GDPR Readiness Roadmap.

HIS Conference Ballymascanlon House, Dundalk 12th October 2017

Assess Readiness

Workshop and questionnaire to determine compliance readiness with GDPR requirements

Data Inventory

Discovery and mapping of data flows. Data Processing.

Gap Analysis

In-depth Gap analysis and remediation planning.

Risk Assessment

Security Risk Assessment, DPIA, and testing of technical and organisational measures

Data Protection Programme

Implement programme and Information Management System

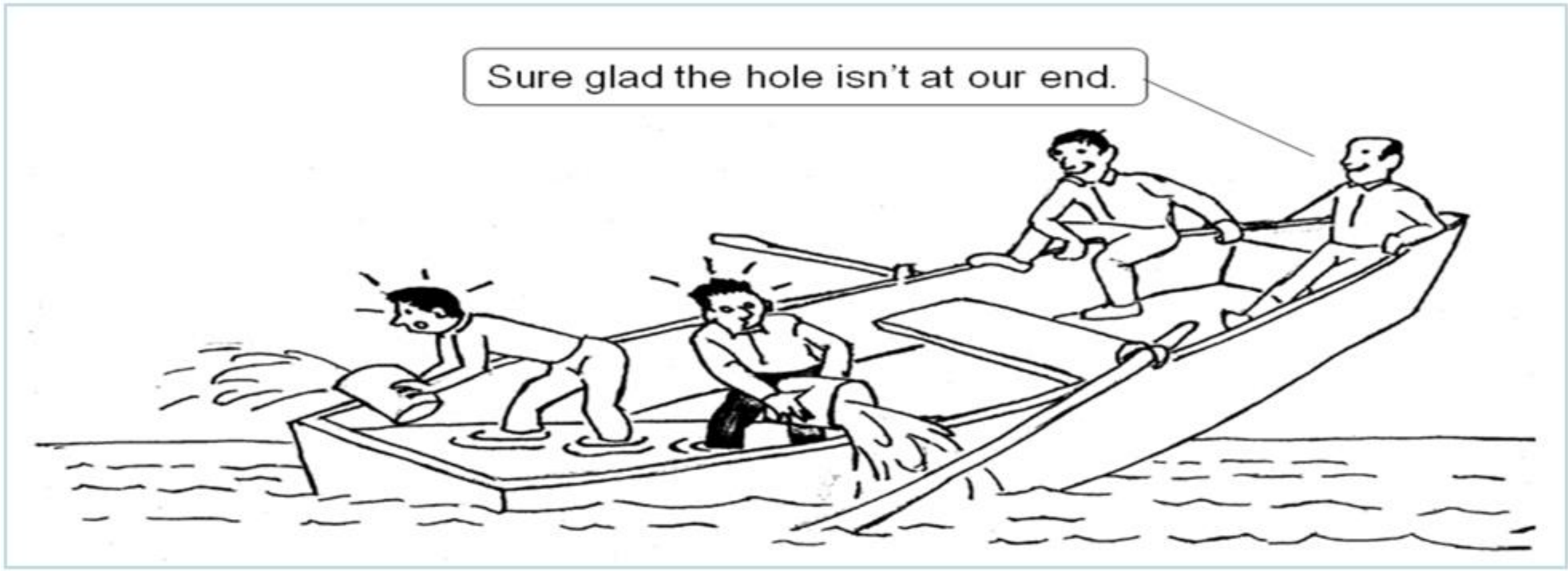
Aisling Hennessy
Head of Legal and Compliance

WardSolutions
Assess | Protect | Detect | Respond

Disclaimer: This presentation does not represent legal advice or purport to be a legal interpretation of legislation, regulation or standard rules. Whilst every effort is made to ensure the information is accurate, responsibility cannot be accepted for any liability incurred or loss suffered as a consequence of relying on any material published herein. Appropriate professional advice should be taken before acting or refraining to act on the basis of this presentation.

WardSolutions
Assess | Protect | Detect | Respond

Collective Responsibility and Accountability



WardSolutions
Assess | Protect | Detect | Respond

Core Principals (Chapter II art.5-11)

Lawful, fair and transparent	specified, explicit and legitimate purposes	adequate, relevant and limited	accurate and, where necessary, kept up to date;	no longer than is necessary for
Article 5(1) (a)	Article 5(1) (b)	Article *5(1) (c)*	Article 5(1) (d)	Article *5(1) (e)*

"..processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')…"

Article 5(1) (f)

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 5(2)

Data Subject Rights (Chapter III art.12-23)

Know the purpose for processing

Article 13

Right of access by the data subject

Article 15

Right to rectification

Article 16

Right to erasure

Article 17

… restriction of processing ..

