All-Party Parliamentary Group on Cyber Security and Business Resilience

Legislative change and the UK position

David Cook
11 December 2024

DLA PIPER

Cyber Security and Resilience Bill

What has been said?

Cyber Security and Resilience Bill

“The existing UK regulations reflect law inherited from the EU and are the UK’s only cross-sector cyber security legislation. They have now been superseded in the EU and require urgent update in the UK to ensure that our infrastructure and economy is not comparably more vulnerable.”

Kings Speech, 17 July 2024

This relates to the EU NIS Directive, transposed into UK law via the NIS Regulations 2018.

NIS is intended to establish a common level of security for network and information systems. It applies to two groups of organisations: ‘operators of essential services’ (OES) and ‘relevant digital service providers’ (RDSPs).

Cyber Security and Resilience Bill

"The Bill will make crucial updates to the legacy regulatory framework by:

- *expanding the remit of the regulation to protect more digital services and supply chains. These are an increasingly attractive threat vector for attackers. This Bill will fill an immediate gap in our defences and prevent similar attacks experienced by critical public services in the UK, such as the recent ransomware attack impacting London hospitals.*

- *putting regulators on a strong footing to ensure essential cyber safety measures are being implemented. This would include potential cost recovery mechanisms to provide resources to regulators and providing powers to proactively investigate potential vulnerabilities.*

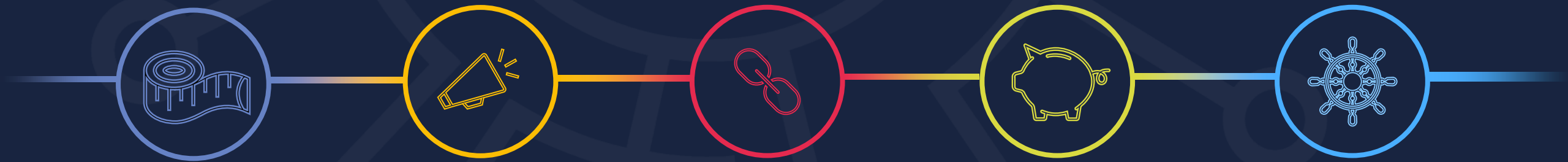
- *mandating increased incident reporting to give government better data on cyber attacks, including where a company has been held to ransom. This will improve our understanding of the threats and alert us to potential attacks by expanding the type and nature of incidents that regulated entities must report."*

Directive on measures for a high common level of cybersecurity across the Union, Directive (EU) 2022/2555 – the NIS2 Directive

Looking for the signposts

How does NIS2 differ from its predecessors?

Key changes to the new regime



Significantly widened scope

Shift to **Essential and Important** entities

Application to **greater number of sectors**

Enhanced reporting

Reporting of significant incidents in three tranches: **24 hrs / 72 hrs / 1 month**.

Supply chain due diligence

Cybersecurity risk management measures require In scope organisations to have thorough understanding of **cyber robustness of supply chain**

Increased fines and enforcement

Fines up to **€10 m/ 2% global turnover** (or €7m/ 1.4% global turnover)

