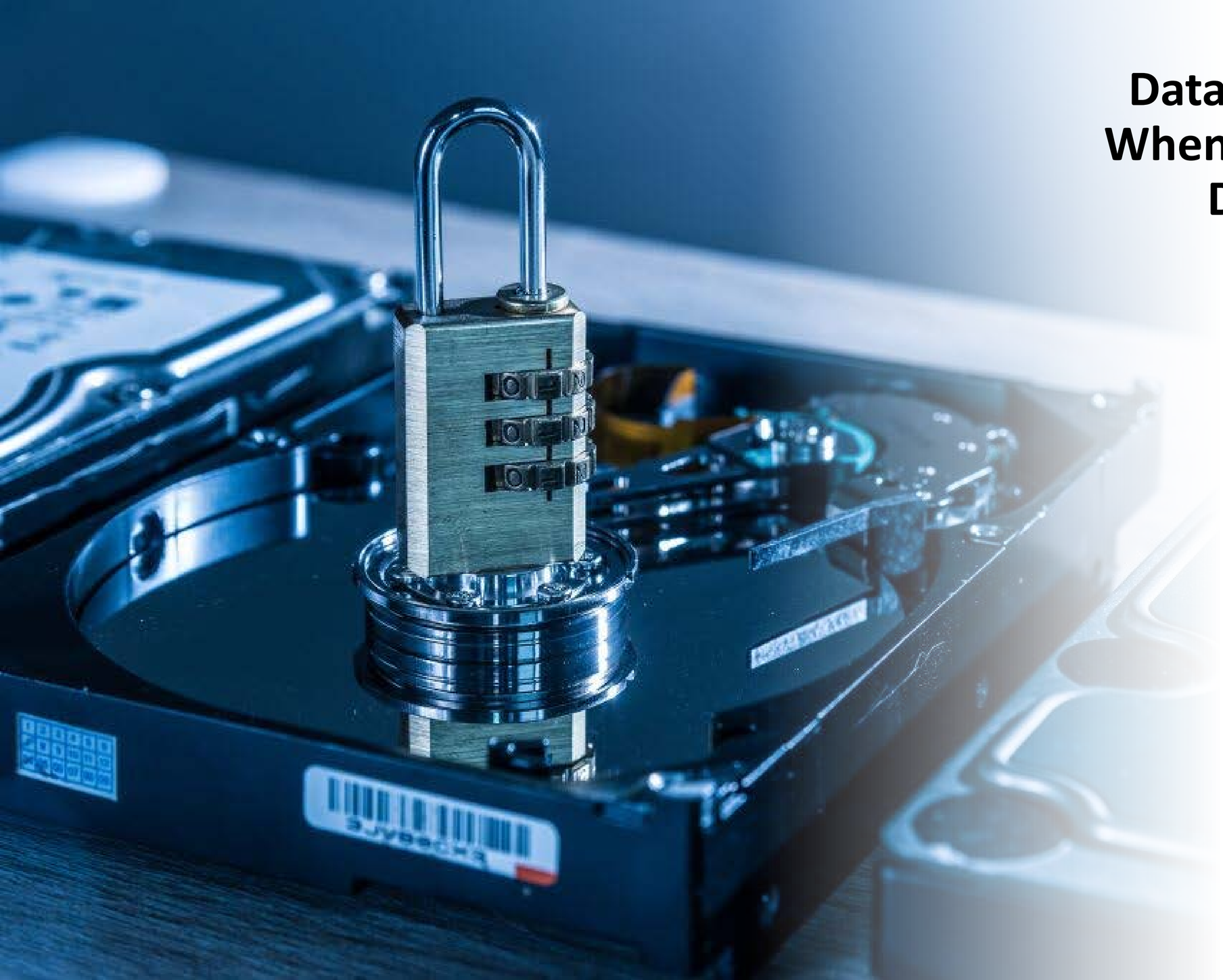


Data Protection Compliance When Recovering Redundant Data Bearing Electronics

Steve Mellings
Founder of ADISA
A UK GDPR Certification Scheme

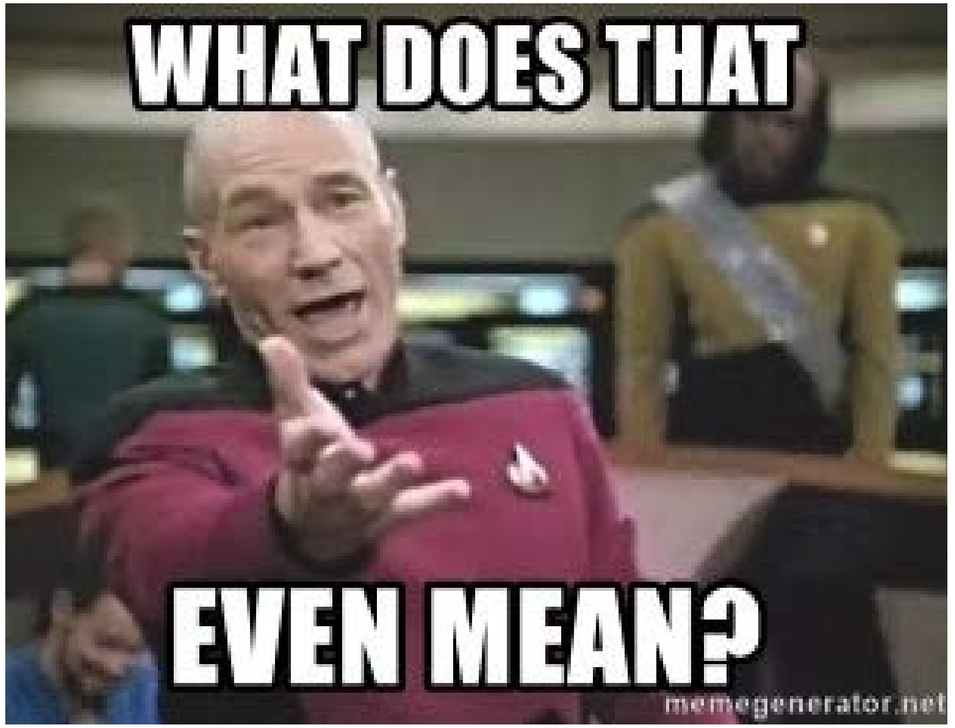
The Data Protection landscape
EU and UK GDPR – Article 4 Definitions

‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, **erasure or destruction**.

EU and UK GDPR – The Data Protection landscape
Article 4 the GDPR: Definitions

If you provide data sanitisation services or hardware destruction services, you are a Data Processor under the eyes of the law.



EU and UK GDPR – The Data Protection landscape
Article 4 the GDPR: Definitions

If you provide data sanitisation services or hardware destruction services, you are a Data Processor under the eyes of the law.

Examples of what it doesn't mean:

"A GDPR compliant data wipe".

"Erase data or destroy hard drives as per GDPR".

"Certified data erasure".

Compliance (sadly) means much more than the act of data sanitisation
We'll explore 2 articles

Article 28 Processor

Requirement	
Article 28 (1)	The controller shall use only processors who provide sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of this regulation.
Article 28 (2)	The processor shall not engage another processor without prior specific or the general written authorisation of the controller
Article 28 (3)	The processor shall be governed by a contract (MOST IMPORTANT PIECE TODAY TO REMEMBER)
Article 28 (3) h	Makes available to the controller all necessary information to demonstrate compliance with obligations laid out in this article and to allow for and contribute to audits, including inspections
Article 28 (3)	The processor shall immediately inform the controller if an instruction infringes this regulation