Article 18

Right to data portability

Article 20

Right to object

Article 21

not subject to decision solely on automated processing

Article 22

Within 1 month
Cannot Charge

Article 12

WardSolutions
Assess | Protect | Detect | Respond

Data Controllers / Processors (Chapter IV art.24-43)

Responsibility of the controller Article 24	Data protection by design and by default Article 25	Processors Article 28	Records of processing activities Article 30	Security of processing Article 32
Notification of a personal data breach Article 33	Communication of a personal data breach Article 34	Data protection impact assessment. Article 35	Designation of the data protection officer Article 37/38/39	

WardSolutions
Assess | Protect | Detect | Respond

DPO

- Public Authorities will require one.
- Group of undertakings can have one between them.
- Can outsource or have in-house.
- Professional qualities – expert knowledge and be able to carry out the tasks.
- Report to highest level of management.
- No conflict

WardSolutions
Assess | Protect | Detect | Respond

DPO

- What will they do?
  - Inform and advise.
  - Monitor compliance.
  - Provide advice when required.
  - Contact point for data subjects and supervisory authority.
  - Need to be involved in proper and timely manner.

WardSolutions
Assess | Protect | Detect | Respond

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Article 32 Security of Personal Data

WardSolutions
Assess | Protect | Detect | Respond

Information Security

State of the art

Costs of implementation

Nature, scope, context and purposes of processing

V

risk of varying likelihood and severity for the rights and freedoms of natural persons

=

appropriate technical and organisational measures to ensure a level of security appropriate to the risk

This is a risk assessment, but impact focussed on the data subject NOT the company.

WardSolutions
Assess | Protect | Detect | Respond

GDPR Readiness Roadmap

Assess Readiness

Workshop and questionnaire to determine compliance readiness with GDPR requirements

Data Inventory

Discovery and mapping of data flows. Data Processing.

Gap Analysis

In-depth Gap analysis and remediation planning.

Risk Assessment

Security Risk Assessment, DPIA, and testing of technical and organisational measures

