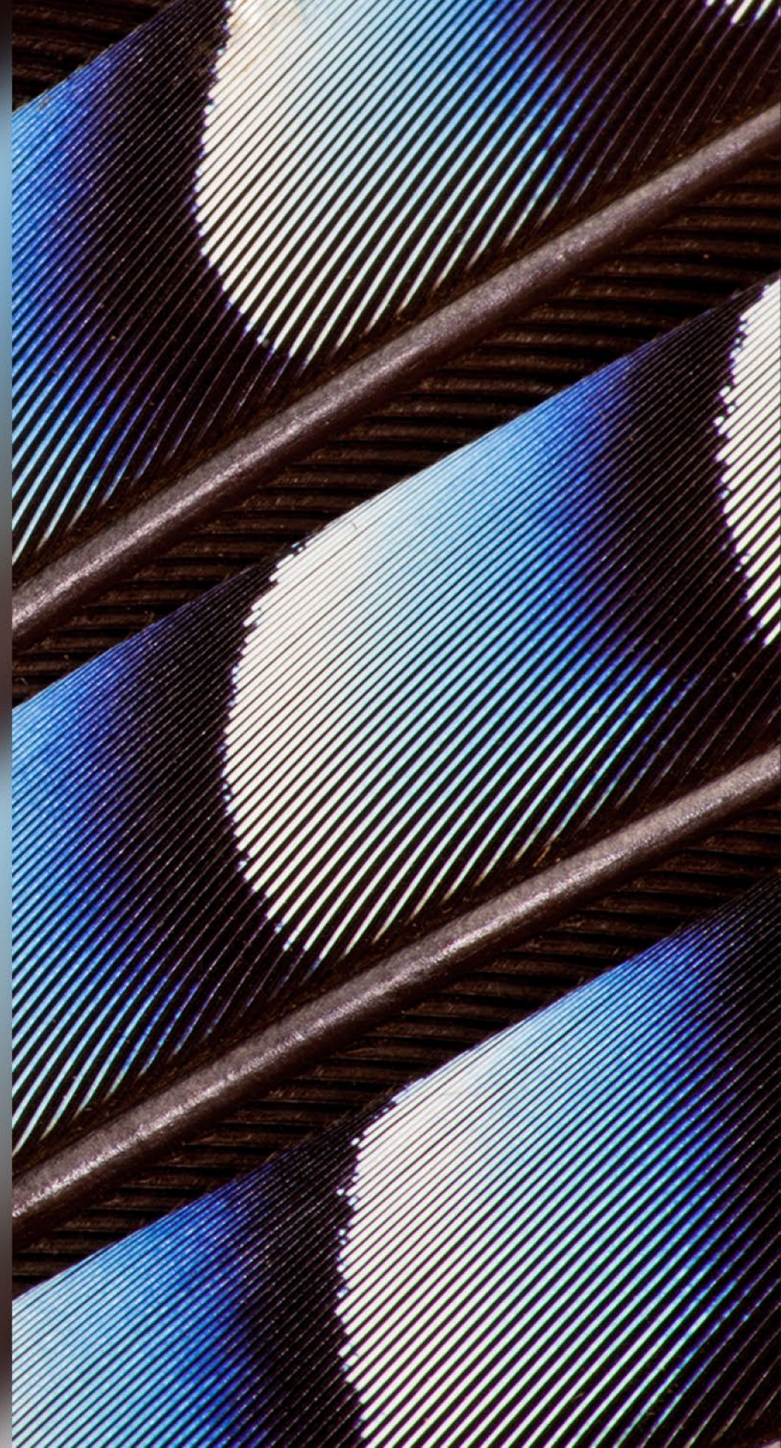
pillsbury

Thank you for joining.
Our program will begin in a moment.

30 OCTOBER 2024

# Key EU/UK Cybersecurity Developments

What Companies Doing Business in the EU/UK Need to Know



# Presenters

## **Steven Farmer** | Partner

steven.farmer@pillsburylaw.com

Steven Farmer co-chairs Pillsbury's Global Privacy, Data Protection and Cybersecurity team. He advises companies, ranging from some of the world's largest multinationals to startups, that are looking to launch or expand in the UK/EU, whilst navigating complex regulatory and legal issues. His client relationships encompass sectors including technology, financial services, energy, manufacturing, aviation and defense.

## **Lee Rubin** | Partner

lee.rubin@pillsburylaw.com

Lee Rubin advises clients on a variety of commercial transactions, primarily technology and complex outsourcing arrangements. His work focuses on the financial services sector where he counsels heavily regulated global entities on contracting and compliance issues, and he also works with vendors supplying services to financial institutions.

