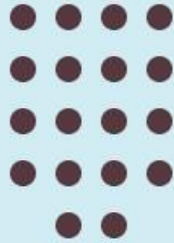


We are starting shortly, please take a seat!



WEBINAR

Demystifying NIS2: A Clear Path to Compliance

Tuesday 7th May 2024 | 12:00 to 13:00 PM GMT

In Partnership with



Lanre Oluwatona PMP, FIP

Data Protection Consultant

ICS Skills



Nollag Conneely

Head of Consultancy
PrivacyEngine



The NIS2 Directive (NIS2)

A breakdown of the network information security directive for critical or essential entities



PRIVACYENGINE



Structure

- **Background**
 - Objectives
 - Timelines
 - Irish approach
- **NIS2**
 - Scope
 - Personal liability
 - Audits
- **Implementation**
 - Policies
 - Framework
 - Training
 - Enforcement



PRIVACYENGINE



Aim of the Directive

The aim of the Directive is to:

- a) **build harmonised** cybersecurity capabilities across the Union;
- b) **mitigate threats** to network and information systems used to provide essential services in key sectors;
- c) **guarantee continuity** of such services when facing incidents;
- d) **expand the scope and statutory provisions** of the first NIS Directive.



PRIVACYENGINE



NIS2 What & When?

- Cybersecurity and privacy are becoming more symbiotic
- NIS2 entered into force on 16 January 2023
 - Member States now have until 17 October 2024 to transpose provisions into national law.
 - 5+ Months before the law takes effect.
 - Current NIS legislation in Ireland (EU Measures for a High Common Level Of Security Of Network And Information Systems Regulations 2018)
- Builds on provisions of NIS1 – Directive 2016/1148
- It also reinforces GDPR provisions
 - Personal data is mentioned 10 times under NIS, 28 times under NIS2.
 - Data Protection is not going away; it's only getting more forceful and exhaustive.



PRIVACYENGINE



Poll 1 What Entity are you?




