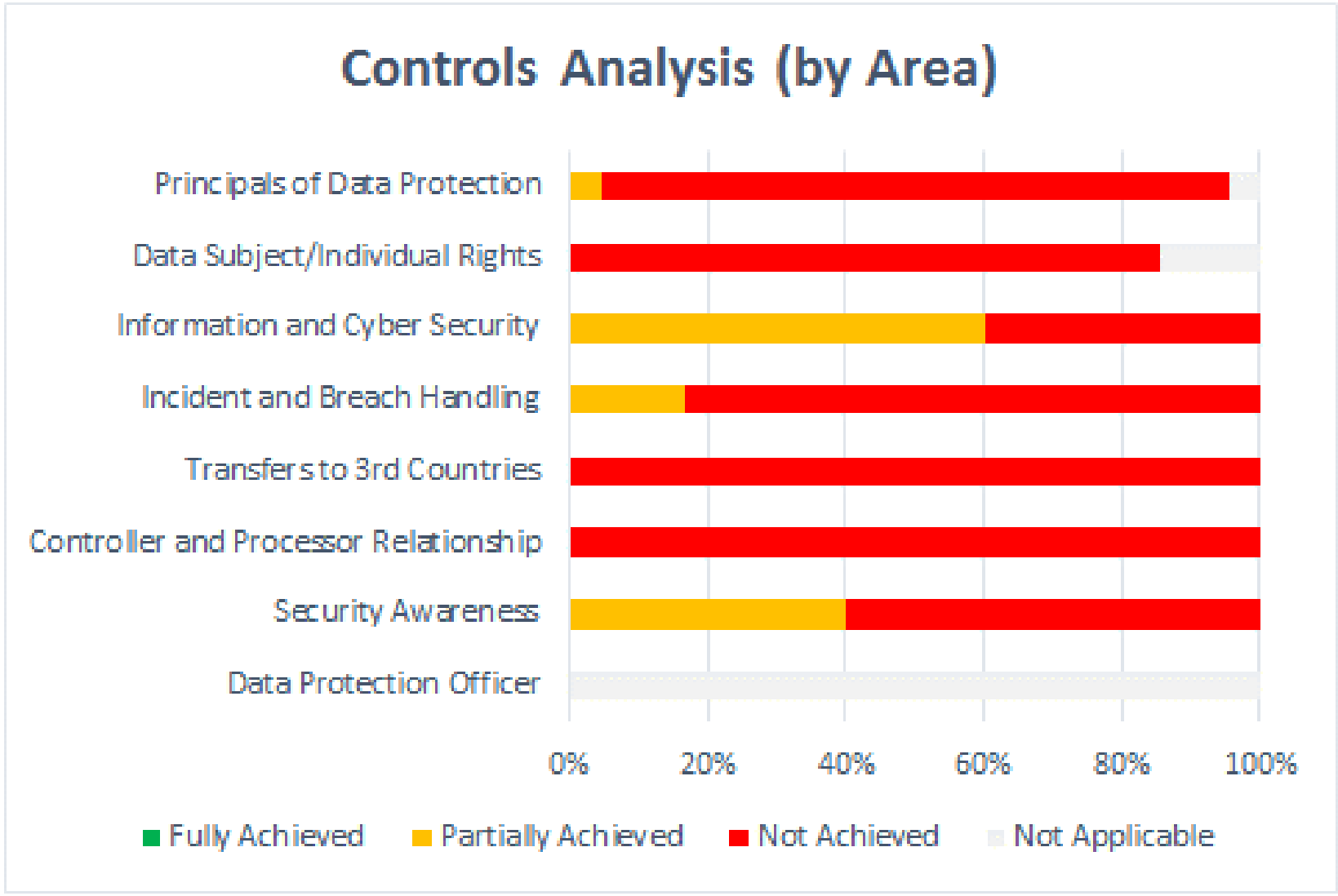
Data Protection Programme

Implement programme and Information Management System

WardSolutions

Assess | Protect | Detect | Respond

Snapshot of GDPR Readiness



WardSolutions
Assess | Protect | Detect | Respond

GDPR Readiness I

Data Inventory

Discovery and mapping of data flows. Data Processing.

1. Identify personal data.
2. Identify where personal data resides and where/how its processed.
3. Map data flows internally and externally
4. Sharing - Include 3rd party
5. Be aware of geographical considerations.

Comprehensive Data Inventory and mapping

WardSolutions
Assess | Protect | Detect | Respond

GDPR Readiness II

Gap Analysis

In-depth Gap analysis and remediation planning.

1. Processing as per core principles, capture legal reason for processing.
2. Can you deliver data subject rights.
3. Do you have the necessary governance structure in place.
4. Can you meet your controller/processor obligations

Identify the GDPR impact and plan technical and organisational measures.

WardSolutions
Assess | Protect | Detect | Respond

GDPR Readiness III

Risk Assessment

Security Risk Assessment, DPIA, and testing of technical and organisational measures.

1. Conduct GDPR risk assessments (privacy / governance/ people/ processes/data information security).
2. Categorise based on risk.
3. Develop GDPR programme.

Prioritised risk assessment and programme

WardSolutions
Assess | Protect | Detect | Respond

GDPR Readiness IV

Data Protection Programme

Implement programme and Information Management System

1. Programme that develops privacy framework to improve posture and compliance with GDPR.
   a) Transform, Operate and Conform
2. Revisit Policy and Procedures
   a) Data protection Policy / Data Privacy Notice / Data Retention Policies / Process for Data subjects Rights / IR Procedures / Information security policies and procedure.
3. Accountability: Records/Compliance portal
   a) Records of processing
4. Information Security Controls.
5. Training

WardSolutions
Assess | Protect | Detect | Respond

Learnings from programmes undertaken

1. Data Mapping needs tools.
    a) Structured and unstructured data and migration from unstructured.
    b) Capture data related to core principles.
    c) Shadow IT and cloud usage
2. Identifying lawful grounds for processing
3. Data Retention/minimisation and subsequent deletion.
4. Not a culture of 'Breach Notification'
5. Accountability - Records of processing not done.
6. Data subjects rights difficult to address (SAR) – IT systems capabilities
7. Relationships/contracts with 3rd party processors.
8. Focus on compliance NOT security/privacy.
9. Need to write or re-write policies.
10. Requirement for a DPO

WardSolutions
Assess | Protect | Detect | Respond