## **Scott Morton** | Counsel

scott.morton@pillsburylaw.com

Scott Morton advises clients on data privacy, data protection and cybersecurity issues, direct marketing, prize competitions and regulatory compliance. His work focuses on the tech and financial services sectors, in particular.

# Agenda

1. Overview of the EU & UK Cybersecurity Landscape
2. EU/UK General Data Protection Regulation (GDPR)
3. Network and Information Systems (NIS)
4. Digital Operational Resilience Act (DORA)
5. Key U.S. Cybersecurity Legislation for UK/EU Companies
6. Key Takeaways

pillsbury

# 1. Overview of the EU & UK Cybersecurity Landscape

pillsbury

# Overview of the EU Cybersecurity Landscape

**Data Protection and Privacy**

- General Data Protection Regulation (GDPR)
- e-Privacy Directive

**Security of Network and Information Security Systems**

- Cybersecurity Directive ((EU) 2016/1148) (NIS 1)
- Directive (EU) 2022/2555 (NIS 2 Directive)
- EU Cybersecurity Act

**Physical Security**

- Critical Entities Resilience Directive

**Product Development**

- EU Cyber Resilience Act
- EU Data Act

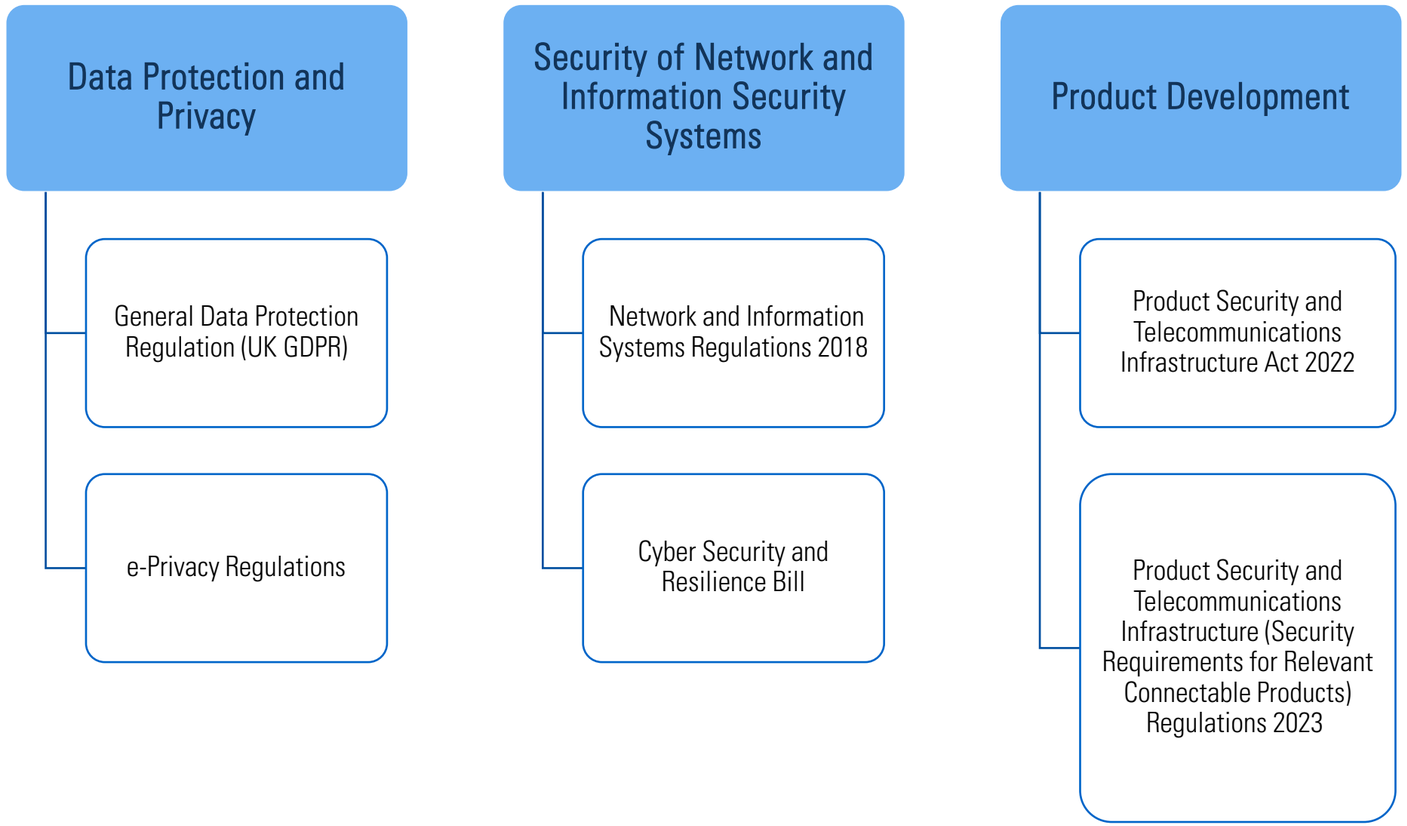
**Sector-Specific**

- Financial Services Entities
  - The Digital Operational Resilience Act (DORA)
  - DORA Directive
  - Payment Services Directive ("PSD2")

