included within asset disposal.

What is ICT asset disposal? (cont.)

Furthermore, whilst technology has changed dramatically in the last decade, the business process of disposal has not. Not only does this process now include different product types, but also different media. Magnetic hard drives are the default media, but with increased usage of smart phones and tablets, solid-state media is becoming more prevalent. We mustn't forget tape either!!!

To increase complexity, let us consider outsource arrangements, the use of cloud and bring your own device (BYOD). We can now see that what at first seemed a simple process is actually far more involved. Whereas companies historically may say "our policy is to destroy all hard drives" this will no longer cover all potential outputs from business or all data carrying media. The recent Ministry of Justice fine[10] for the loss of an unencrypted back up hard drive shows that data protection efforts must focus on all areas where data carrying assets are managed, not just whilst on the network

A failure to see the hardware they are disposing of as anything other than "old tin", to view it as waste management, or simply as an asset for resale isn't enough. Companies must understand that when they release their IT and telecommunication assets they need to apply the same attention to asset management and security as they do to the assets when in life. Asset disposal is an evolving and important business process, which when controlled through an intelligent asset disposal policy can manage risk and promote re-use and therefore create both financial and social benefits.

Current UK Data Protection Act 1998.

In order to keep the legal jargon as light as possible, this is a very simple introduction to the Data Protection Act 1998 and is largely taken from the Information Commissioner's Office website.

The UK Data Protection Law is designed to safeguard data held about individuals and is a complex and very broad ranging piece of legislation, but is underpinned by eight basic principles.[2]

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 Two of the Data Protection Act is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule Three of the Data Protection Act 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.

In addition the Information Commissioner's Office offers the following guideline in regard to what activities are regulated by the Data Protection Act: [2]

The Act regulates the "processing" of personal data.
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.

So we can see that The Data Protection Act 1998 applies to data about an individual regardless of whether the data created can be attributed to an individual, either as subject matter or author. Failure to abide by the spirit of the eight principles will result in a company failing to comply with the letter of the law. Sounds simple doesn't it? Let's relate it to ICT Disposal.

Relating the current UK Data Protection Act to ICT Asset Disposal.

Before discussing the Act, let me get the disclaimer in! I'm not a lawyer and law can be interpreted and argued in many different ways. As such this interpretation should be viewed as ONE interpretation based on various discussions with in-house and external council and with the Information Commissioner's Office (ICO) itself. Furthermore by reviewing the penalty notices issued by the ICO and with previous regulatory fines (such as the old FSA), a trend can be identified in terms of failings by the data controller, where actions have been brought against them for breach, as a result of a failure in the disposal process.

Whenever the UK Data Protection Act 1998 is discussed, the eight principles are used as THE point of reference and for asset disposal principle seven is the key. To reprise: "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."

When pressed Alastair Barter of the ICO stated that the term "Appropriate" was used because the law had to be as relevant to a butcher as it is a banker. A simple but very rational way of explaining why, in some people's eyes, the law leaves room for interpretation and lacks clear guidance.

But when the Seventh principle is laid bare, it is really rather simple. Ask yourself, "Are my current processes appropriate to the data which I am transacting and to the industry in which I am operating?" If you cannot answer that in anything other than a clear affirmative, then you have cause for concern.

Within asset disposal we can break the key compliance areas down into the two sections within the Seventh Principle; Technical and Operational.

Key Requirement 1: Appropriate Technical Measures.

The greatest technical decision for the data controller to make is to define the act of sanitisation itself, as different media types can have different processes applied to them in order to make data irretrievable. Sadly, within IT Asset disposal the breaches which occur are generally not as a result of a forensic level attack or of a failure of an erasure product, but occur as a result of no effort being made to sanitise data on the device at all, in other words operational failure. As such, companies who focus entirely on the act of sanitisation itself only protect themselves from one aspect of potential breach.

That being said, it is essential in order to comply with law, to have a very prescriptive and measured approach to sanitising each media type. To have within your policy "Must ensure all data is erased" does not go far enough, as in one person's eyes that could mean just deleting the files and leaving them in the recycle bin. Clearly this would not be acceptable, but to ensure an organisation can show appropriate technical measures ADISA argues that data controllers should be very clear about what technology should be brought to bear on each media, to ensure that data is not available to either the next asset holder or to a potential threat adversary. ADISA advocates the use of an "Approved means of sanitisation table" such as Table 1.