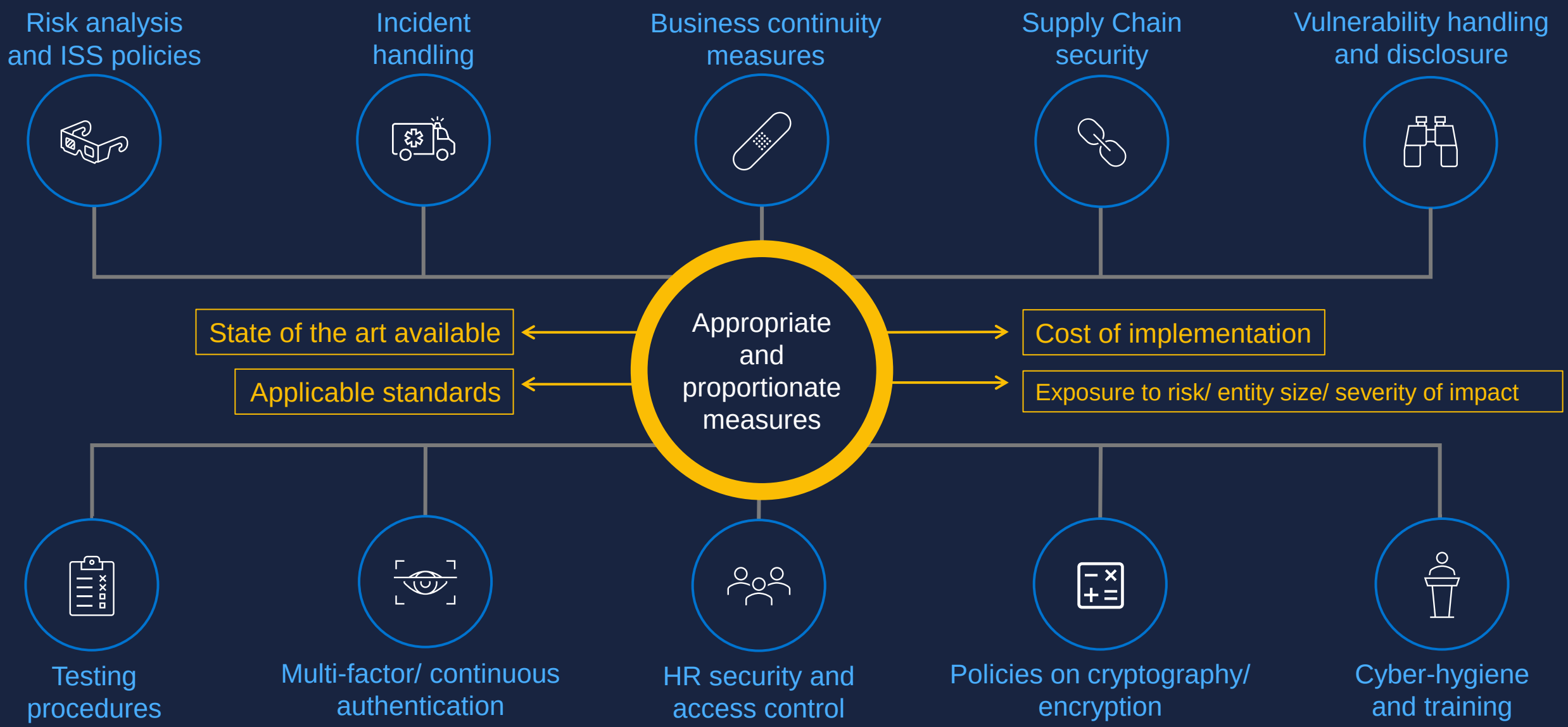
Proactive/ reactive enforcement including **audits, rights of information and temporary suspension** of management

Management obligations

Enhanced responsibility for approving cybersecurity risk management measures.

Potential **personal liability** for management

NIS2 | Cyber security risk management measures



Divergence or alignment?

Commercially disadvantageous to not align wherever we can do. Cyber security and digital networks, and the associated risks, pervade national borders. A short-term competitive advantage is likely to lead to a long-term net loss to the UK.

Multinational organisations will have lots of laws to comply with and so tend to benchmark against the highest standard applied in any one jurisdiction across all jurisdictions in which they operate. No benefit to the UK to impose a lower standard.

Specific areas to concentrate alignment:

- Cyber security controls
- Reporting obligations

Specific areas where divergence might be possible:

- Governance and oversight
- Liability
- Supply chains
- Contracts

EU Digital Decade

Looking at the bigger picture

What is the EU Digital Decade?

The EU's comprehensive framework underpinning all actions related to sustainable digital transformation in Europe ensuring technology and innovation work for people

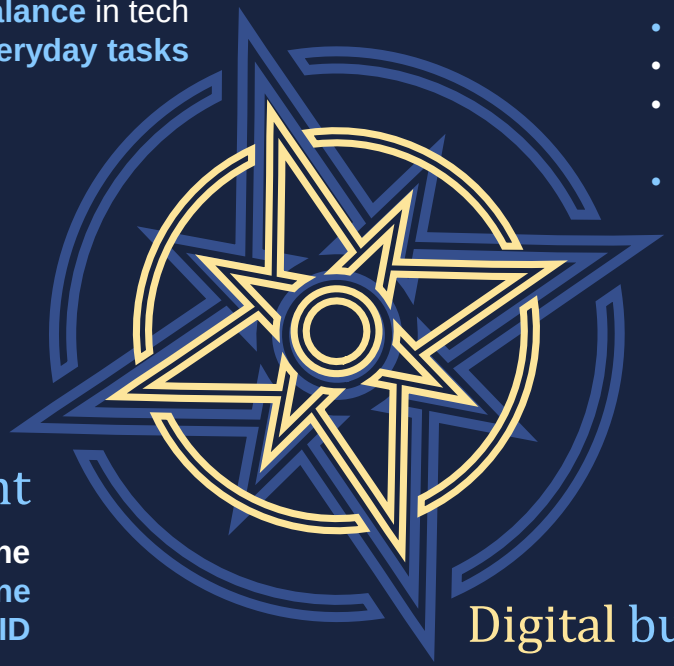
Key targets for 2030

Digital skills

- 20 million+ employed **ICT specialists**
- More **ICT graduates**
- Better **gender balance** in tech
- 80% of adults using tech for **everyday tasks**

