EU LEGISLATION GUIDANCE

NIS2 NETWORK & INFORMATION SYSTEMS DIRECTIVE

riskevolves

WHAT IS IT?

NIS2 is an updated version of the EU's Network and Information Systems Directive, aimed at enhancing cybersecurity across member states. It builds upon the original NIS Directive (Directive (EU) 2016/1148) with several key enhancements.

UK BUSINESS RELEVANCE

NIS2 may apply to UK businesses operating in the EU or providing services to EU entities:

Essential Entities:

- Energy (electricity, oil, gas)
- Transport (air, rail, water, road)
- Financial Services
- Healthcare
- Drinking Water Supply
- Digital Infrastructure
- Public Administration

Important Entities:

- Postal and Courier Services
- Waste Management
- Manufacture of Critical Products
- Food Supply
- Space
- Digital Providers

CRITERIA FOR APPLICABILITY

While NIS2 is an EU directive, it may impact UK businesses in several ways. Consider the following questions to determine if NIS2 applies to your organisation:

- Does your company operate in a covered sector within the EU?
- Do you provide critical services to EU-based customers?
- Are you a medium-sized or large enterprise (≥50 employees or ≥€10 million annual turnover)?
- Do you operate in a high-risk sector (e.g., healthcare, energy) even as a smaller business?
- Are you part of the supply chain for essential or important entities covered by NIS2?
- Do you process or store data for EU-based entities that fall under NIS2's scope?

If you answer "yes" to any of these questions, your business is likely subject to NIS2.

KEY DATES:

Entry into force: 16 January 2023

Implementation deadline: 17 October 2024

Application date: 18 October 2024

COMPLIANCE WITH NIS2

If NIS2 applies to your business, take the following steps:

1. **Assess Applicability**: Determine if you're an "essential" or "important" entity under NIS2.
2. **Conduct Gap Analysis**: Assess current cybersecurity against NIS2 requirements.
3. **Develop Compliance Plan**: Create a road-map to meet NIS2 requirements by October 2024.
4. **Implement Risk Management**: Establish robust risk assessment and management processes.
5. **Enhance Incident Response**: Develop procedures aligned with NIS2's reporting timelines.
6. **Strengthen Business Continuity**: Update plans to ensure service continuity during disruptions.
7. **Address Supply Chain Security**: Manage cybersecurity risks across your supply chain.
8. **Ensure Governance**: Involve senior management in cybersecurity oversight.
9. **Provide Training**: Implement regular cybersecurity training for all staff.
10. **Prepare for Audits**: Maintain thorough documentation of cybersecurity measures.

By following these steps, organisations can work towards NIS2 compliance and enhance their cybersecurity posture.

DORA DIGITAL OPERATIONAL RESILIENCE ACT

riskevolves

WHAT IS IT?

The Digital Operational Resilience Act (DORA) is an EU regulation aimed at strengthening the digital resilience of financial entities. DORA sets out requirements for the security of network and information systems supporting the business processes of financial entities.

DORA addresses the increasing reliance on technology in financial services and the growing number of cyber-attacks. It applies to a broad spectrum of entities in the financial sector, including banks, insurers, investment firms, and payment service providers. The regulation also aims to harmonise ICT risk management requirements across the EU financial sector, promoting a consistent approach to digital operational resilience.

Importantly, DORA's scope extends beyond traditional financial institutions to include ICT service providers, such as cloud services and data centres, recognising their critical role in the sector's digital infrastructure.

KEY DATES:

Entry into force: 16 January 2023

Date of applicability: 17 January 2025

UK BUSINESS RELEVANCE

It applies to a wide range of UK-based financial entities with operations, subsidiaries, or customers in the EU, including:

- Banks and credit institutions
- Investment firms
- Insurance and reinsurance companies
- Payment service providers and electronic money institutions
- Asset management companies and funds
- Trading venues and financial market infrastructures
- Third-Party ICT Providers: DORA also covers third-party ICT service providers, including cloud service providers, data centres, and software vendors.

CRITERIA FOR APPLICABILITY

- Does your company provide ICT services to EU financial institutions?
- Do you have operations in the EU involving critical ICT support to financial services?
- Are you a UK-based financial entity with branches or subsidiaries in the EU?

If you answer "yes" to any of these questions, your business is likely subject to the Digital Services Act.

COMPLIANCE WITH DORA

If DORA applies to your business, take the following steps:

1. **Identify applicability**: Review your business structure, services, and EU operational footprint.
2. **Determine your role**: Understand your specific obligations as a financial institution or ICT provider.
3. **Strengthen ICT Resilience**:
   - Regularly assess and mitigate ICT risks
   - Develop a resilience framework
   - Ensure external ICT providers meet DORA standards
4. **Implement Incident Management**:
   - Set up mechanisms for prompt detection, reporting, and resolution of ICT-related incidents
   - Ensure compliance with DORA's reporting timelines
   - Train employees on incident detection and reporting responsibilities
5. **Prepare for Audits and Regulatory Scrutiny**:
   - Document ICT security measures, resilience frameworks, and incident management processes
   - Build relationships with relevant EU regulatory bodies

Following these steps, UK businesses can comply with DORA and remain competitive in the EU financial market.

