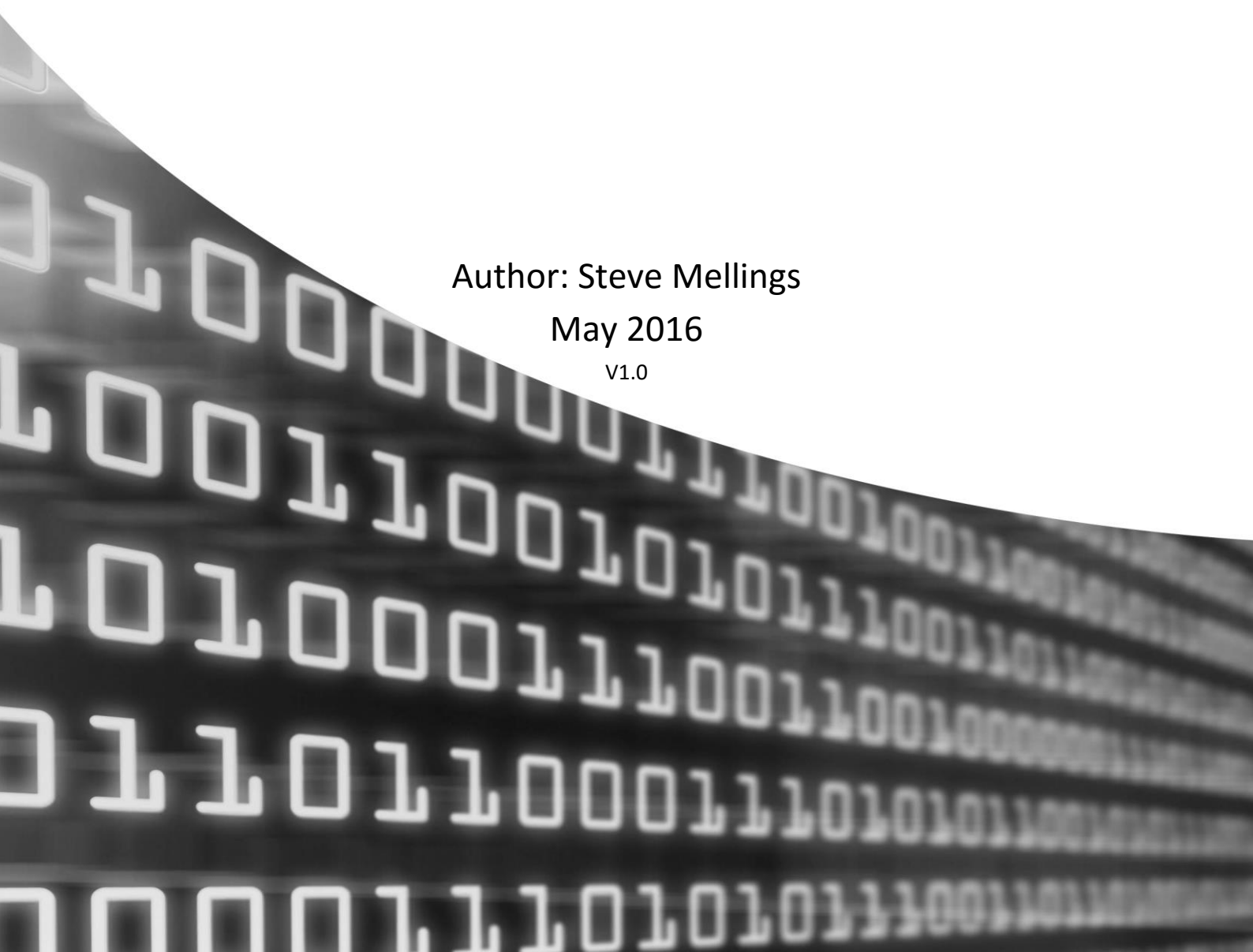
ADISA

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

ADISA WHITE PAPER

An overview of EU Data Protection Regulation 2016 in terms of asset recovery / disposal and how the ADISA Certification Scheme helps its members and their customers meet these new regulatory requirements.



Author: Steve Mellings

May 2016

V1.0

Abstract.