**Other**

- EU AI Act

# Overview of the UK Cybersecurity Landscape



# 2. EU/UK General Data Protection Regulation (GDPR)

pillsbury

# Overview of GDPR – Key Cybersecurity Requirements

- Applies to the collection, processing and security of personal data.
- Introduced key cybersecurity measures to strengthen data security across sectors.
- Applies to EU/UK and non-EU/UK businesses offering goods/services or monitoring data subjects in the EU/UK.
- Security Measures (Article 32)
  - Controllers and processors must implement appropriate technical and organizational measures to ensure data security.
  - Certifications and codes of conduct may be used to demonstrate compliance.
- Processor Obligations (Article 28)
  - Controllers must only engage processors with sufficient guarantees of GDPR compliance (Article 28(1)).
  - Contracts must include detailed security provisions, including confidentiality and cooperation obligations

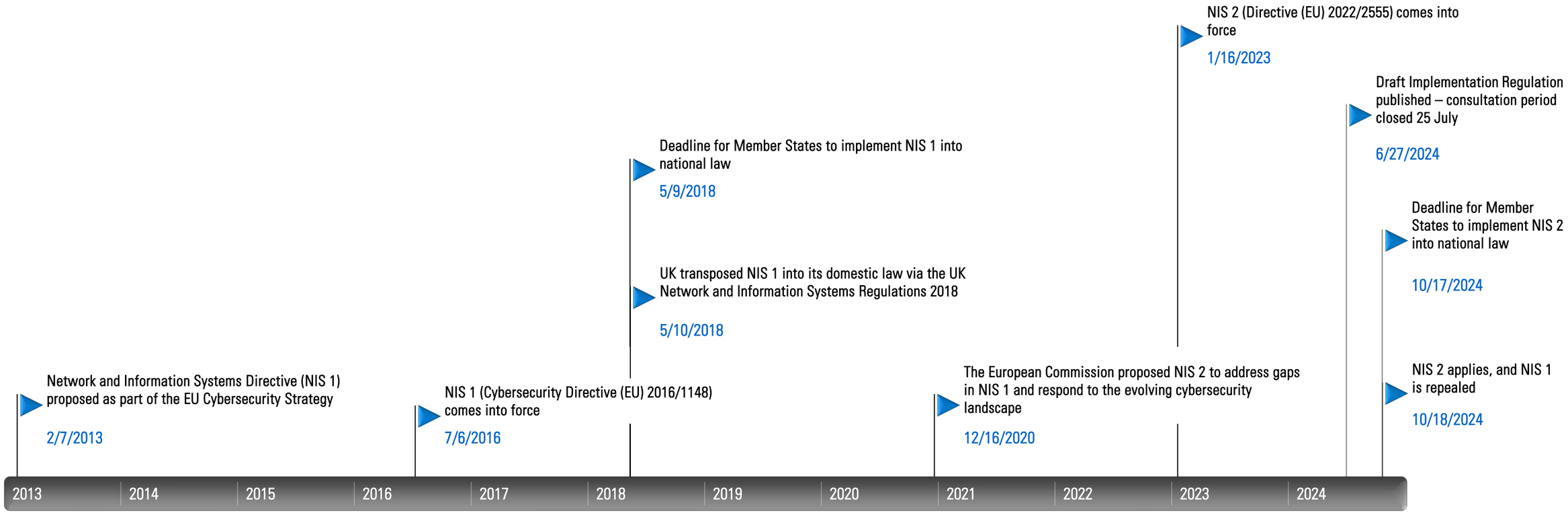
# Other GDPR Obligations Relevant to Cybersecurity

- Data Minimisation (Article 5(1)(c))
- Data Retention (Article 5(1)(e))
- Data Protection by Design and by Default (Article 25)
- Accountability (Article 5(2))
- Data Breach Notification
  - Controllers must notify supervisory authorities **without undue delay** and at least within **72 hours** of becoming aware of a personal data breach, unless it's unlikely to risk individuals' rights (Article 33).
  - If a breach is likely to result in a high risk to individuals, data subjects must also be informed without undue delay (Article 34).
  - Processors must notify controllers **without undue delay** (Article 33.2).

