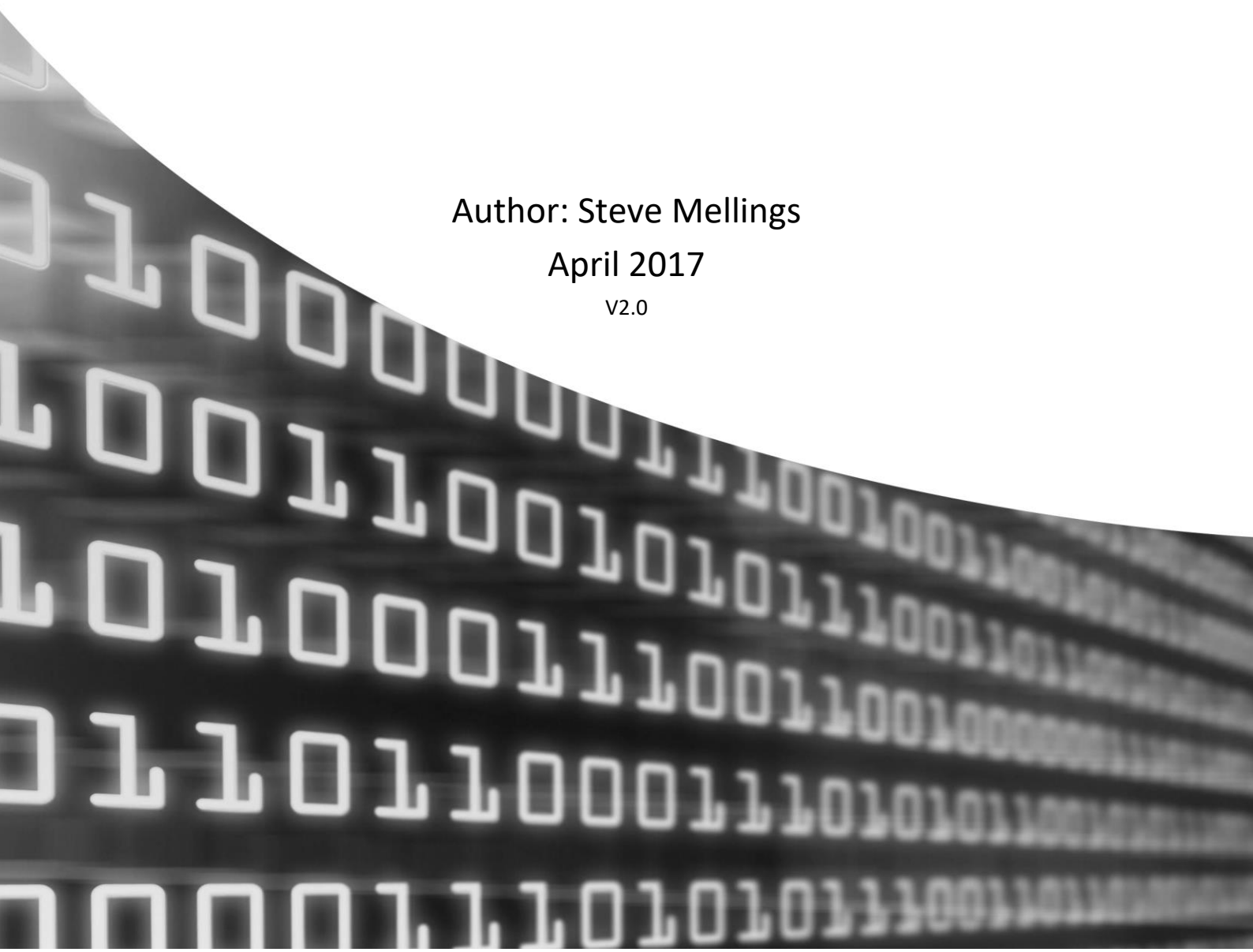
ADISA

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

ADISA WHITE PAPER

The implications of the EU General Data Protection Regulation 2016 for ICT Disposal

(and how ADISA Certification helps data processors and data controllers meet changing regulations)



Author: Steve Mellings

April 2017

V2.0

Abstract on EU GDPR and Brexit

The EU General Data Protection Regulation (GDPR) became law in May 2016, giving member states two years to enshrine it into their own legal frameworks. This is an undertaking the UK will fulfil, despite Brexit. Both Secretary of State Karen Bradley and Information Commissioner Elizabeth Denham have confirmed that it will be unaffected by the Article 50 process.

Whilst the specific details of each country's laws are yet to be determined, it is important that the underlying requirements are understood now so organisations can prepare to implement necessary changes.

This paper explores the impact of GDPR on a particular data processing activity: ICT Asset Disposal and reviews how the ADISA Certification Scheme can help both data processors and controllers meet what is a landmark piece of legislation.

NB: In July 2016, I wrote a white paper on the impact of GDPR on asset disposal and the potential Brexit impact. This paper supersedes that entirely and approaches the subject with the benefit of recent clarity on the matter.

