

The new cyber order

*Understanding NIS2, the CRA and
Europe's digital sovereignty agenda.*

Wi-Fi name: **Public**

Password: **mhcpublic**

Please note that photographs will be taken

Welcome address



Julie Austin

Partner, Data & Technology
Mason Hayes & Curran

LAW	OBJECTIVE	APPLIES TO	STATUS	KEY OBLIGATIONS/CORE FEATURES	
GDPR	Protection of personal data	Controllers Processors	In force	- Key principles: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, accountability - Data breach reporting: risk (regulator) and high risk (data subjects)	- Reporting timeframe: 72 hours - Reporting route: Data protection authorities (single entry point proposed by the Digital Omnibus) - One stop shop: yes
NIS2	Resilience of critical services - security of network and information systems	Important entities Essential entities	Transposition date 17 October 2024. Ireland has not yet transposed	- Cybersecurity risk management measures (e.g. policies on risk analysis and information system security, incident handling, supply chain security, business continuity, human resources security) - Governance - Incident reporting: significant incidents & cyber threats	- Reporting timeframe: 24 hours - Reporting route: Relevant competent authority (single entry point proposed by the Digital Omnibus) - One stop shop: only for the digital sector
CRA	Resilience of products with digital elements (e.g. apps, and their remote data processing solutions)	Manufacturers Importers Distributors	Vulnerability reporting: 11 September 2026 Other obligations: 11 December 2027	- Security by design - Vulnerability handling requirements - Conformity assessments & CE markings - User communication & transparency	- Incident Reporting: actively exploited vulnerabilities and severe incidents - Reporting timeframe: 24 hours - Reporting route: CSIRT (single reporting platform) - One stop shop: incident reporting only
CSA2	Resilience of ICT supply chains	N/A	Not in force - at proposal stage	- ICT supply chain security: enables EC to designate high-risk suppliers (HRS) and high risk third countries & prohibit use of HRS in key ICT assets - Extend scope of the European Cybersecurity Certification Scheme to allow for certification of overall cybersecurity posture, not limited to ICT products, services and MSPs.	- Stringent requirements for electronic communication networks inc. phase out of HRS from key network assets - Reforms ENISA's role - Targeted amendments to NIS2
CADA	Resilience of the EU	Cloud, AI, and data center infrastructure operators in the EU. Primarily aimed at the public sector	Target date for adoption Q4 2027	- To address EU digital autonomy, foreign data access laws and perceived broader privacy and cybersecurity risks 4-tier union level assurance framework for cloud service providers relating to the processing, storage and control of data - strict criteria	- Data centre acceleration zones - Cloud and AI leadership initiatives - Regional experience and acceleration centres for AI

AGENDA

THE Digital Regulatory SERIES

6:40pm

Panel 1

Policy, supervision and enforcement in focus followed by audience Q&A

7:15pm

Panel 2

Where regulation meets reality, real world implementation and overcoming challenges followed by audience Q&A

8:00pm

Closing remarks – Oisín Tobin

8:00pm – 8:30pm

Drinks reception

PANEL ONE

THE
Digital Regulatory
SERIES

Policy, supervision and enforcement in focus



Dr Marnix Dekker
*Deputy Head of Unit,
Resilience of Critical Sectors,
ENISA*



Valéry Vander Geeten
*Head of Legal,
Centre for Cybersecurity Belgium (CCB)*

PANEL MODERATOR



Helen Dixon
*Global Digital Regulatory Consultant,
Mason Hayes & Curran*



Audience Q&A

Wi-Fi name: **Public**
Password: **mhcpublic**

PANEL
TWO

Where regulation meets reality, real world implementation and overcoming challenges

THE
Digital Regulatory
SERIES



Alice O'Malley

*Group Cyber Strategy and
Governance Manager,
EirGrid*



Dylan Gannon

*Associate General Counsel
for Cybersecurity & AI,
Meta*



**Francisco Alves
de Matos**

*Compliance Director,
Legora*



Jevan Neilan

*Partner, Data & Technology
Mason Hayes & Curran*

PANEL MODERATOR



Ciara O'Rourke

*Associate,
Data & Technology,
Mason Hayes & Curran*



Audience Q&A

Wi-Fi name: **Public**
Password: **mhcpublic**

Closing remarks



Oisín Tobin

Partner, Data & Technology
Mason Hayes & Curran

The new cyber order

*Understanding NIS2, the CRA and
Europe's digital sovereignty agenda.*

Thank you