



Making compliance simple, every day

Cracking the Code: NIS2 & DORA Legislation Made Simple

Dr Muneebah Kara | Anna Walters

© Risk Evolves Ltd 2024. Unauthorised copying and re-use is forbidden.



WHO ARE WE?

We're on a mission to take consulting from dreary to delightful. Our clients love our friendly, jargon-free and personal approach, but we're more than just happy faces.

We lead by example, holding ourselves to high standards of governance, risk management, and compliance.

Quite simply, we would never ask our clients to do something we wouldn't do ourselves.

TODAY'S SESSION

- Explain the NIS2 and DORA
- What they mean for you
- Learn the steps for compliance
- Discover how to stay ahead in the ever-changing landscape of digital security and regulation



European Digital laws: current, new & proposed

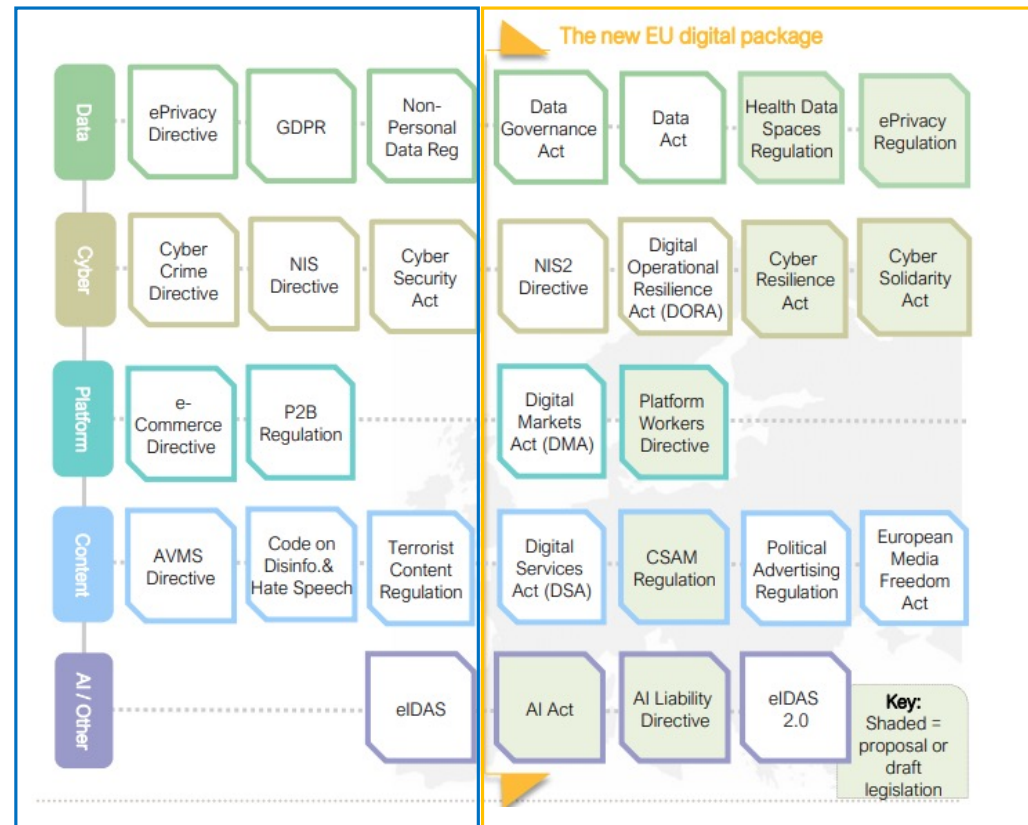


Image from Linklaters: EU – DGA, Data Act, NIS2, DSA... confused? (linklaters.com)

European legislative horizon

- **NIS 2 Directive** - Replacing the existing Network and Information Systems Directive (NIS1), the scope is widening and imposes increased cyber security and breach notification obligations on essential and important entities. Oct 24 to transpose into national law (Note UK still has NIS1)
- **DORA** - The Digital Operational Resilience Act (DORA) is an EU Regulation that will impose significant cyber security obligations on financial services institutions and regulate critical third parties
- **The Data Act** This Regulation will regulate the use of data from “Internet of Things” (IoT) devices and make it easier to switch between cloud services. It is aimed at regulating the use, access, and sharing of data generated by businesses, consumers, and public sector bodies in order to unlock the potential of data by ensuring fair access to and use of data across industries, driving innovation & competition.
- **Digital Services Act** – This Regulation aims to regulate online platforms & digital services. Its primary goal is to create a safer digital space. It applies to a broad range of digital services, including online marketplaces, social media platforms, and search engines
- **AI Act** - This Regulation introduces tiered regulation of artificial intelligence systems; some uses are banned, some are subject to significant compliance obligations, some are subject to very limited regulation
- **Cyber Resilience Act** (Close to adoption) - This Regulation will impose cyber security obligations on those supplying products containing digital technology such as consumer devices like IoT gadgets to industrial machinery and software used in critical infrastructures

NIS2 - am I in scope?