Digital infrastructure

- **Gigabit connectivity** for everyone
- **High-speed 5G mobile coverage** everywhere
- EU production of **20% of world's semiconductors**
- 10,000 **climate-neutral**, highly secure cloud edge notes to ensure **fast data access**
- **EU quantum computing** by 2025



Digital government

- **Key public services** should be **100% online**
- Everyone can access **health records online**
- Everyone can use **eID**

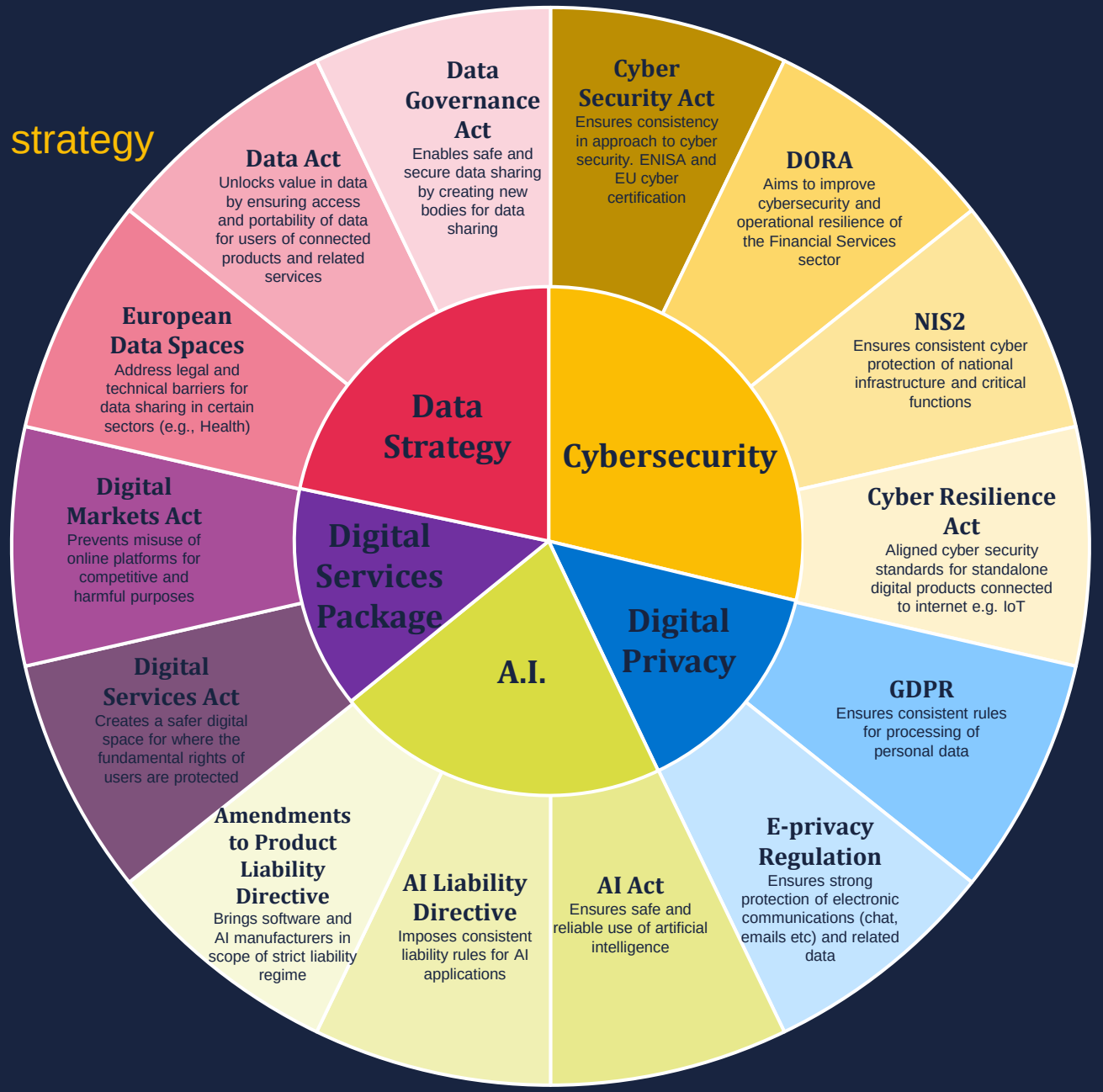