- Essential
- Important
- Don't know

















PRIVACYENGINE



Essential business sectors

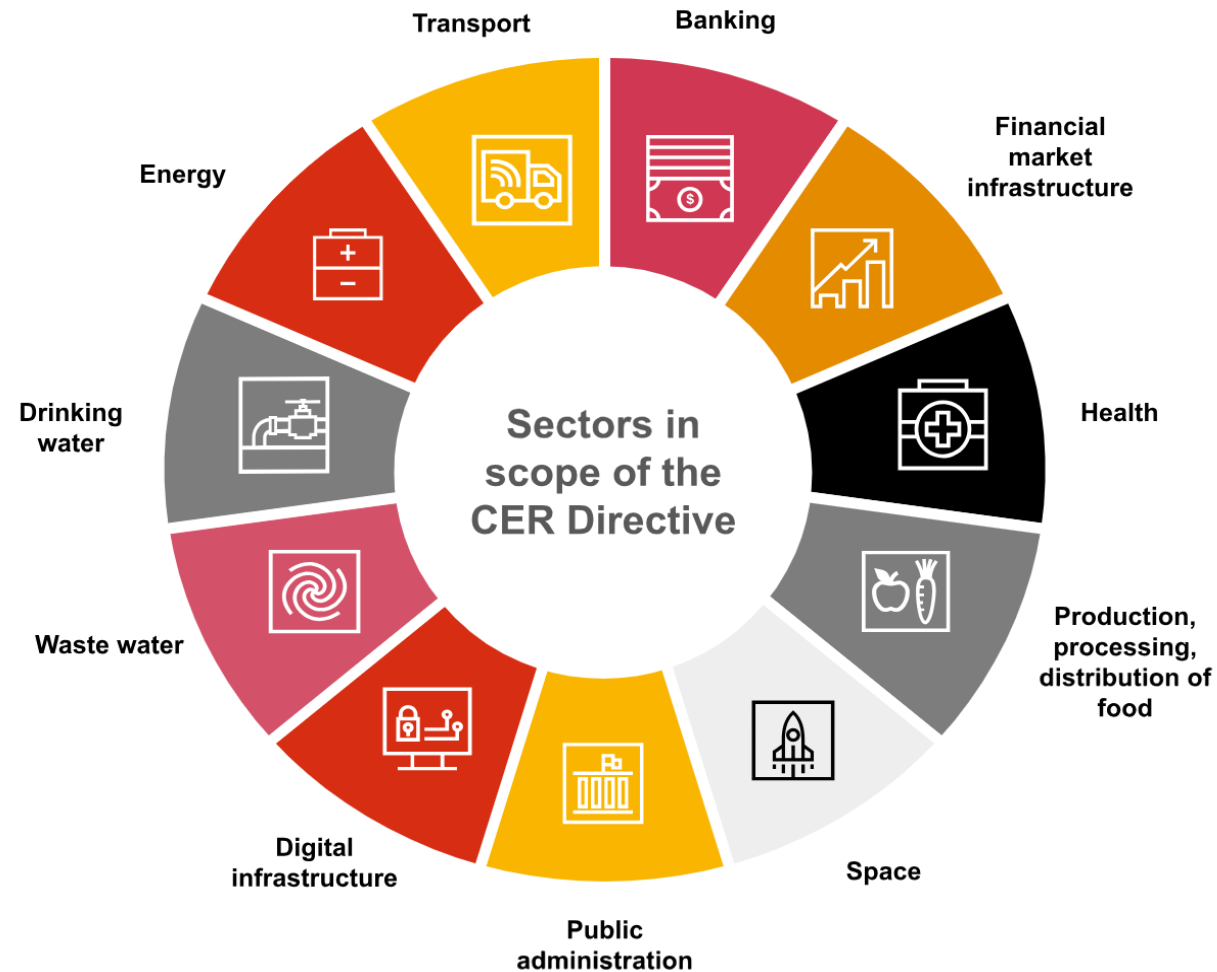
Energy  Electricity  Gas  Oil  Hydrogen  District heating and cooling					Transport  Air  Rail  Water  Road				Health  Healthcare providers  Pharmaceutical industry		Space 
Drinking water 	Waste water 	Public administration 	Digital infrastructure 	Banking 	Financial market infrastructures 	ICT service management (B-to-B) 					

Important business sectors

Postal and courier services 	Waste management 	Digital providers  Online marketplaces  Online search engines  Social networking services platforms			Chemicals  Manufacture, production and distribution	Food  Production, processing and distribution	Research 
Manufacturing  Manufacture of medical devices and <i>in vitro</i> diagnostic medical devices  Manufacture of computer, electronic and optical products  Manufacture of electrical equipment  Manufacture of machinery and equipment n.e.c.  Manufacture of motor vehicles, trailers and semi-trailers  Manufacture of other transport equipment							

 Sectors added by NIS 2 directive

Critical Entities Resilience Directive (CERD)



Defining entities under the directive

Essential Company

- ≥ 250 employees or more than 50 million in revenue (Large Entity)
- Operates in Annex I of Sectors with High Criticality
- It can include medium and small-micro companies in certain sectors

Important Company

- 249-50 employees or more than 10 million in revenue (Medium Entity)
- Operate in Annex 1 and Annex 2, which can be broken down into various sectors
- It can include large and small-micro companies in certain sectors

Note: Determining whether an entity is essential or important within the meaning of the Directive will be done on a case-by-case basis, with probable guidance from the NCSC.

Poll 2 What did you become aware of NIS2?

- Webinar
- <6 months
- 6-12 months
- >12 months

Poll 3 What sector are you?