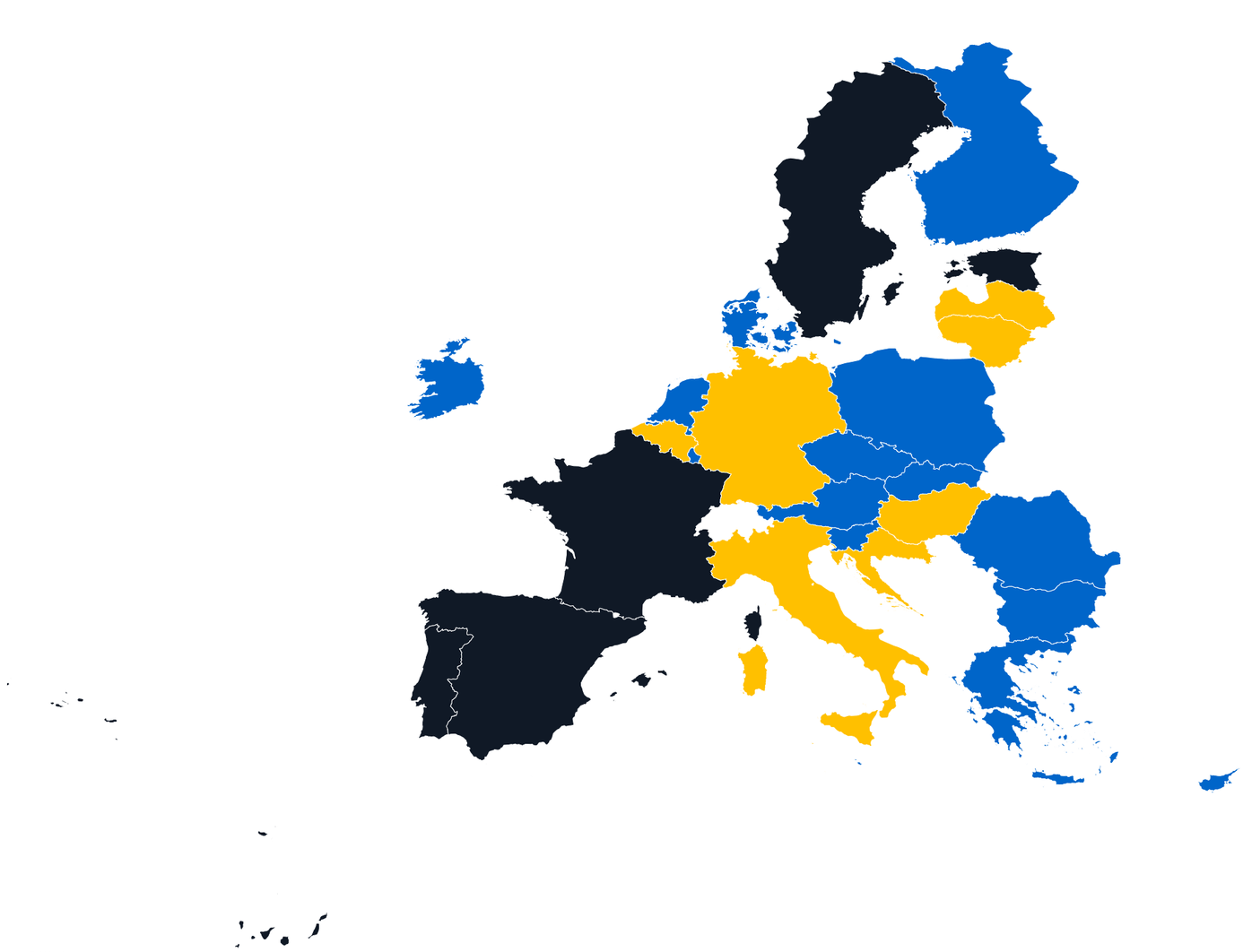
# 3. Network and Information Systems Directives (NIS)

pillsbury

# Timeline


Network and Information Systems Directive (NIS 1) proposed as part of the EU Cybersecurity Strategy
2/7/2013
NIS 1 (Cybersecurity Directive (EU) 2016/1148) comes into force
7/6/2016
Deadline for Member States to implement NIS 1 into national law
5/9/2018
UK transposed NIS 1 into its domestic law via the UK Network and Information Systems Regulations 2018
5/10/2018
The European Commission proposed NIS 2 to address gaps in NIS 1 and respond to the evolving cybersecurity landscape
12/16/2020
NIS 2 (Directive (EU) 2022/2555) comes into force
1/16/2023
Draft Implementation Regulation published – consultation period closed 25 July
6/27/2024
Deadline for Member States to implement NIS 2 into national law
10/17/2024
NIS 2 applies, and NIS 1 is repealed
10/18/2024
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024