Relating the current UK Data Protection Act to ICT Asset Disposal (cont.)

Media Type	Product Set	Risk Level	Process to be undertaken within Company A	Means of Sanitisation to be achieved at Partner Site
Magnetic Hard Disk Drives	All	High	Remove from Parent, inventory drive, remove controller board, secure stores, destroy to 22mm using third party on site shred	n/a
Magnetic Hard Disk Drives	All	Normal	Inventory Chassis, Secure Stores, Ship	CESG Approved Over writing at baseline level. Failed devices are destroyed by an approved physical means at partner site
NAND Based Media	Laptops and general storage	All	Inventory Chassis, Secure Stores, Ship via Secure Tote	Company Approved Over writing software to be used. Failed devices are destroyed by an approved physical means at partner site
NAND Based Media	Smart Phones	All	Manufacturers reset, Inventory via IMEI	Company Approved Over writing software to be used. Failed devices are destroyed by an approved physical means at partner site
NAND Based Media	Networking	All	Inventory. Manufacturers reset	Write bad data to device, manufacturers reset
Hybrid Disk Drives	All	All	Remove from Parent, inventory drive, Secure Tote	Destruction to 22mm
Magnetic Tapes	All	All	Inventory, Secure Tote	Destruction to 22mm
Optical Disks	All	All	Inventory, Secure Tote	Destruction to 2mm
Paper / Microforms	All	All	On Site Shredding in every office	Collected

Table 1: A sample of an “Approved means of media sanitisation.

A prescriptive approach such as this is a crucial part of policy development and provides the starting point of building both internal and external operational processes. The examples here are purely for illustrative purposes and follow a risk-based methodology.

Relating the current UK Data Protection Act to ICT Asset Disposal (cont.)

Key Requirement 2: Appropriate Organisations Measures.

To say that asset disposal as a process is viewed dismissively, not only by many individuals but also by many organisations, would be an understatement. Crude processes controlled by loose policy and delivered by poorly managed partner arrangements, leaves much to be desired and in both of the recent penalty notice charges issued by the ICO it is the lack of control over the process which has been the underlying issue.

My personal opinion as to what should be deemed as appropriate is based largely on how organisations manage and protect their assets when in life. Most visitors to a data controller are required to sign in at a reception, they are escorted whilst on site and generally are kept in areas of relatively inert operational activity; meeting rooms, etc. So why do companies have such attitudes to visitors and yet when businesses release assets they often do so with very little control over the companies and people who provide these services. My own argument is that as you are releasing data bearing assets from the controls of your own environment, that the procedural controls that you expect from your partners should EXCEED those of your normal business operations.

Policy.

The starting point for appropriate organisation procedures would be the existence of a policy. Without a policy there is no organisational control and no guidance for individual action. Policy should be fit for purpose, meaning it dictates the technical aspects of the process and also dictates internal and external procedures. It should include prescriptive statements including how data is to be sanitised, how assets are to be managed at each stage.

Service Specification and Vendor Selection.

Organisational measures need to include a clear specification for vendor selection. For the NHS Surrey[8] penalty the ICO expressly reference “free service” indicating that a decision based purely on lowest bid (and other factors clearly) will leave the data controller exposed should the worst happen. The vendor selected should be able to provide evidence of professional competence to deliver the service. For ICT asset disposal I will of course say, ADISA Certification; as that is the very reason why the programme was developed. In the UK alone there are 750 service providers all seemingly offering comparable services, but the number offering a competent secure process is, in my experience, less than 10 per cent of those in the market at a whole. This is no reflection on their professional diligence, but simply a reflection on how business end users have traditionally placed their business. A poor quality downstream is a greater reflection on customer expectation than on the industry itself.

Contract.