- Energy
- Finance
- ICT (B2B)
- Transport
- Banking
- Health
- Drinking Water
- Wastewater
- Digital Infrastructure
- Public Service Providers
- Public Administration
- Space



PRIVACYENGINE



Critical Entities Resilience Directive (CERD)

- The CER Directive acknowledges that the types of threats and hazards we face are more diverse, frequent and complex than ever before
- Article 6: Identification of Critical Entities
 - Organizations likely to be deemed a ‘critical entity’ should consider now what the deadline and milestones will mean for them and take action proactively to anticipate the requirements
- Article 13: Resilience measures of Critical Entities:
 - Member States must ensure that Critical Entities implement appropriate measures contained in a resilience plan or equivalent document to prevent incidents from occurring, ensure adequate protection of critical infrastructure, address the impact of and recovery from incidents, and guarantee adequate employment security management. Critical Entities will need to formulate initiatives to meet new resilience mandates
- Article 15: Incident Notification:
 - Within 24 hours of detecting an incident that disrupts or could disrupt the provision of essential services, the Critical Entity will be required to give an initial notification to the competent authority

Resilience!!

- What is Resilience?
 - Cyber resilience refers to an entity's ability to continuously deliver the intended outcome, despite cyber attacks. Resilience to cyber attacks is essential to IT systems, critical infrastructure, business processes, organisations, societies, and nation-states.
- Digital Operational Resilience Act (DORA)
 - Financial Services
- Draft Regulatory Technical Standards (RTS) 17th July 2024
 - Date of application 17th Jan 2025
- European Systemic Cyber Incident Coordination Framework (EU-SCICF)
 - DORA, NIS2, CERD, CSIRT

Irish Approach?

- By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this NIS2. They shall immediately inform the Commission thereof.
 - Dept of Environment, Climate and Communication
- They shall apply those measures from 18 October 2024.
- National Competent Authorities not yet defined, but along current lines
 - Digital Service Providers (DSPs)
 - NCSC
 - Operators of Essential Services (OESs)
 - e.g. Commission for Regulation of Utilities (CRU), Central Bank
- Joint Investigations
- Information sharing
- NIS2 and CERD combined into regulation
 - This may bring forward CERD

NIS2 Directive

- Scope
- Personal liability
- Articles
- NIS2 Implementation

Personal Liability

- *“In an attempt to lower the pressure put on IT departments to single-handedly ensure the security of the organization and to change the sentiment of whose responsibility cybersecurity is, NIS2 includes new measures to hold top management personally liable and responsible for gross negligence in the event of a security incident”*
- Specifically, NIS2 allows Member State authorities to hold organisation managers personally liable if gross negligence is proven after a cyber incident. Failure by management to comply with NIS2 requirements could result in serious consequences, including liability, temporary bans and administrative fines as provided for in the implementing national legislation.
- Management must:
 - Approve the adequacy of the cybersecurity risk management measures taken by the entity;
 - Supervise the implementation of the risk management measures;
 - Follow training in order to gain sufficient knowledge and skills to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the entity
 - Offer similar training to their employees on a regular basis;
 - Be accountable for the non-compliance
- Criminal prosecutions and liability?

Poll 5 Do you have confidence in current training?

- Yes
- No

Poll 6 Which levels does your training include?