# Status of Member State implementation




SUMMARY AS OF 30 OCTOBER 2024

**7**

Member States have implemented NIS 2

**15**

Member States have published draft laws

**5**

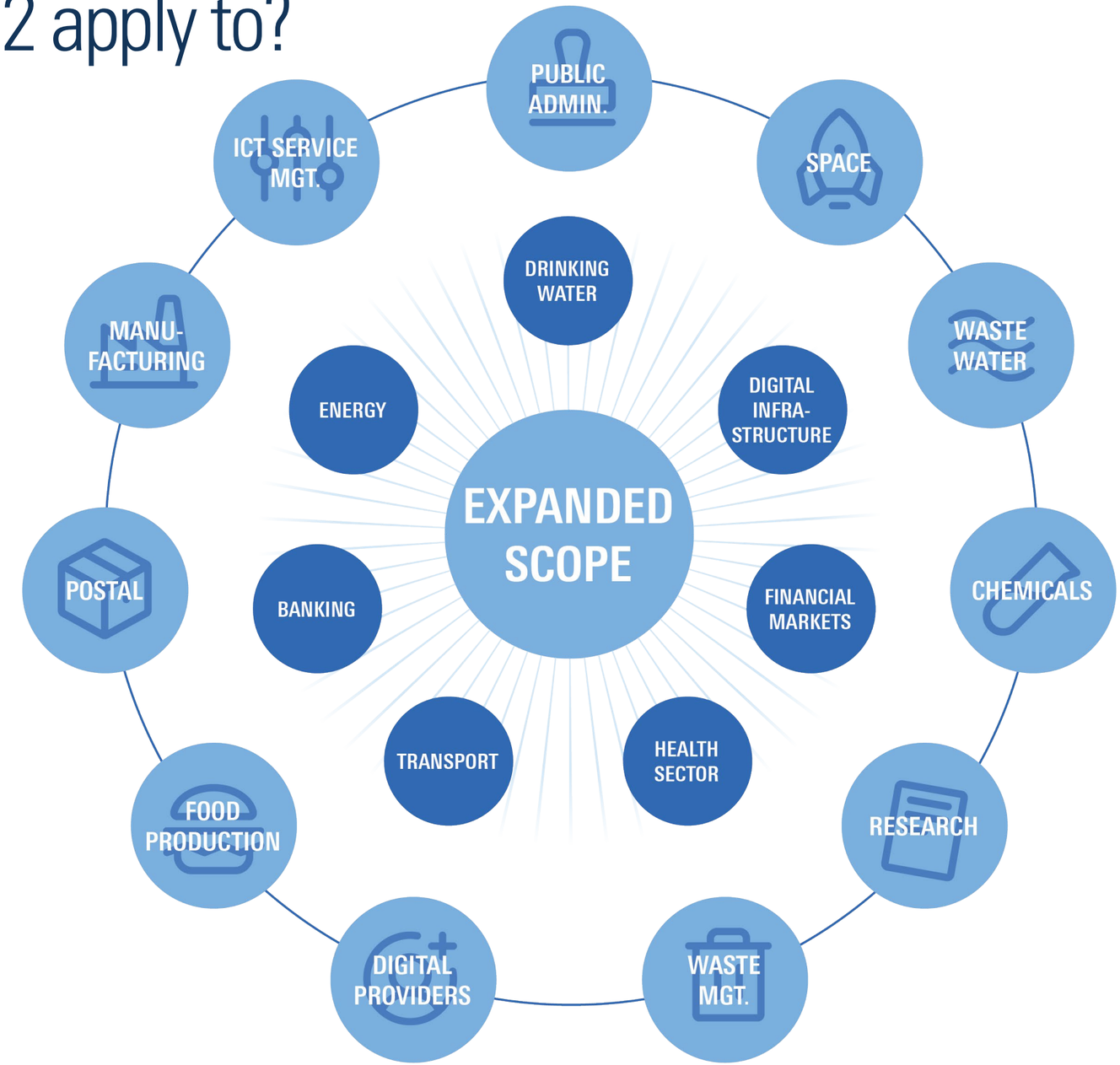
Member States have not published draft laws