Article 28 (5)	Processor may comply with an approved code of conduct as a means of providing sufficient guarantees

Article 32 Security of Processing

Requirement	
Article 32 (1) d	The controller and processor shall implement appropriate technical and organisational measures to ensure a level of security to include a process for regularly testing, assessing and evaluating the effectiveness of those measures to ensure the security of processing
Article 32 (2)	In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing…….

Let’s explore appropriate….

Requirement	
Article 32 (1) d	The controller and processor shall implement appropriate technical and organisational measures to ensure a level of security to include a process for regularly testing, assessing and evaluating the effectiveness of those measures to ensure the security of processing

Who determines what is appropriate?

~~**ADISA**~~ ~~**Industry**~~

RISK OWNER

In the eyes of the law the risk owner is responsible for determining the risk treatment which will be based on principles which vary from one company to another

Current issue of compliance…..

- Controller MUST evidence “Appropriate Technical and Operational Measures”.
- What is deemed “appropriate” depends on the controller’s own determining factors.
- Asset Recovery has many high-risk processes with different levels of controls to mitigate those risks.

At the moment……the industry is making those decisions

THE TAIL IS WAGGING THE DOG!

ADISA's journey to becoming a UK GDPR Certification Scheme

- 2 years to get Standard 8.0 ICO approved.
- 1 year to get UKAS Accreditation for the audit process.
    - 7 separate audits.

This means ADISA Asset Recovery Standard 8.0 meets both Article 42 and Article 43 of the UK GDPR.