Digital business

- 75% of companies using **Cloud, AI or Big Data**
- Double the number of **unicorn startups**
- 90% of **SMEs taking up tech**

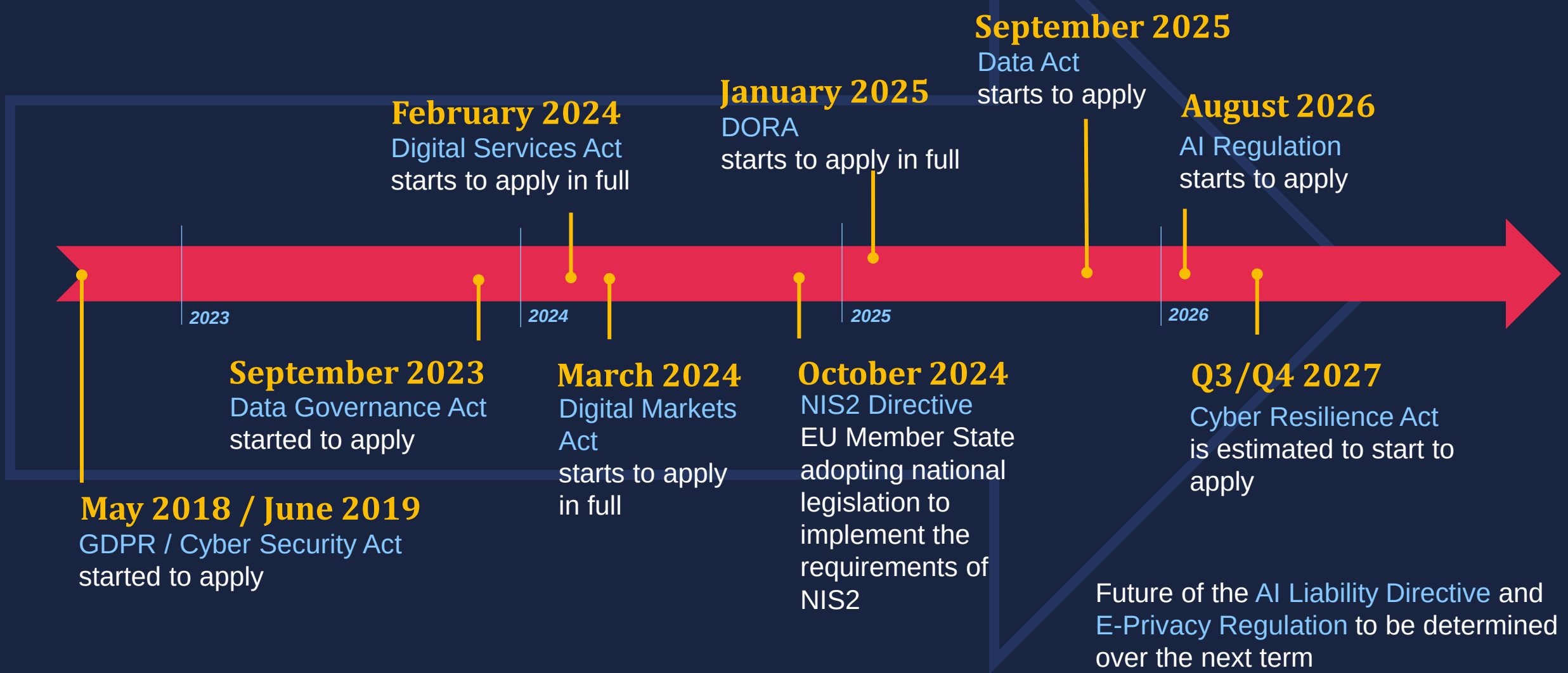
Legal Framework

Legislative initiatives enabling Digital Decade strategy

Aimed at supporting the EU's Digital Decade strategy, which is projected to add €270 billion annually to EU GDP by 2028



Timetable for the adoption of the legal framework



Thank you.