If your UK company falls into any of the following sectors and operates within the EU market or provides services to EU-based customers, NIS2 may apply to you.

Essential Entities

A grid of icons representing sectors classified as Essential Entities under NIS2. The grid is divided into two columns. The left column has a blue-to-purple gradient background and contains icons for Health Sector (heart with pulse), Banking (classical building), Financial markets (line graph with upward arrow), Transport (truck), Digital Infrastructure (router), Energy sector (wind turbines and power lines), and Drinking water (faucet with drop). The right column has a red-to-pink gradient background and contains icons for Public Admin (city buildings), Space (rocket and satellite), and Waste water (water drop).

Important Entities

A grid of icons representing sectors classified as Important Entities under NIS2. The grid has a red-to-pink gradient background and contains icons for Public Admin (router), Post & Courier (postbox), Chemical manufacturing, production & distribution (flasks and hexagons), Waste Management (trash bin and recycling symbol), Research (microscope), Manufacturing (factory), and Food production & distribution (truck and food items).

'important entities' will also need to comply with the regulations; although subject to less regulatory oversight

DORA - am I in scope?

DORA is relevant to UK-based companies, especially where you have operations, subsidiaries, or customers in the EU.

Covered Entities

- Credit Institutions
- Banking
- Insurance
- Payment Services
- Asset Management co's and funds
- Trading Venues
- Financial Market Infrastructure

- Data Centres
- Cloud Services
- Software Vendors

If your UK-based business provides technology or ICT services to EU-based financial institutions, you may be subject to DORA's regulations

Key themes

- Details and requirements are different for each legislation
- Key themes across the package of digital laws is to strengthen cyber security requirements across a wide range of sectors, industries and devices
- In addition to strengthening security requirements, they encourage greater transparency and coordination
- As end users, managers or manufacturers of many of these services or devices, these new regulations are aimed at protecting business and users.
- They will move us all into adopting, and adapting to a different approach to cybersecurity and risk management

Essentially these new legislations moves us from a “we’re doing our best” approach to a more informed and robust risk analysis and risk management approach.

ISO standards +++

- ISO27001 supports a strong alignment with NIS2.
- ISO22301 Business Continuity will also add an additional BC and DR framework

Additional requirements include:

- **Strong governance** - Corporate management liability is a key feature. It will involve management bodies including the CEO, board of directors and senior management being trained and directly involved in overseeing the cyber risk management plan.
- **Robust assessments & plans** – Organisations will be required to conduct cyber resilience risk assessments and analyse their ability to respond & continue operating during high-risk situations.
- **Incident reporting** – incidents to be reported within 24 hours with follow-up report no later than 72 hours
- **Supply Chain** – Organisations will be required to consider how security might impact organisations you interact with. Evaluate extended supply chains and identify certain third-party supplier vulnerabilities

What should I do?

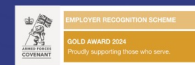
Act now!

- ✓ Read the regulations
- ✓ Bring together the right team
- ✓ Seek support & guidance
- ✓ Don't try to eat the elephant
- ✓ Watch out for snakeoil

Steps to consider

- Assess Your Applicability
- Map out your EU operations
- Understand supply chain impact – upstream & downstream
- Do your gap analysis
- Review & strengthen cybersecurity measures
- Adopt or adapt your Risk Management Framework
- Train your teams
- Prepare for regulatory enforcement
- Stay informed on updates
- Monitor regulatory changes - including UK adoption
- Other areas of consideration e.g insurance, policy, certifications, comms plans

ANY QUESTIONS?





WARWICKSHIRE
TRAINING HUB

WANT SKILLS THAT HELP YOU STAND OUT?

Funded training places available, delivered
by award-winning industry experts
across warwickshire.


[Visit the website to find out more.](#)

WARWICKSHIRE **TRAINING**HUB.CO.UK



CONNECT WITH US

 info@riskevolves.com

 +44 (0)1926 800710

 [@riskevolves](#)

 [@riskevolves](#)

THANK YOU FOR JOINING
US