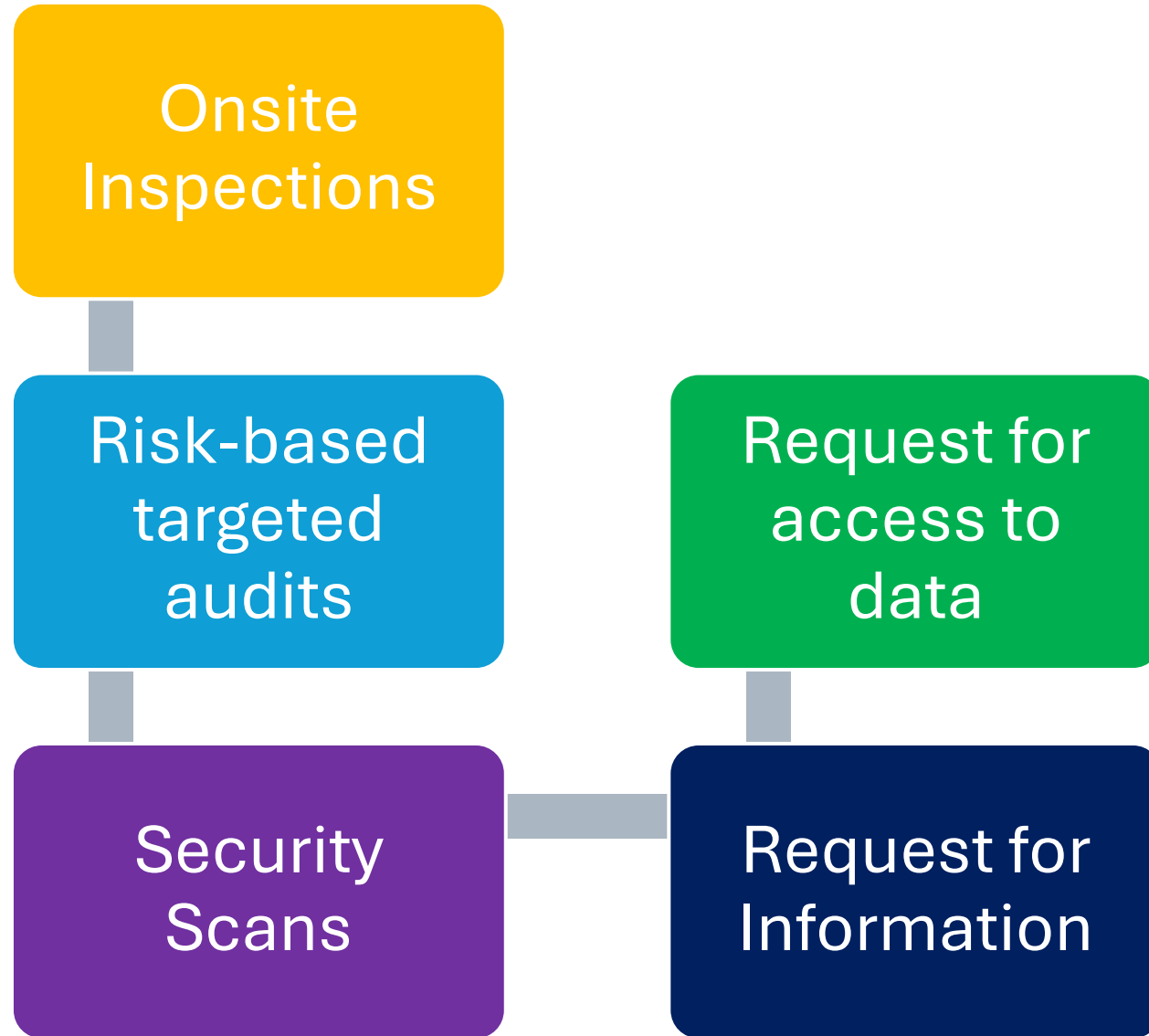
- Board
- Management
- All staff
- Data champions