In April 2016 the EU GDPR, was finally agreed in Brussels, it was formally published in the Official Journal on 4 May and became enforceable on 25 May 2016. This piece of legislation is the most significant amendment to European Data Protection or privacy law since the original Directive 95/46/EC was passed in 1995. With many companies already struggling to protect their data, their ability to show compliance to this new regulation is in doubt. Particularly as this new law 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. With two years for each member state to enshrine this into their own national law, organisations are quickly looking to understand where they stand not only from an operational position of protecting data, but moreover, how they would be perceived from a regulatory compliance position.

There is some good news for companies faced with this burgeoning responsibility. The solution for one part of data protection, end of life asset disposal and data sanitisation, is already in place. This paper reviews the law changes in terms of data processing activities and overlays how the existing ADISA Certification programme can help companies meet their regulatory requirements.

The target audience for this paper are organisations who dispose of ICT assets and hold personal information on these assets. Within those organisations the paper should be read by any person in a role with a data protection oversight or in a compliance or relevant operational role.

In addition the paper is targeting ADISA certified members to enable them to see how their certification can help their customers meet their regulatory responsibilities.

Introducing the Business Process

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, 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 few years the UK Information Commissioner has levied fines of over £500,000 for data breached as a result of this process. In the US, a leading drinks manufacturer suffered a significant breach 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.

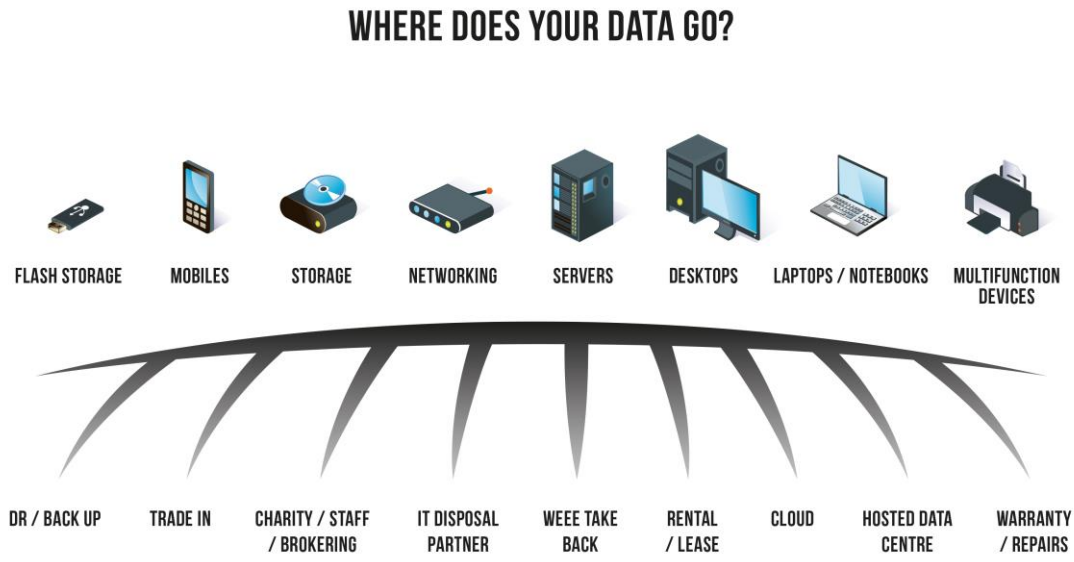


Diagram 1. Sample of business processes and product sets which are included within asset disposal.

Introducing the Business Process (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, bring your own device (BYOD) and the Internet of Things. 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 fine on a UK central government department 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.

EU Data Protection Regulation 2016 Articles Relevant to Asset Disposal

The EU General Data Protection Regulation 2016 was passed into European Union law in May 2016 and with each member state having two years to enshrine it into their own national law, should be taken as the bench mark piece of legislation which organisations need to review when considering data protection.

This legal document is extremely in-depth and includes many core concepts that won't be covered in this paper. What follows is the identification of critical parts of this legal document that apply to organisations who either release assets or those who collect them as part of an end of life asset disposal process. Where possible the requirement has been written verbatim but due to space some have been summarised, but the reference point will enable review against the original document.