Introduction

The EU General Data Protection Regulation 2016 should be taken as the benchmark piece of legislation organisations need to review when considering data protection.

GDPR has two broad sections. The first contains the recitals which should be viewed as points of reference when considering the second which contains the articles.

These are specific requirements organisations falling under the scope of GDPR need to consider. Not all are relevant to all organisations but where they are relevant they MUST be complied with.

Recital Guidance relevant to Data Processing

Recital 81

Requirement	How ADISA Certification meets this
Data controllers should only use data processors who: 1. 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.* *ADISA has an online Academy which also gives members a clear training path for their technical and operational staff to ensure they constantly have the knowledge they need to be effective.*
2. Adhere to an approved code of conduct	*In July 2016, a voluntary code was approved by ADISA members and has been distributed for them to sign and adhere to.*
3. 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 by May 2018.*
4. Operate under the terms of a contract	*Within the ADISA Standard members MUST have contracts in place with their customers OR be able to show where their customers have refused this and, therefore, where the member identifies themselves as not accepting data processing responsibilities.*

Recital 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	*ADISA Standard, written in 2010 and recognised by DIPCOG, is a risk assessment of the entire process from point of collection to point of data-safe. Audit summary reports (ASRs) are produced, highlighting where risks to the integrity of the process exist and how each member has managed to mitigate them to an acceptable level. These documents are available to members' customers.*

Recital 84

Requirement	How ADISA Certification meets this
The controller should be responsible for carrying out a data protection impact assessment for data processing operations	*The ASR documents can be used by data controllers as the basis for external privacy impact assessments, as the document in its entirety is an assessment of risk to the physical asset and to the processes applied to the media to sanitise it.*

Articles applicable to data processing

The articles within GDPR are requirements which must be met by businesses which qualify.

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 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 to ensure technical and operational staff are constantly updated with essential information.*
The processor shall not engage another processor without prior specific or the general written authorisation of the controller	*Within the ADISA Standard the use of downstream data processors is not permitted unless 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 is 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 relevant industry-leading Standard, but 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. The ADISA Incident Management Service for members includes a notification process for their customers.*
The controller shall notify the supervisory authority within 72 hours of becoming aware of it	*Data Controllers will be able to subscribe to The Incident Management Service 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 on-site 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 areas of risk 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 July 2016, a voluntary code of conduct was approved by ADISA members and has been circulated for them to sign and adhere to.*

Article 42 and 43 – Certification and Certification Bodies

Requirement	How ADISA Certification meets this
Certification shall be voluntary and via a transparent process	*The ADISA published Standard includes in great detail the certification process.*
Processors which submit 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 some information provided is not currently at a satisfactory level.*
Certification bodies shall be accredited to ISO 17065	*ADISA does not currently hold this but is working towards achieving it and will do so in Jan 2018.*
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 ADISA. (If it wishes to continue.)*
Certification bodies will have established procedures for the issuing, periodic review, and withdrawal of data protection certification.	*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, to the annoyance of many in the industry, skewed heavily in terms of "price".

What is also known is that 66 per cent of the public sector currently breaks UK Data Protection law when disposing of ICT assets, something borne out by an ADISA poll of more than 400 respondents.

This suggests that; even though GDPR is very clear, not only in the criteria identified here but throughout the whole document, data controllers have a long way to go to demonstrate compliance when disposing of assets.

There will doubtless still be some who will say: "So what . . . we have another law for organisations to ignore." But the more informed will see it as something of a sea-change in terms regulating the data protection efforts of organisations.

Not only have the maximum fines (Article 83) increased to €20,000,000 or up to four per cent of global turnover, but there is a requirement for a mandatory breach notification (Article 33) within 72 hours. Mandatory notification is something already in place in many US states so 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."

ADISA's position is that, unless a data controller is able to show they have engaged with data processing in a manner seen as complying with the EU GDPR, then the transaction would be viewed as unlawful, and therefore classed as breach.

At ADISA we estimate that about 85 per cent of all collections made would currently fall into this category due to lack of either contracts in place, a code of conduct and certification or formal risk assessments. So is the future of asset disposal one in which most collections are classed as data breach and require either party to disclose to the relevant data regulator? It certainly looks that way.

The good news for organisations is that our industry, operating as the final part of the data protection process, has been slowly getting its act together. ADISA-certified companies operate to a rigorous published Standard, and more to the point, undergo continuous auditing to ensure compliance.

The Standard was revised in 2015 in preparation for GDPR and our members will be working hard to ensure they are one group which operates within the law and helps their customers comply. Since January 2016 ADISA has suspended four companies and permanently excluded one. It makes sense for data controllers looking to dispose of ICT assets that they should engage an ADISA-certified organisation. Not only will they be able to show compliance with the relevant parts of the new

regulation, but they will know they are dealing with industry-leading companies to whom they can entrust their brand, reputation and liability without undue concern.

www.adisa.global

+44 845 557 7726

info@adisa.global