When looking to use external parties they should be governed by a contract, which includes a clear and prescriptive service specification. This specification should include relevant guarantees in regard to their compliance with the service specification and should clearly state that the partner selected is designated as the data processor. This point is essential when looking at the changes in the Data Protection Act, potentially coming into force later this year, which are expanded on later.

Relating the current UK Data Protection Act to ICT Asset Disposal (cont.)

Ongoing Management.

It is crucial that this relationship is then managed, not only in a transactional sense, but also in a monitoring sense. Regular audits, ideally unannounced, will ensure that the processor will be viewed as an extension of the data controller's own environment and that the processor is being assessed in a continuous and random way. A recent freedom of information research project into local councils showed that a staggering 60% of responders have NEVER audited their ITAD partner and a further 10% audited over two year ago.

Inventory Control and Verification.

The controller themselves have a number of very key organisational responsibilities, not least being the creation of a proper inventory list. I say "proper" as many of the inventory lists provided to the industry are nothing short of fiction. A strong position would be to have a full and accurate inventory of assets, which are then transferred into the custody of the processor at the point of release from the controller. This can then be verified against the audit report received and against any certificates of overwriting which may be produced. This is the most crucial part of where asset disposal goes wrong. Companies who release assets to any third party without knowing what they have actually released can clearly not be deemed as executing appropriate organisational measures.

Some companies have the opinion that, "We're ok", "We've never had a problem" but that almost fatalist stance is simply waiting for the inevitable to happen. Professor Andrew Blyth of University of South Wales has performed a disk study over the last few years which has, on average, shown that over 40 per cent of all hard drives bought through auction sites contain data, and very little forensics are required to recover that data. Furthermore, in Africa, scene of much of our e-waste dumping, there are organised gangs scavenging the waste dumps, not for the cabling that upon burning will release the much sought after copper, but for hard drives. From these they seek data and use that for blackmail purposes. Just ask United States Republican Congressman Robert Wexler, who was blackmailed by a gang from Ghana[9,] after his data was found in a landfill. Rest assured, just because your name isn't in the headlines, the volume of data in the broker and e-waste market is truly astounding.

So we have introduced a seemingly simple business process of ICT asset disposal and related that to current legislation with recommendations for some (very) basic steps, which the data controller should take in order to show compliance. When these steps are reviewed, it may surprise many that in my experience spanning over 15 years in and around this process, I would say that, being generous, less than 20% of businesses comply with the basic steps I have suggested. This is leaving their execution of this process in the lap of the gods and owing more to good fortune and almost certainly good suppliers and people, rather than good organisational control.

So we now look forward, to the changing face of legislation and technology and hypothesise what additional steps may be required by a company seeking compliance in this process.

The changing face of Data Protection.

The current Act was passed into law in 1998 and since then, whilst the law has stayed still, the Internet, social media, mobile working, cloud computing and a general attitude of decreasing our privacy and increasing our availability, has swept through, not only the business world, but also our very culture. In the face of this, the law, which is meant to help protect privacy of the individual, has clearly been left behind and after acknowledging this; the EU commission are currently re-writing their 1995 directive from the ground up.

It should be stressed that at this point in time – September 2014 – there are thousands of amendments still to be discussed and some crucial elements to be agreed, including whether it becomes Law rather than a Directive. There are, however, some key elements which are clear and widely expected to be approved and for the world of IT asset disposal it is essential for companies to understand these and to bring their houses into order.

When you consider that the previous section highlighted how many companies are deficient in complying with the existing law, why should any new law change make a difference?

Increased penalties.

There is a seed change from the regulators in terms of the powers, which they can bring to bear; currently in the UK the ICO can impose a fine of a maximum of £500,000. Eye watering to many, but to large corporates a figure they could cover easily. This is changing with the rumours being two to five per cent of global turnover, or a maximum of €100m fine being able to be levied. Clearly these figures are not set in stone but the stick has now got much bigger!

Mandatory Breach Notification.