Reference Point 81

When using a data processor the data controller should only use processors who;

Requirement	How ADISA Certification meets this
Provide sufficient guarantees, in terms of expert knowledge and ability to deliver the service.	The ADISA Auditing process not only confirms verification that the service provider meets the industry-leading Standard in this area, but also includes a schedule of unannounced spot check audits. This measures continual conformance to the Standard AND via the FREE monitoring service enables data controllers to receive copies of audit documents in a timely fashion. The new ADISA Academy also provides members with a clear training path for their technical and operational staff to ensure they are constantly updated with required knowledge in order to perform their tasks.
Adhere to an approved code of conduct.	In June 2016 ADISA will launch a code of conduct for its members. This will be submitted to the UK Information Commissioners Office for approval.
Adhere to an approved certification mechanism.	The ADISA certification scheme is an established process and the auditing programme is currently working towards UKAS accreditation (ISO 17065) with the intention of achieving this in January 2017.
Operate under the terms of a contract.	Within the ADISA Standard members have to have contracts in place with their customer OR be able to show where their customers refuse and therefore where the member identifies themselves as not accepting data processing responsibilities.

Reference Point 83

Requirement	How ADISA Certification meets this
The controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks.	The ADISA Standard, written in 2010 and recognised by DIPCOG, IS a risk assessment of the entire process. The audit summary reports (ASR) which are produced, highlight where risk to the integrity of the process exists and how each member has managed to mitigate that risk to an acceptable level. These documents are available to members' customers to help them meet this requirement.

Reference Point 84

Requirement	How to comply
The controller should be responsible for carrying out a data protection impact assessment for data processing operations.	Further to point 83, the ASR documents can be used by data controllers as the basis for, or as the document in entirety, for a data protection impact assessment.

Article 28 – Processor

Requirement	How ADISA Certification meets this
The controller shall use only processors who provide sufficient guarantees to implement appropriate technical and organisational measures.	The ADISA Auditing process not only confirms verification that the service provider meets the industry-leading Standard in this area, but also includes a schedule of unannounced spot check audits. This measures continual conformance to the Standard AND via the FREE monitoring service enables data controllers to receive copies of audit documents in a timely fashion. The new ADISA Academy also provides members with a clear training path for their technical and operational staff to ensure they are constantly updated with required knowledge in order to perform their tasks.
The processor shall not engage another processor without prior specific or general written authorisation of the controller.	Within the ADISA Standard the use of downstream data processors is not permitted unless prior screening has taken place by ADISA or in a formal way by the member AND the data controller has authorised this.
The processor shall be governed by a contract.	Criteria 3.1 (a) and (b) within the ADISA Standard covers this.

Requirement	How ADISA Certification meets this
Makes available to the controller all necessary information to demonstrate compliance with obligations laid out in their article and to allow for and contribute to audits, including inspections.	The ADISA Certification scheme us underpinned with an extensive audit process resulting is documented evidence pertaining to the delivery of the data processing service.
The processor shall immediately inform the controller if an instruction infringes this Regulation.	Criteria 3.1(b) requires ADISA members to inform their customers when despite requesting one, they cannot operate under a contract. Criteria 3.1(a) outlines critical elements to be included in the contract to enable the data controller to meet their regulator requirement.

Article 32 – Security of Processing

Requirement	How ADISA Certification meets this
The controller and processor shall implement appropriate technical and organisational measures to ensure a level of security to include a processor for regularly testing, assessing and evaluating the effectiveness of those measures to ensure the security of processing.	The ADISA Auditing process not only confirms verification that the service provider meets the industry-leading Standard in this area, but also includes a schedule of unannounced spot check audits. This measures continual conformance to the Standard AND via the FREE monitoring service enables data controllers to receive copies of audit documents in a timely fashion.