# Who does NIS 2 apply to?

- NIS 2 applies to:
  1. Public or private entities operating in the sectors listed in Annex I or II to NIS 2
  2. Which qualify as medium-sized enterprises, or exceed the ceilings for medium-sized enterprises:
     - Medium-sized enterprises – employ more than 50 persons with annual turnover and/or annual balance sheet exceeds €10 million
     - Large-sized enterprises – employ more than 250 persons with annual turnover exceeding €50 million and/or annual balance sheet exceeds €43 million
  3. Provide their services or carry out their activities within the EU
- NIS 2 also applies to entities of any size, for example, if they provide certain services (e.g., electronic communications, trust services, domain names), are sole providers of critical services, or if their disruption could impact public safety, security, health, or create systemic risks.
- Member states can also apply NIS 2 to local government or schools and universities, especially if they are involved in important research work.

# Who does NIS 2 apply to?

# Who does NIS 2 apply to?



# Who does NIS 2 apply to?

# What are the jurisdiction and territoriality requirements of NIS 2?

- **General rule:**
  - Entities fall under the jurisdiction of the Member State where they are established.
- **Digital Infrastructure Providers:**
  - Jurisdiction is determined by the Member State where their “main establishment” is located in the EU.
- **Main Establishment Determination:**
  - Based on where cybersecurity risk-management decisions are made;
  - Where cybersecurity operations are carried out; or
  - Where the highest number of employees are based.
- **Non-EU Digital Infrastructure Providers :**
  - Must designate an EU representative in a Member State where services are offered.

# What are the registration requirements?

- There are two registration requirements under NIS 2, namely:
- Member state register
  - By 17 April 2025, member states must create a list of essential and important entities, updated at least every 2 years.
  - To do this, member states must require such entities to provide at least the following information to competent authorities: (i) name, (ii) address and contact details, (iv) sector and subsector; and (v) list of member states where in scope services are provided (Article 3.4).
- ENISA Register
  - By 17 January 2025, ENISA must create a list of certain providers including those operating in the digital infrastructure sectors, ICT service management and digital providers (providers of online market places, search engines and social networking services platforms).
  - Member states must require such entities to provide specific information to competent authorities by 17 January 2025.

# Required security measures

**Management Oversight (Art. 20 & 32.5)**

- Policies on risk analysis and information system security
- Incident handling
- Business continuity, such as backup management, disaster recovery and crisis management
- Supply chain security
- Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
- Policies and procedures to assess effectiveness of measures
- Basic cyber hygiene and training
- Policies and procedures regarding cryptography and encryption
- Human resources security, access controls and asset management
- MFA, secured communications and secured emergency communication systems