CRA CYBER RESILIENCE ACT

EU CYBERSECURITY REQUIREMENTS FOR PRODUCTS WITH DIGITAL ELEMENTS

riskevolves

WHAT IS IT?

The Cyber Resilience Act (CRA) is a new piece of EU legislation aimed at improving the cybersecurity of products with digital elements, including software and connected devices. The CRA seeks to establish a common set of cybersecurity requirements for the design, development, and marketing of products sold in the EU to ensure they are secure throughout their life-cycle. The legislation applies to a broad range of digital products, from consumer devices like IoT gadgets to industrial machinery and software used in critical infrastructures.

The CRA's goal is to reduce vulnerabilities in digital products and minimise the potential for cyberattacks that could disrupt business, consumer privacy, or even national security.

KEY DATES:

Entry into force:

Still in Proposal Stage

Date of applicability:

Expected to be 24 months after entry into force

Implementation deadline:

Expected to be 36 months after entry into force for certain provisions

UK BUSINESS RELEVANCE

The CRA may impact UK businesses that manufacture, sell, or distribute digital products in the EU market.

It applies to:

- Consumer products (e.g., smart home systems, wearables, IoT devices)
- Software (standalone and embedded)
- Industrial products (machinery, equipment, critical infrastructure systems)
- Hardware and IT systems with digital components

CRITERIA FOR APPLICABILITY

- Do you manufacture, distribute, or sell connected devices or software to the EU market?
- Are your digital products used within the EU, directly or via a third party?
- Does your business develop software or provide digital services integrating with physical products sold in the EU?

If you answer "yes" to any of these questions, your business is likely subject to the Cyber Resilience Act.

COMPLIANCE WITH THE CRA

If CRA applies to your business, take the following steps:

1. **Assess Your Applicability**
   - Identify covered products
   - Review EU market presence
2. **Integrate Cybersecurity in Product Development**
   - Embed cybersecurity throughout the product life-cycle
   - Regularly assess products for vulnerabilities
   - Plan for secure updates and patch management
3. **Meet Cybersecurity Requirements**
   - Ensure products meet minimum cybersecurity requirements
   - Maintain records of cybersecurity measures and testing results
4. **Prepare for Regulatory Oversight**
   - Be ready for audits
   - Develop a plan for detecting, responding to, and reporting cybersecurity incidents

By following these steps, UK businesses can ensure compliance with the Cyber Resilience Act and maintain their ability to operate in the EU market.

DATA ACT EU REGULATION ON DATA SHARING

riskevolves

WHAT IS IT?

The Data Act is a key piece of legislation proposed by the European Union (EU) aimed at regulating the use, access, and sharing of data generated by businesses, consumers, and public sector bodies. The act aims to unlock the potential of data by ensuring fair access to and use of data across industries, driving innovation, competition, and value creation in the EU's data economy.

It focuses on:

- Enhancing the availability of data for public and private entities.
- Protecting the rights of businesses and individuals when it comes to data access and sharing.
- Promoting the interoperability and portability of data.

The Data Act applies to a wide range of sectors and industries where data is generated, collected, and used, including the Internet of Things (IoT), connected devices, cloud services, and AI applications.

KEY DATES:

Entry into force: 11 January 2024

Date of applicability: 12 September 2025

UK BUSINESS RELEVANCE

The Data Act may impact UK businesses dealing with EU-generated data or working with EU-based partners.

It applies to:

- Manufacturers of connected devices
- Service providers (e.g., cloud computing, data processing, AI solutions)
- Data aggregators
- Public sector entities
- Supply chain partners: UK businesses that are part of the supply chain for EU companies covered by the Data Act, even if they don't directly handle EU data themselves.

CRITERIA FOR APPLICABILITY

- Does your business handle EU-generated data from IoT devices, connected products, or digital services?
- Do you provide cloud or digital services to EU companies or process EU customer data?
- Are you involved in cross-border data-sharing arrangements with EU entities?

If you answer "yes" to any of these questions, your business is likely subject to the Data Act.

COMPLIANCE WITH THE DATA ACT

If the Data Act applies to your business, take the following steps:

1. **Assess Your Applicability**
   - Determine your data roles (holder or user)
   - Review data-sharing practices
2. **Strengthen Data Governance**
   - Ensure fair and non-discriminatory data-sharing contracts
   - Protect trade secrets and confidential information
   - Implement interoperability standards
3. **Prepare for Data Access Requests**
   - Establish clear processes for handling requests
   - Be aware of public sector data request situations
4. **Review Contractual Relationships**
   - Ensure compliance with third-party service providers
   - Inform stakeholders about their data rights

By following these steps, UK businesses can ensure compliance with the EU Data Act and maintain their ability to operate in the EU market.

AI ACT EU LEGISLATION ON ARTIFICIAL INTELLIGENCE

riskevolves

WHAT IS IT?

