

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

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.

Collective Responsibility and Accountability

Illustration showing a boat with a hole in the bottom. One person is pointing to the hole and saying "Sure glad the hole isn't at our end." This illustrates the concept of collective responsibility where individuals focus on their own safety rather than the overall risk to the group.

Core Principals (Chapter II art.5-11)

Lawful, fair and transparent Article 6(1) (a)	specified, explicit and legitimate purposes Article 6(1) (b)	adequate, relevant and limited Article 6(1) (c)	accurate and, where necessary, kept up to date. Article 6(1) (d)	no longer than is necessary for Article 6(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")."

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	

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	

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

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.

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:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- 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

Information Security

State of the art	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
Costs of implementation				
Nature, scope, context and purposes of processing				

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

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

Snapshot of GDPR Readiness

Controls Analysis (by Area)

Area	Fully Achieved	Partially Achieved	Not Achieved	Not Applicable
Principles of Data Protection	100%	0%	0%	0%
Data Subject/Individual Rights	80%	10%	10%	0%
Information and Cyber Security	60%	30%	10%	0%
Incident and Breach Handling	20%	10%	70%	0%
Transfers to 3rd Countries	100%	0%	0%	0%
Controller and Processor Relationship	100%	0%	0%	0%
Security Awareness	40%	10%	50%	0%
Data Protection Officer	0%	0%	100%	0%

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

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.

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

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.
 - Transform, Operate and Conform
2. Revisit Policy and Procedures
 - 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
 - Records of processing
4. Information Security Controls.
5. Training

Learnings from programmes undertaken

1. Data Mapping needs tools.
 - Structured and unstructured data and migration from unstructured.
 - Capture data related to core principles.
 - 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