# How is supply chain security impacted?

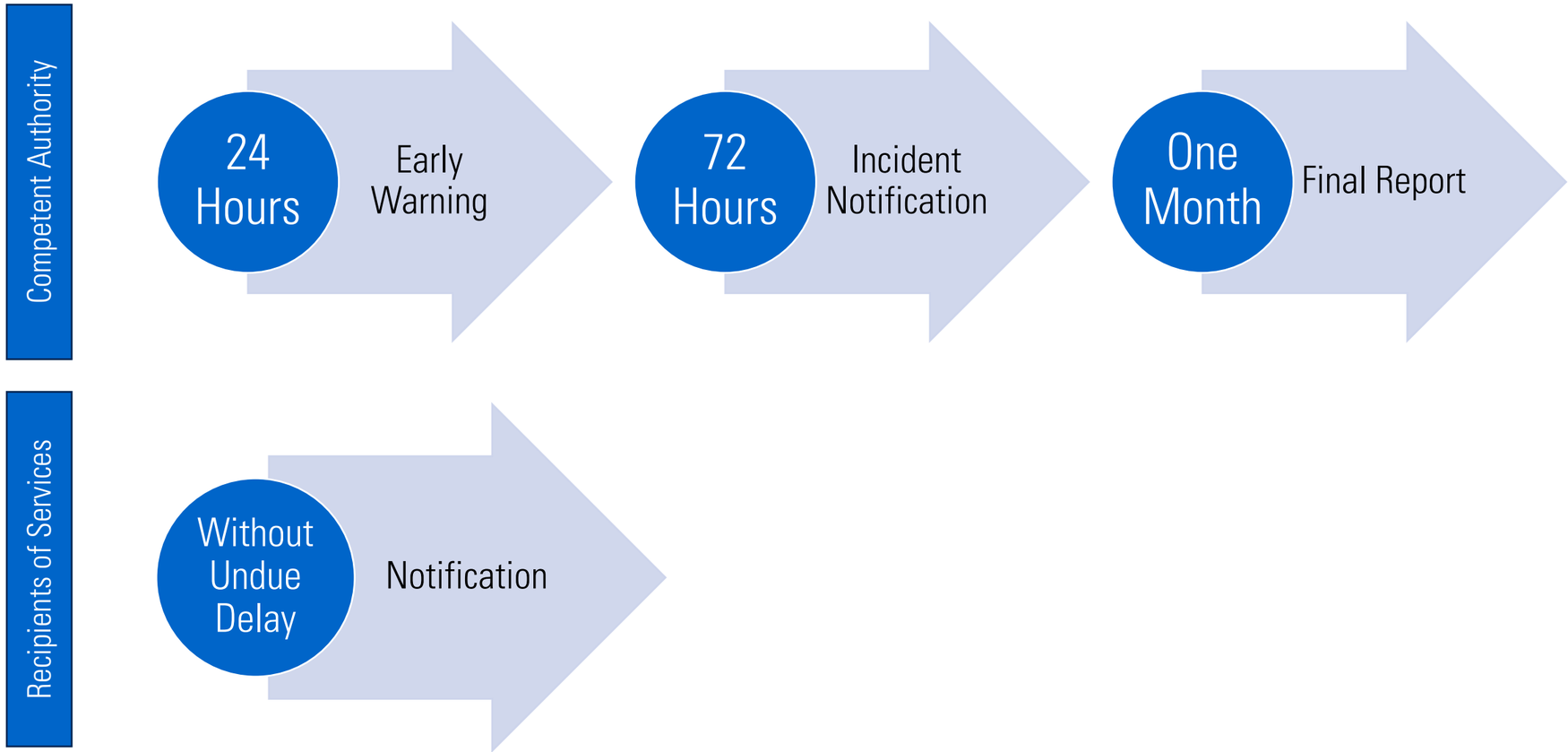
- NIS 2 has a particular focus on supply chains.
- Entities are required to implement measures relating to supply chain security.
- When considering what measures are appropriate, entities will need to take account of:
  - The vulnerabilities specific to each direct supplier and service provider.
  - The overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.
  - The results of the coordinated security risk assessments of critical supply chains carried out at the EU level.
- Practically speaking, entities will have to perform third-party security assessments and incorporate appropriate security requirements in their third-party contracts.

# What is the Implementing Regulation?

- Commission Implementing Regulation in force from 17 October 2024.
- Applies to:
  - DNS service providers, top-level domain name registries, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.
- Sets out more detail on the specific elements that must be covered in the security measures.
- Also outlines specific cases in which a security incident is considered to be significant.

# What are the incident reporting requirements?

**Incident that has "significant impact":** Any incident that: (a) has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned, or (b) has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.



# Enforcement under NIS 2

- Enforcement Powers
  - Competent authorities can inspect, audit, and request documents.
  - Essential entities face stricter measures, including the potential for certification suspensions and executive bans (not applicable to Important entities).
- Fines:
  - **Essential Entities:** Up to EUR 10 million or 2% of global turnover.
  - **Important Entities:** Up to EUR 7 million or 1.4% of global turnover.
  - Periodic penalty payments may be imposed to enforce compliance.

# Key Steps for NIS 2 Compliance

## Determine Applicability

- Identify if your organisation falls under NIS 2, and if so, (i) whether it is classified as an essential or important entity, (ii) the relevant jurisdictional scope.

## Reporting Requirements

- Identify applicable reporting requirements and deadlines.

## Review and Map Requirements

- Assess the specific obligations (cyber risk management, incident reporting) that apply and consider differences across Member States.

## Conduct a Gap Analysis

- Audit current security and incident response measures to identify gaps relative to NIS 2 requirements.

## Consider Wider Legislative Landscape

- NIS 2 should be read alongside other similar obligations (e.g., GDPR, DORA, proposed Cyber Resilience Act).

## Address Supply Chain Security

- Extend new security controls and incident reporting obligations to suppliers, as required by NIS 2. Consider contract remediation.

## Budget for Compliance Costs

- Plan for increased ICT spend, particularly if your organisation wasn't previously covered by NIS 1.

## Implement Staff Training

- Conduct regular training for staff at all levels to build cyber awareness and ensure compliance with NIS 2.