Currently, outside of the telecommunication sector[3], it is not mandatory to notify the data regulator of any actual breach. This results in the register of those suffering a breach being largely populated by public sector offenders, rather than in the commercial sector. This has caused much criticism of the public sector, and in particular the NHS, but it is my belief that this is a cultural issue as opposed to actual culpability. In a company governed by shareholders where brand is key I may feel significantly less inclined to disclose a breach to the ICO unless it was so significant (Zurich 2010[7]) or it was sure to make the press. However, this is changing, within the new act there is provision for obligatory breach notification to happen. The mechanics of this remain unclear and the crucial question of "what constitutes a breach" is also unclear, but this is further evidence of the hardening of the position of the law.

Legal liability for data processors.

Companies who collect ICT assets for data sanitisation services are classed as data processors when contracted to do so by a controller. Even where no contract exists, if a professional understanding is in place it could be argued that the supplier can be classed as a processor. At present there is no legal liability should these companies fail to do what they say they are doing, in other words, currently the data controller owns all of the risk. In one of the high profile breaches mentioned previously we know of commercial action being taken against the supplier by the controller, NOT by the ICO. With the new regulation the data processor will have legal liability alongside the controller.

The changing face of Data Protection (cont.)

Largely to address cloud computing this subtle but important change will see those companies who offer data processing services step out of the shadows and into the firing line. As such in order to have your partners share in the liability a professional relationship will be required. Ad-hoc collections of “a room of old kit” won’t be classed as professional. At ADISA we are already encouraging our members to engage with their customers in a far more formal way than many are expecting. This enables our members to control the engagement and effectively manage their own risk. When the law changes any company that is happy to just turn up and collect with little control is not controlling their risk and liability. This change has even be identified by the insurance sector with the first data processor insurance policy being released in September 2014.[11]

Changing technology.

Whilst not directly relating to legislation there is a whole host of ICT initiatives, which could impact significantly on ICT disposal. Bring your own device (BYOD) brings a whole host of challenges, not least that for many users devices utilising solid state storage (SSD) would be preferable. At present with SSD there are no government-approved software overwriting products leaving the secure minded companies the option of physical destruction. The idea of seizing a leaving member of staff’s own device and then shredding it will be an interesting one for the corporate lawyers to address. Of course, ensuring that no data is stored on the device is one option, but for smart phones that is clearly not feasible. So when an employee leaves, taking their tablet or phone with them, what are your options? In order to show compliance the same controls need to be in place, as with any end of life device and thus the disposal process outlined in the previous section should apply here.

For cloud service providers’, data replication and storage management make it extremely challenging to control precisely where your data is and what is happening to it. On a very basic level data it is still stored on a physical device and if that storage device fails you would never know, but the question of what happens to that device remains. When engaging with the cloud clear controls need to be put in place for many areas where security is concerned, but the addition of specific controls over the disposal of failed or refreshed hardware is essential. It would be important to also classify the cloud provider as a data processor, but as they are only responsible for hardware (in many instances) then this could be a challenge. To have data services such as sanitisation bundled with the service would allow designation of the provider to be a data processor and therefore liability would be shared with them.

Data Protection Officer.

For businesses of a certain size, I have heard 250 or 400 data subjects being used as the entry point, they will be required to have a designated role; Data Protection Officer. This role will have express responsibility for the company’s overall data protection activities and at the time of going to press, the job specification will have elements mandated by law including a guaranteed time in position making this perhaps the safest, but least desired role in many organisations!

Referring back to my author’s note, assuming that the DP Officer role is given genuine responsibility and status within a business, then this could perhaps be the starting point for a change in culture within business, which could see the pace of improvement in this area accelerate.

Conclusion

For many companies compliance with law, with industry regulations, or even with their internal policies can sometimes be an opt-in and opt-out approach. The pressure of business ensures that focus is given to those areas where operations directly impact the business itself. However, with the rumoured changes to the data protection law getting more clarification and support, data protection is an area that only the brave will ignore.

For those who have data protection, information security or even brand protection within their remit, all aspects where their own company could be compromised needs to be reviewed, a risk assessment to take place and remedial actions to be enacted. One such area must be the process of ICT asset disposal as this is clearly part of the overall battlefield of information security/data protection.

In order to comply with existing legislation and to future proof against changing legislation the following (in my opinion) would be deemed as “Appropriate Technical and Organisations Measures”.

