# The Network and Information Systems Directive (NIS2)

May 2024

ROPES & GRAY

# Agenda

1. Introduction to NIS2

2. Three Core Obligations

3. Countdown to October 2024

# 1. Introduction to NIS2

ROPES & GRAY

# The EU Cyber Landscape: A Reminder

- The European Union has become the most heavily regulated jurisdiction in the world for cybersecurity – as well as one of the most attractive for criminals and bad actors, from solo hackers to nation states.

- In addition to the existing laws – EU GDPR and UK GDPR; ePrivacy Directive (EU) and ePrivacy Regulations (UK) – there is a raft of new legislation which aims at regulating and strengthening cybersecurity in a range of key sectors.

- The Directive on minimum cybersecurity standards to be implemented across the EU ("NIS2") is the one of most important of these new laws for your business – NIS2 will take effect in **October 2024**.

# NIS2: The View From 30,000 Feet

- NIS2 is an EU directive designed to strengthen the IT security posture of organisations that operate in certain highly critical sectors – **including the healthcare and medical device industries**.

- It replaces and strengthens the current framework – known as NIS1 – that was introduced in May 2018 (the same month as the GDPR) but which proved ineffective and has been overshadowed by the GDPR.

- NIS2 will apply to all healthcare organisations in scope for NIS1 ("services provided by health professional to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provisions of medicinal products and medical devices"), as well as a range of new entities, including **medical device manufacturers**.

- **TAKEAWAY**: NIS2 must be implemented in generally the same way across the EU (subject to some derogations). Member States have until **17 October 2024** to do this, at which point NIS2 will apply…

# Scope of Application

- NIS2 applies to a **wide range** of healthcare and medical devices businesses, including:
  - Entities providing healthcare in the EU.
  - Manufacturers of medical devices (including *in vitro* diagnostic devices).
  - Entities carrying out R&D of medicinal products.
  - Manufacturers of patient file management software.

- Although most of these entities are already subject to some form of cybersecurity regulation in the EU (GDPR and NIS1), NIS2 expands the scope of these laws – **including on an extra-territorial basis…**

- NIS2 will apply to entities which: (1) provide services or carry out activities in the EU; (2) are a "medium-sized enterprise" (annual turnover of more than **€10 million** and employ more than **50 members of staff**); and (3) are listed in one of the Annexes of the Directive.

- Entities are also classified as "important" or "essential" – important entities are subject to an *ex-post* enforcement regime, whereas essential entities are also subject to an *ex-ante* regime.

# NIS2 Enforcement

- **Overview**: EU Member States are required to introduce rules that provide for effective, proportionate and dissuasive penalties and other measures for breaches of NIS2.

- Administrative penalties can be the greater of up to **€7m or 1.4% of annual worldwide turnover** (for important entities) and up **to €10m or 2% of annual worldwide turnover** (for essential entities).

- There is also scope for **criminal penalties** – an approach that aligns with trends in EU regulation.

- Infringing entities can be required to make public statements setting out the details of their non-compliance **and** naming the individuals responsible for breaches of NIS2.

- NIS2 gives national regulators wide investigational powers, including on-site audits, document requests and orders to remedy non-compliance (likely within a short period).
  - The last of these is increasingly being used under the GDPR – and in practice is worse than a fine.

# 2. Three Core Obligations

ROPES & GRAY

# Core Obligation #1: Governance and Controls

- **Overview**: An entity's "management bodies" must approve and oversee the implementation of an IT risk management compliance programme that meets the requirements of NIS2.
  - Member states can introduce laws that ban individuals from acting in a management function.

- The board and senior management must **maintain an active role** in understanding and directing your approach to cyber risk – including through training to keep their knowledge up to date.
  - Given the speed at which the cybersecurity world is developing, this won't always be an easy task.

- **NEXT STEPS**: Management bodies can be held liable for non-compliance, so you should:
  - Make management aware **now** about the NIS2 assessment process and their role going forward.
  - Help them understand what's needed: gap assessments; institutional backing; investments.
  - Roll out training **before** NIS2 takes effect (ideally starting as soon as possible).

# Core Obligation #2: ICT Risk Management

- **Overview**: Entities must have in place an appropriate and documented IT risk management framework that helps them address risks quickly and comprehensively. As a minimum it will include:
  - Implementing policies, procedures and tools, including reporting lines.
  - Adopting robust security systems and advanced resilience testing.
  - Helpfully, these measures can be applied on a **proportionate** and **risk-based basis…**

- … But you will also need to flow down you NIS2 obligations to its customers and supply chains.
  - Review and evaluate the adequacy of vendors' security standards.
  - Use cryptography and encryption where appropriate.

- **NEXT STEPS**: Although most organisations in the EU are already subject to some form of cybersecurity regulation, NIS2 significantly expands the scope of these laws and will apply to most of your business activities in the EU as well as directly to some customers and service providers.

# Core Obligation #3: Incident Reporting

- **Overview**: Entities must be able to identify, manage and notify "significant" security incidents – whether or not personal data are involved…

- An incident is significant if it has caused or is capable of causing: (1) **severe operational disruption;** or (2) **considerable material or non-material damage** to affected individuals.

- Reporting timelines are among the most involved – and in some cases, the shortest – in the EU:
  - **Initial Notification**: Significant incidents must be notified within **24 hours** of becoming aware.
  - **Secondary Notification**: Must be made no later than **72 hours** after the initial notification.
  - **Final Report**: Not later than one month from the initial notification.

- Entities must also notify individuals (i.e., patients/users) of some incidents **without undue delay**.

- **NEXT STEPS**: Existing reporting procedures are unlikely to be sufficient, meaning that you should: (1) assign roles and responsibilities for NIS2 breach reporting; (2) establish incident response procedures (these can be folded into a wider framework); and (3) train relevant staff.

# Countdown to October 2024

ROPES & GRAY

# Mapping the Next 18 Months

- Although the requirements are different, you should leverage your GDPR/cyber compliance programme – and the experience gained through putting that in place – to inform your NIS2 strategy.

- **Given the impact that NIS2 will have, it should be treated as seriously as the GDPR.**

- As a first step, we recommend taking the following actions:
  - Assess which business lines will be impacted and identify key stakeholders (internal and external).
  - Determine the extent to which current processes and procedures can be leveraged or updated.
  - Identify compliance gaps – both organisational and technical – and agree on remediation priorities.
  - Ensure that management is involved from the outset so it can help to play an active role in the journey.

- **TAKEAWAY**: Don't bury your head in the sand. 6 months feels like a long time but our experience with the GDPR is that too many organisations left it to the last minute – and some are still playing catch up…

# How We Can Help

- Ropes & Gray has significant expertise designing and helping hundreds of firms implement their privacy, data protection and security compliance programmes in the EU and UK.

- We also have deep experience in assisting our clients' investee companies with ongoing monitoring and remediation of their privacy, data protection and information security compliance programmes.

- We are working with clients to identify and plan for the measures they need to take for NIS2.

- Several of these companies also have a monthly "hotline" in place with Ropes & Gray for data privacy and security advice that they are now also using for assisting with NIS2 implementation.

**Edward Machin**
**Counsel**
edward.machin@ropesgray.com
**DD: +44 20 3847 9094**

ROPES & GRAY