

Introduction to the regulations in the NIS2 Directive






Objectives

- To achieve a high common level of cybersecurity across EU members states.
- To create a high level of harmonisation with regard to security requirements and reporting obligations across the Union.

Background

- With the ever-increasing digitalisation of personal and work life, it has become increasingly evident that cyber-threats, be they by criminals or nation-state actors, pose an evolving risk to the everyday working of society.
- The Network and Information Security Directive (NIS 1 - [EU 2016/1148](#)) set the precedent for EU legislation when it came to cybersecurity. Its goal was to achieve a high common level of cybersecurity across EU members states. It resulted in member states designating key "entities" as "Operators of Essential Services" (OES) or "Digital Service Providers" (DSP) and led to regulations being put in place in national law around the area of Cybersecurity, including incident notification by such entities.
- The NIS1 Directive included national supervision of critical sectors: EU Member states have to supervise the cybersecurity of critical market operators in their country: supervision is anticipated in critical sectors (energy, transport, water, health, digital infrastructure and finance sector), supervision is required for critical digital service providers (online market places, cloud and online search engines).

"Even though NIS2 is largely built on the current NIS directive, there are major upcoming changes that will require consideration." - [Deloitte](#)

	Risk Ownership	Management bodies will have a crucial and active role
	Enforcement	Competent Authorities can impose Administrative fines up to 10 million EUR or 2% of the total global annual turnover of the company
	Security Requirements	NIS2 provides a list of security measures that shall be implemented
	Supply Chain Security	Entities should perform due diligence of their supply chain
	Incident Reporting	Entities should submit an initial notification within 24 hours to the relevant competent authority of any significant cyber threat that could have potentially resulted in a significant incident. Furthermore, the recipients of their services must be informed of incidents that are likely to adversely affect the provision of that service.

"The speedy digital transformation of our society has expanded the threat landscape and is bringing about new challenges, which require adapted and innovative responses... such responses should aim to increase preparedness ...and the Union's capabilities to prevent, detect, respond to and mitigate cyber threats and be prepared to act in crisis."

**European Commission,
NIS 2 inception
Impact assessment document**

Perspectives of .IE PAC Registrar representatives

"Cost increases associated with NIS2 'accuracy' & bureaucracy could be terminal for many Registrars". **Michele Neylon, Blacknight Solutions.**

"NIS2 will raise the standard of cyber security risk management for all Registrars. This is a fundamentally good thing - we should be doing this already." **Kelly Salter, team-blue.**

"It's important that Law Enforcement and IP lawyers can contact domain name holders when there are allegations of illegality or online intellectual property infringement". **Prudence Malinki, MarkMonitor.**

"There is a need for more information. We will need to see the national legislation quickly, in order to prepare properly for NIS2 regulatory compliance". **Ciaran Morris, FCR Media.**




In Ireland

- The "National Competent Authority" is the NCSC.
- The "single point of contact" is the Department of Communications CSIRT.



Roinn Cumarsáide, Gníomhaíthe ar son na hAeráide & Comhshaoil
Department of Communications,
Climate Action & Environment



		
Huge fines	Real reputational risk	Large investment required
The NIS Directive and local legislation introduces potential fines that may vary per member state, but for some will be in line with GDPR. This is a big and serious change compared to the limited sanctioning possibility under the old regime.	Enforcement activities by national regulators will increase. Non compliance breaches will hence be brought to light sooner. Risk of reputational consequences will therefore become all the more real.	With the NIS Directive and Local legislation a significant effort and investment is required by identified entities to comply with the security regulations.

"All businesses are increasingly dependent on third party services - from major cloud providers, through the ecosystem of software as a service (SaaS) providers and managed service providers, to a new world of data and analytics service providers.

*In the old days, our IT was on-premises, defended by firewalls and barriers, **under our control and our management.** This model is dead, and with it comes a raft of new digital infrastructure providers that we depend on for hosting, for platform and for service provision.*

NIS is being revised to reflect this reality."

Dani Michaux, EMA Cyber Leader, KPMG Ireland