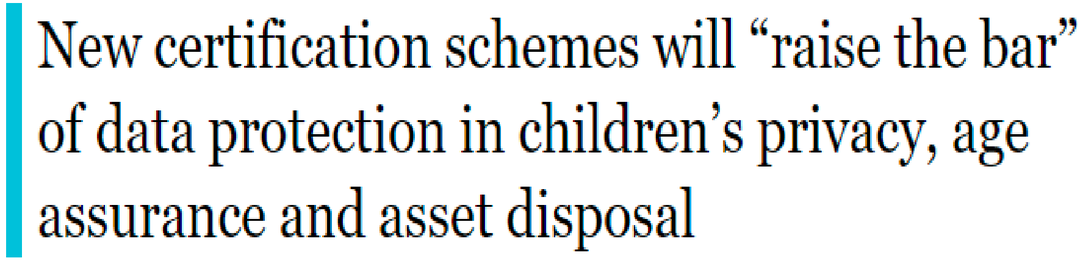
ADISA ICT Asset Recovery Certification 8.0

Approval date 19 July 2021

ADISA Asset Recovery Standard is a standard for processors or sub-processors providing data sanitisation services. This is where information is permanently removed from IT hardware such as computer hard drives or photocopiers so they can be securely disposed of or reused. The standard sets data protection requirements for the organisations performing these services. Certification is issued against this standard.

Scheme criteria

- **ICO-CSC/003** ADISA ICT Asset Recovery Standard 8.0 v3.0 Part 1: Introduction and Explanation Notes
- **ICO-CSC/004** ADISA ICT Asset Recovery Standard 8.0 v3.0 Part 2: Criteria

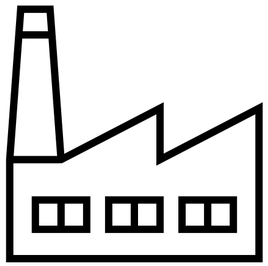


New certification schemes will "raise the bar" of data protection in children's privacy, age assurance and asset disposal

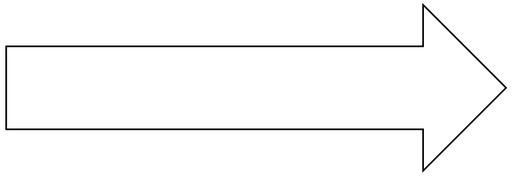
The Current Compliance position

Data Protection Law

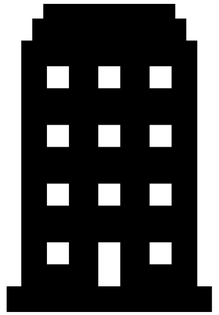
Industry



Industry Certifications



Customers

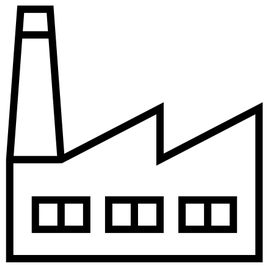


ISO Standards

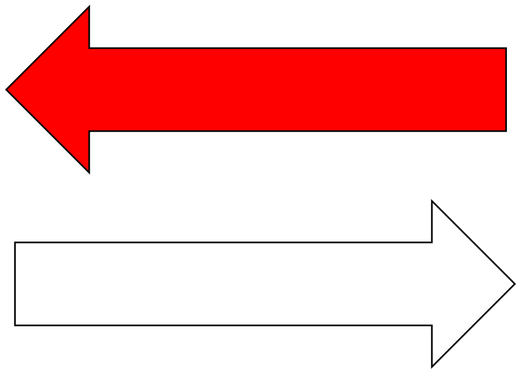
The Current Compliance position

Data Protection Law

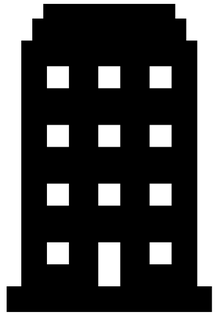
Industry



ADISA Standard 8.0



Customers



Data Impact Assurance Levels

5 metrics to determine the service you need to be provided.

- Threat.
- Risk Appetite.
- Category of Data.
- Volume of Data.

- Finally, assess the impact of a data breach.

Threat Level	Threat Actor and Compromise Methods
Low	Casual or opportunistic threat actor only able to mount unsophisticated attacks.
Medium	Motivated, targeted threat actor such as organised crime or journalists or hackers applying professional methods to access the physical device and / or data.
High	Government-sponsored organisations using sophisticated techniques with unlimited time and resources to access the physical device and / or data.

Threat	**High**	**3**	**4**	**5**
	Medium	**2**	**3**	**4**
	Low	**1**	**2**	**3**
		High	**Medium**	**Low**
	Risk Appetite			

Compliance is too confusing…..
The good news…..

Over 40 companies are already certified to 8.0 showing that GDPR compliance is achievable and commercially viable.

ADISA's responsibility is to liaise with the regulators to map out what compliance looks like – you don't need to!

Standard 8.0 is VERY similar to previous ADISA Standards. This is evolution rather than revolution.

edpb
European Data Protection Board

ADISA is already working with the Irish Data Commission to get Standard 8.0 (EU) approved.

ADISA®

Thank you

Come and meet with us on Booth 314

info@adisa.global
www.adisa.global