# 4. Digital Operational Resilience Act ("DORA")

pillsbury

# What is DORA?

- The Digital Operational Resilience Act (DORA) is an EU regulation that entered into force on January 16, 2023 – it will apply from January 17, 2025
- Strengthens the IT security of financial entities such as banks, insurance companies and investment firms, and makes sure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption
- Harmonizes the rules relating to operational resilience for the financial sector applying to different types of financial entities and information and communication technologies (ICT) third-party service providers, seeking to mitigate attacks and other risks, such as supplier failure, service deterioration and concentration risk

# Key Pillars

| | |
|---|---|
| ICT risk management | Principles and requirements on ICT risk management framework |
| ICT third-party risk management | Monitoring third-party risk providers<br>Key contractual provisions |
| Resilience testing | Basic and advanced testing |
| ICT-related incidents | General requirements<br>Reporting of major ICT-related incidents |
| Information sharing | Exchange of information and intelligence on cyber threats |
| Oversight of critical third parties | Oversight framework for critical ICT third-party providers |

# “Criticality” definitions

- “Critical” ICT provider
  - Critical third-party service providers (CTPPs) will be subject to direct regulatory oversight by the European Supervisory Authorities (ESAs)
  - ESAs will designate the CTPPs based on criteria relating to the systemic impact of the quality of financial services should the ICT provider face a large-scale operational failure and financial entities’ reliance on the same ICT providers
- “Critical or important function”
  - Disruption of the function would materially impair the financial performance of the client, or the soundness or continuity of the client’s services and activities
  - Defective performance of the function would materially impair the client’s continued compliance with its regulated status or compliance with law

# Financial Entities: Operational Compliance

## Vendor Communication

- Preparation of DORA-specific questionnaires to understand vendor intentions around compliance
- Questionnaires could range from a simple ask of whether vendors expect to fall within the scope of DORA, to detailed assessments

## Compliance Checks

- Conduct risk management exercises in collaboration with vendors
- May include penetration testing and visibility and understanding of supply chains

## Risk Register

- Placement of vendors on a risk register
- DORA-related risks identified will require remediation, involving further discussion and collaboration with vendors

# Financial Entities: Contracts Compliance

- Content requirements imposed for all ICT services contractual arrangements between financial entities and ICT providers
- An additional set of mandatory provisions are required for contracts where the ICT provider's services support the financial entity's critical or important functions
- DORA compliance project is needed which will likely involve a gap analysis and repapering of a number of ICT contracts

# Approach for ICT Providers

- Categorization: Assessment of services (critical/important or not)
- Client communications: Prepare due diligence/RFP responses; whitepapers
- Discovery and mapping: Identify and locate all client contracts that are categorized as ICT services, review and categorize them according to DORA requirements
- Gap analysis: Identify the gaps in compliance with DORA contractual requirements
- Remediation: Create DORA addendum/standard clauses
- Negotiation

# Summary of DORA Implications

- Governance and Accountability
- Investment in Resilience Capabilities
- Collaboration and Information Sharing
- Third-Party Risk Management
- Regulatory Oversight and Enforcement

# 5. Key U.S. Cybersecurity Legislation for UK/EU Companies

pillsbury

# Key U.S. Cybersecurity Legislation for UK/EU Companies

- **Computer Fraud and Abuse Act**
- **Defend Trade Secrets Act**
- **Cybersecurity Information Sharing Act (CISA):** Encourages threat information sharing between private companies and the federal government.
- **Federal Information Security Management Act (FISMA):** Requires federal agencies and contractors to secure information systems and report security practices.
- **Health Insurance Portability and Accountability Act (HIPAA):** Establishes standards for protecting sensitive patient health information.
- **Gramm-Leach-Bliley Act (GLBA):** Mandates financial institutions to protect consumers' personal financial information.
- **California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA):** Grants California residents rights over their personal data and imposes obligations on businesses.
- And so on…

# 6. Key Takeaways

pillsbury

# Key Takeaways – Common Themes

- Harmonization of standards
- Strengthening of institutions
- Risk management
- Accountability
- Focus on critical infrastructure
- Awareness and training

# Key Takeaways

**Conduct Analysis**: Undertake an analysis to identify applicable cybersecurity laws affecting your business activities, including those currently in force and upcoming regulations.

**Perform Gap Analysis**: Assess your current security posture against the identified laws to pinpoint areas for improvement.

**Remediate Gaps**: Address any gaps by implementing necessary policies/response plans and ensuring that existing security accreditations align with UK/EU requirements.

**Registration and Notification Obligations**: Consider if any registration or notification obligations apply to your business.

**Raising Awareness and Ongoing Monitoring**: Ensure readiness for potential incidents via training and raising awareness of threats and escalation procedures. Implement ongoing audit procedures.

**Supply Chain Due Diligence**: Evaluate supply chain due diligence requirements and take necessary steps to remediate contractual agreements with suppliers.

pillsbury

# Questions?