The AI Act is a significant piece of European Union (EU) legislation aimed at regulating artificial intelligence (AI) systems and ensuring their ethical and safe use. The Act establishes a comprehensive framework for AI, focusing on the risk-based regulation of AI applications. Its primary goals are to promote the development and use of AI technologies that are safe and respect fundamental rights, while ensuring that high-risk AI applications are subject to stringent requirements and oversight.

The AI Act classifies AI systems into different risk categories—unacceptable risk, high risk, and minimal risk—and applies varying levels of regulation based on these categories.

KEY DATES:

Entry into force: 1 August 2024

Date of applicability:

General provisions: 2 August 2026

Prohibited practices: 2 February 2025

GPAI and governance: 2 August 2025

Certain high-risk AI systems: 2 August 2027

UK BUSINESS RELEVANCE

Although the UK is no longer part of the EU, the AI Act may impact UK-based companies that:

- Develop or supply AI systems used in the EU
- Use AI systems that affect EU users or consumers
- Collaborate with EU entities on AI solutions
- Provide AI-powered services or products to EU customers
- Have subsidiaries or branches operating within the EU
- Process data of EU citizens using AI technologies
- Are part of a supply chain that includes EU companies using AI systems

CRITERIA FOR APPLICABILITY

- Do you develop or provide AI systems used by EU entities or consumers?
- Are you involved in deploying high-risk AI applications in the EU?
- Do you have EU operations or partnerships involving AI technology?

If you answer "yes" to any of these questions, your business is likely subject to the AI Act.

COMPLIANCE WITH THE AI ACT

If the AI Act applies to your business, take the following steps:

1. **Assess Your Applicability**
   - Classify your AI systems by risk category
   - Evaluate your EU market presence
2. **Implement Compliance Measures**
   - For High-Risk AI Systems:
     - Regularly evaluate risks
     - Maintain detailed records
     - Implement monitoring and control mechanisms
     - Establish incident reporting procedures
   - For Minimal Risk AI Systems:
     - Follow best practices for transparency, fairness, and accountability
3. **Stay Informed**
   - Monitor updates to the AI Act and related guidance
   - Engage with industry associations and regulatory bodies for support

By following these steps, UK businesses can ensure compliance with the EU AI Act and maintain their ability to operate in the EU market.

DSA DIGITAL SERVICES ACT

EU LEGISLATION ON ONLINE PLATFORMS & DIGITAL SERVICES

riskevolves

WHAT IS IT?

The Digital Services Act (DSA) is EU legislation regulating online platforms and digital services. It aims to create a safer digital space by enhancing accountability and transparency, especially for content-hosting platforms. The DSA applies to online marketplaces, social media, and search engines, setting standards for content moderation, advertising transparency, and user rights protection.

The DSA harmonises rules across the EU to promote a fairer digital environment. It introduces tiered obligations, with stricter requirements for very large platforms reaching a significant portion of EU consumers. Additionally, the DSA empowers users by giving them more control over their online experiences, including the right to challenge content moderation decisions and opt out of certain types of targeted advertising.

KEY DATES:

Entry into force: 16 November 2022

Date of applicability:

For very large online platforms and very large online search engines: 17 February 2024

For all other entities: 17 February 2025

UK BUSINESS RELEVANCE

The DSA may impact UK-based companies operating online platforms or digital services used within the EU.

It covers:

- Online Intermediaries (internet access providers, cloud providers, hosting services)
- Online Platforms (social media, app stores, marketplaces, content-sharing platforms)
- Search Engines
- Very Large Online Platforms (VLOPs) with over 45 million EU users
- Digital Service Providers offering services to EU consumers or businesses, even if not established in the EU

CRITERIA FOR APPLICABILITY

UK businesses may be subject to the DSA if they:

- Have users or customers within the EU
- Host or distribute user-generated content in the EU
- Enable cross-border sales to EU consumers
- Provide digital services or platforms accessible to EU users

If you answer "yes" to any of these questions, your business is likely subject to the Digital Services Act.

COMPLIANCE WITH THE DSA

If the DSA applies to your business, take the following steps:

1. **Assess Your Applicability**
   - Classify your AI systems by risk category
   - Evaluate your EU market presence
2. **Implement Compliance Measures**
   - For High-Risk AI Systems:
     - Regularly evaluate risks
     - Maintain detailed records
     - Implement monitoring and control mechanisms
     - Establish incident reporting procedures
   - For Minimal Risk AI Systems:
     - Follow best practices for transparency, fairness, and accountability
3. **Stay Informed**
   - Monitor updates to the AI Act and related guidance
   - Engage with industry associations and regulatory bodies for support

By following these steps, UK businesses can work towards compliance with the Digital Services Act and maintain their ability to operate effectively in the EU digital market.

NEED EXPERT GUIDANCE ON YOUR COMPLIANCE JOURNEY?
CONTACT RISK EVOLVES TODAY

WWW.RISKEVOLVES.COM

01926 800710