Article 33 – Notification

Requirement	How ADISA Certification meets this
The processor shall notify the controller without undue delay after becoming aware of a personal data breach.	As ADISA members do not know what data they are processing, the intention is to treat the loss of control over an asset that could carry data as being a data breach. In June 2016 ADISA will be launching an Incident Management Service for our members. This will include a notification process for their customers.
The controller shall notify the supervisory authority within 72 hours of becoming aware of it.	The Incident Management Service will also be available for Data Controllers to subscribe to and it will include a supervisory authority notification process.
The notification should include as much information regarding the incident as possible including measures taken or proposed to mitigate its possible adverse effects.	The Incident Management Service includes a structured review process including practical onsite interviews, forensics if required and a root cause analysis.

Article 35 – Data Protection Impact Assessment

Requirement	How ADISA Certification meets this
The controller prior to processing shall carry out a data protection impact assessment for processing likely to result in high risk.	The ADISA ASRs can be used by Data Controllers as a means of pre-screening potential partners as they identify where risk exists and what countermeasures are in place to decrease that risk.
The assessment shall include measures to evaluate risk and what mechanisms have been put in place to mitigate that risk.	

Article 40 – Code of Conduct

Requirement	How ADISA Certification meets this
Associations and other bodies representing categories of processors may prepare a code of conduct and submit it to the supervisory authority for approval.	In June 2016 ADISA will launch a code of conduct for its members. This will be submitted to the UK Information Commissioners Office for approval.

Article 42 and 43 – Certification and Certification Bodies

Requirement	How ADISA Certification meets this
Certification shall be voluntary and via a process which is transparent.	The ADISA published Standard includes in great detail the certification process.
Processors which submit its processing certification shall provide the certification body with all information and access to conduct the certification process.	Within the new code of conduct this will be a requirement, as currently some information provided is not done so to a satisfactory level.
Certification bodies shall be accredited to ISO 17065.	ADISA does not currently hold this but is working towards achieving this and will do so in Jan 2017.
Certification bodies shall be able to demonstration their independence and expertise in relation to the subject matter.	As a result of this requirement and also general dissatisfaction with its operation the ADISA Advisory Council is going to change with the council being operated outside of ADISA. (If it wishes to continue.)
Certification bodies will have established procedures for the issuing, periodic review and withdrawal of data protection certifications.	The ADISA Audit Scheduling, Audit Review and Audit Failure processes meet this.
Certification bodies shall have established procedures to handle compliance and infringements of the certification or the manner in which the processor is operating under certification.	As part of the Incident Management Service any complaint or disclosure made to ADISA about a member by a third party would be classed as an incident and investigated. This will also be covered within the Code of Conduct.

Conclusion

It is widely acknowledged that the current procurement process for ICT asset recovery services is skewed heavily in terms of "price" and many in the industry who provide data processor services bemoan how data controllers currently approach this business process.

As such, despite the EU Data Protection Regulation 2016 being very clear, not only in the few criteria identified above but throughout the 97 articles which data controllers have to comply with, there will be some who will say "so what, we have another law for organisations to ignore".

This fatalistic stance is understandable but it is clear when reviewing the reception to this new law that it is viewed as a sea change in terms of regulation of the data protection efforts of organisations. Not only have the maximum fines (Article 83) increased to €20,000,000 or up to 4% of global turnover but there is also a requirement for mandatory breach notification (Article 33) within 72 hours.

Let us view the EU GDPR definition of data breach:

"'Personal Data Breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

It would seem that unless a data controller is able to show evidence of how they have met the requirements identified above when they select their asset disposal (data processing) partner then any collection made would be classed as breach. At ADISA we estimate that about 85% of all collections made would currently fall into this category due to the lack of a contract, lack of code of conduct and certification and lack of formal risk assessments being made.

The good news for organisations is that our industry, operating as the final part of the data protection process, has been slowly getting our act together. ADISA Certified companies are not perfect, no one ever is, but they are operating to the best published Standard in this sector and more to the point undergo vigorous auditing to ensure compliance. Since January 2016 ADISA has suspended four companies and permanently excluded one. It makes sense for data controllers that when looking to dispose of ICT assets they should seek to engage with one of the ADISA Certified organisations. Not only will they be able to evidence compliance to the relevant parts of the new EU Data Protection Regulation 2016, but they will also know they are dealing with the industry leading companies to whom they can entrust their brand, reputation and liability without undue concern.