PRIVACYENGINE



Audits



Implementation

- Policies
- Framework ISO27001 NIST
- Training
- Enforcement



NIS2 Policy Requirements

Policy Name	NIS 2 Article	Description
Information Security Policy	Article 21(2)(a)	<ul style="list-style-type: none"> Security protocols for information systems Guidelines for using encryption to protect data
	Article 21(2)(j)	<ul style="list-style-type: none"> Procedures on the use of Multi-Factor or Continuous Authentication Solutions
Business Continuity, Crisis Management, and Recovery Plan	Article 21(2)(c)	<ul style="list-style-type: none"> Strategies for maintaining operations during and after disruptions Strategies for managing crisis situations Strategies for data recovery
Supplier Security Policy & Agreements	Article 21(2)(d)	Security requirements for suppliers and partners
Employee and Management Training Plan	Article 21(2)(g)	<ul style="list-style-type: none"> Training on management responsibilities for overseeing cybersecurity Training for all employees on cybersecurity awareness
IT Hygiene Policy	Article 21(2)(g)	Essential cybersecurity practices for IT systems
Human Resources Security Policy	Article 21(2)(i)	Security protocols for managing employee access and behaviour
Asset Management Policy & Inventory	Article 21(2)(i)	<ul style="list-style-type: none"> Procedures for managing and tracking IT assets Procedures for controlling access to systems and data
Cybersecurity Risk Management Framework	Article 21(1)	<ul style="list-style-type: none"> Overall approach to managing cybersecurity risks Methods for assessing and prioritizing cybersecurity risks
Cybersecurity IT Policy	Article 21(2)(a)	<ul style="list-style-type: none"> Security protocols for information systems
	Article 21(2)(h)	<ul style="list-style-type: none"> policies and procedures regarding the use of cryptography and encryption Requirements for using multi-factor authentication
	Article 21(2)(j)	<ul style="list-style-type: none"> Protocols for secure voice, video, and text communication Procedures for secure internal communication during emergencies
Risk Analysis Policy	Article 21(2)(a)	Guidelines for analysing cybersecurity risks
Incident Response Plan & Log	Article 21(2)(b)	Procedures for handling cybersecurity incidents
Secure Development & System Acquisition Policy	Article 21(2)(e)	Procedures on the security of network and information systems during acquisition, development, and maintenance, which includes effectively handling vulnerabilities and disclosure.
Cybersecurity Effectiveness Policy	Article 21(2)(f)	Methods for measuring the effectiveness of cybersecurity measures (Penetration Testing/Vulnerability Scanning/Breach demonstrations)
Supplier Risk Assessment & Management Plan	Article 21(3)	Processes for assessing and managing security risks associated with suppliers

Implementation

Article 21 of NIS2 compels organisations to take *“appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services”*

• Risk analysis & IT security policies	• Policies to assess Cybersecurity measures.
• Incident handling procedures	• Cyber hygiene and cybersecurity training
• Business continuity plans	• Cryptography and encryption policies
• Security in Network and IT systems acquisition	• Human resources security, access control policies
• Supply chain security	• Multi-factor authentication (MFA)

Breaking down NIS2

MEASURES MUST BE

- Proportionate to risk, size, cost, and impact & severity of incidents
- Take into account the state-of-the-art, and where applicable relevant European and international standards

ENTITIES MUST

- Take into account:
- Vulnerabilities specific to each direct supplier and service provider; and
- The overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedure

PENALTIES

- Must be effective, proportionate & dissuasive
- A maximum of at least 10,000,000 EUR or up to 2% of the total worldwide annual turnover of the **Essential Entity**, whichever is higher.
- A maximum of at least 7,000,000 EUR or 4% of the total worldwide annual turnover of the **Important entity**, whichever is higher

Poll 4 Do you use a Governance Framework?

- NIST
- ISO
- SOC
- Other
- None



Thank You!!

- Next Webinar
 - Based on the technical controls
 - Include industry leaders
- Slides will be sent out
- Reach out for follow up
 - nollag.conneely@privacyengine.io
 - lanre@datapriv.ie



PRIVACYENGINE



ADPO Speakers



Cian
O'Brien

Deputy
Commissioner, Data
Protection
Commission Ireland



Florence
Gaullier

Vercken, Gaullier



Emma
Martins

Chief Commissioner
of the UK Data &
Marketing
Commission



Cecilia
Alvarez

Meta



Ashley
Winton

Mishcon de Reya



Linda
NiChualladh

Citi



Kieran
McCorry

Microsoft



Barry
Scannell

William Fry



Jared
Browne

ADPO



Will Burke

LinkedIn



Nollag
Conneely

Privacy Engine



Jason Guy

EY



Paula
Carney-
Hoffler

ADPO



Maeve
Dunne

Conference
Chairperson
ADPO

ADPO Conference 9th May
Radisson Blue Hotel
Sign Up
www.ics.ie/adpo/adpoconference2024

PrivacyEngine NIS2 Gap Analysis
<https://www.privacyengine.io/nis2-questions/>