- An approved means of media sanitisation encompassing all media types.
- A policy, which controls the release of these media types within all business activities.
- Internal procedures, which ensure a consistent approach to this activity, across all product sets, departments and locations and which shows adherence to the policy.
- Full asset management throughout the process and verification at each point.
- Third party contracts clearly defining the operator as the data processor and controlling any downstream processing including a strong e-waste strategy.
- Detailed and measurable specification for service delivery.
- Evidence of professional competence of supply chain, including them holding relevant industry standards and certifications.
- Management of the process through a comprehensive audit schedule.
- Reporting on the process with incident reviews, to take place as matter of course.

Of course, the pressure on business IT teams is enormous. These teams are expected to deal with more different technologies than ever before, in environments which are often out of their control. All of this with a smaller budget and fewer resources available. However, by building an intelligent ICT disposal programme along the previously suggested outlines, businesses will not only be able to show compliance with required legislation, but they will also protect their own data from exposure. Furthermore they will be able to maximise the opportunity from old infrastructure through re-deployment, re-sale or donation.

Intelligent policy leads to intelligent processes and intelligent solutions. Without these elements being in place then compliance with the current and future act is clearly not evidenced and the ICT disposal process is one managed by good fortune rather than organisation control. If this is the case for your business then ask yourself, why do we bother locking the data centre door at night, what harm could possibly happen?

References.

[1] Oliver Letwin disposes of parliamentary papers in a public bin. (http://www.bbc.co.uk/news/uk-15301859)

[2] Information Commissioner's Office Website.
(http://ico.org.uk/for_organisations/data_protection/the_guide/the_principles)

[3] Directive on Privacy and Electronic Communications Act.

[4] Phrase coined by Joe Mount, Tabernus "Skin in the Game "article from ADISA Magazine April 2013.
(http://www.adisa.org.uk/wp-content/themes/adisa/Magazine/April2013.pdf)

[5] Staff member steal and sell laptops from Coca Cola.
http://www.cio.com/article/747246/Coca_Cola_Suffers_Data_Breach_After_Employee_Borrows_55_Laptops

[6] Information Commissioner's Office fines The British Pregnancy Advice Service £200,000 for data breach.
http://www.techweekeurope.co.uk/news/anonymous-bpas-receives-200k-ico-fine-141022

[7] Zurich fines £2.3m for loss of back up tapes http://www.out-law.com/page-11333.

[8] Penalty Notices from the Information Commissioner's Office made to Brighton and Sussex University Hospital Fine – £325,000. http://www.adisa.org.uk/wp-content/uploads/2013/09/bsuh_monetary_penalty_notice.pdf and NHS Surrey Fine – £200,000. http://www.adisa.org.uk/wp-content/uploads/2013/09/nhs-surrey-monetary-penalty-notice.pdf

[9] ADISA Magazine September 2012. (http://www.adisa.org.uk/wp-content/uploads/2012/12/ADISA_Magazine_Issue2.pdf)

[10] Information Commissioner's Office fines Ministry of Justice £180,000.
http://ico.org.uk/news/latest_news/2014/repeated-security-failings-lead-to-180000-fine-for-moj-26082014

[11] IRS Data Processor Indemnity Insurance Policy.

Further Reading

National Institute of Standards and Technology: Guidelines for Media Sanitisation 800-88.
http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf

CESG approved products list.
http://www.cesg.gov.uk/finda/Pages/CCITSECResults.aspx?post=1&type=Data+Erasure&status=Certified&sort=name

ADISA ITAD Standard.
http://www.adisa.org.uk/wp-content/uploads/2013/05/ADISA-2013-ITAD-Standard-v1.4.pdf

Information Commissioner's Office – Guidelines for IT Asset Disposal.
http://www.adisa.org.uk/wp-content/uploads/2013/09/ico_presentation_disposal_of_personal_data1.pdf

Training Opportunities

The ADISA certified professional training course is run with the University of South Wales. Download the course brochure here: http://adisa.org.uk/wp-content/uploads/2013/09/ADISA%20Certified%20Professional%20Training%20Brochure.pdf

Disclaimer

Neither the ADISA, nor any of its employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information contained within this document.