Nordic region

NIS2 and Beyond: Evolving Cybersecurity Priorities in the Nordic Region

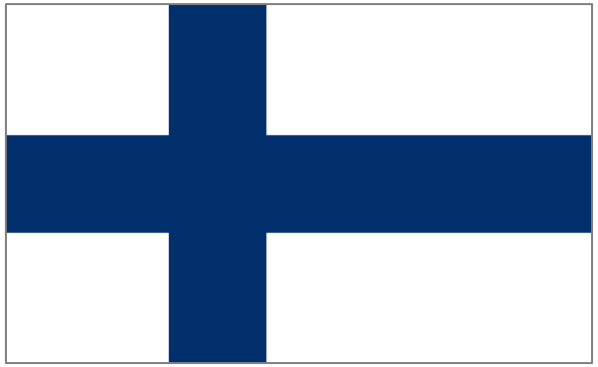
PECB REGIONAL WEBINARS

Agenda

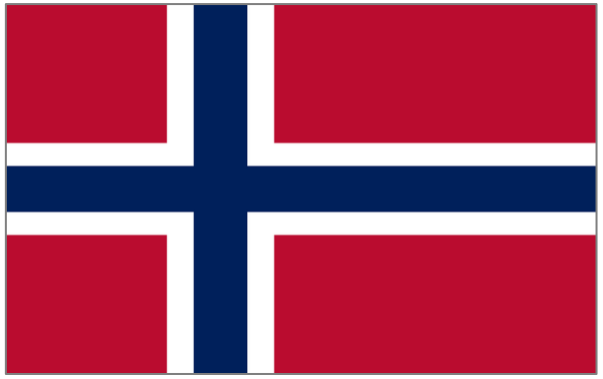
1. NIS2: Where are we now?
2. The Challenges
3. The Next Big Thing

1. NIS2: Where are we now? The Nordics

- Not transposed nor in hearing.
- Expected to be sent in hearing later this year.

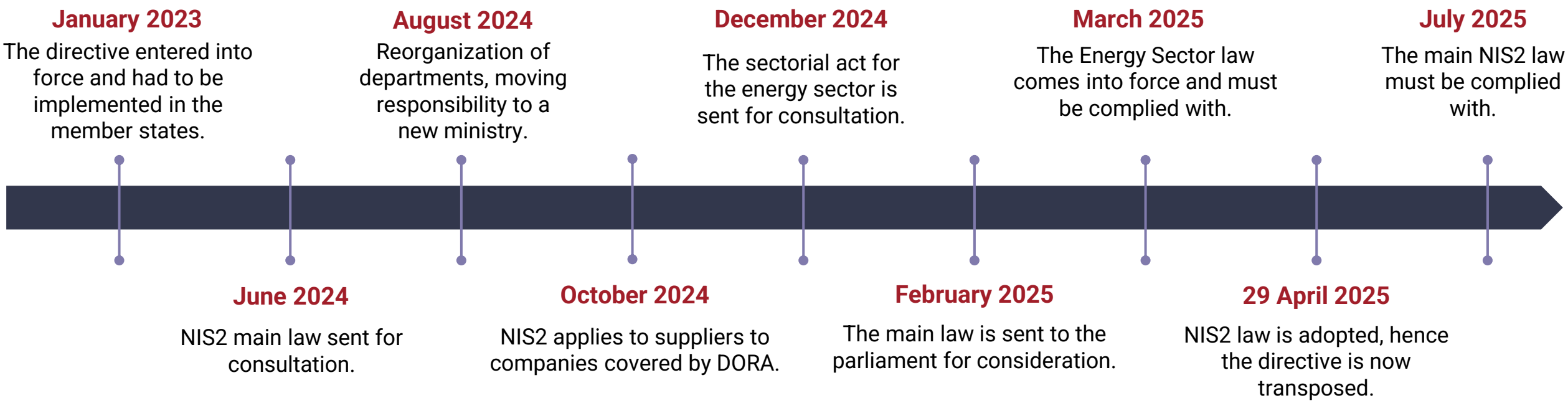


- The Cybersecurity Act entered into force on April 8, 2025.
- The compliance journey for organizations continues into 2026.



- No date set for the implementation of NIS2.
- The National Security Authority states that it will happen during 2026.

1. NIS2: where are we now? Denmark



1. NIS2: Where are we now? Denmark

Guidelines from the Danish primary authority:

On the general scope of the directive:

On the governance:

On the Cybersecurity risk-management measures:

1. NIS2: where are we now? Denmark

New scope on systems:

"Article 21(1), second subparagraph, of Directive (EU) 2022/2555 specifies how the proportionality of such measures should be assessed. The obligation laid down in Article 21(1) of Directive (EU) 2022/2555 requiring essential and important entities to take appropriate and proportionate cybersecurity risk-management measures refers to all operations and services of the entity concerned, not only to specific information technology ('IT') assets or critical services that the entity provides.

1. NIS2: where are we now? Denmark

What does this new scope mean for entities covered by NIS2 in Denmark?

Risk assessments:

- Everything needs some sort of screening or risk assessment.

Documentation:

- Everything need documentation of what has been done.

Mitigation:

- All risks need to be identified and treated.

Vendors:

- Every vendor needs to be assessed on criticality.

1. NIS2: Where are we now? Denmark

The Danish definition of management bodies from Article 20:

Private companies:

The Board of Directors;
The Executive board;
The part that is most akin to the Executive Board.

Public Authorities:

The top administrative management in the authority;
Usually the Executive Board.

1. NIS2: Where are we now? Denmark

The requirements for the management bodies from Article 20:

Relevant courses can be general courses on cyber and information security, management courses and workshops on managing cyber and information security risks, courses and certifications in recognized European and international security standards or the unit's own internally organized courses and seminars on cyber and information security targeted at management.

1. NIS2: Where are we now? Denmark

Article 20 acceptable examples:

*On the **board of directors of a private company**, two of the members have knowledge of strategic management of cyber and information security. One of the members has completed a board training course focusing on managing cyber security risks. The other board member has a certification in a relevant security standard.*

*In a **public authority**, a half-day seminar is held once a year for the members of the authority's cyber and information security committee, which includes representatives from the executive board (management body). The authority itself has organized the seminar, which focuses on the threat landscape, risk management and strategic management of cyber and information security in public authorities.*

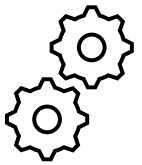
2. The challenges

Rise of the hybrid threat

Aiming at destruction

Utility and public sector as ground zero

Skills gap



OT-security

2. The challenges: Hybrid threats

The Nordic countries become targets of not just cyber warfare, but also **hybrid warfare**.

Examples include **gas pipelines and unidentified drones** around nuclear power plants or military installation.

NIS2 has an **all-hazards approach to risk assessments and CER has a focus on physical security**, but are we up to the task?

- In the physical realm we mostly see security around continuity.
- We see very little focus on how hybrid threats can affect our systems or services.
- Most of us lack the experience to combine the digital and physical.

2. The challenges: Destruction

Many of our clients see much more **scouting and probing instead of quick encryption** with malware.

We also see attacks aimed at **disruption or destruction**, instead of just money.

How do we deal with threat actors, that are **motivated by something other than money**?

- We have a higher focus on disaster recovery and on discovery part of NIST CSF.
- Redundancies used to be only for the large companies, but even medium-sized companies are now looking into more redundancy for the infrastructure that supports their services.

2. The challenges: Utility and public sector

Our clients in the utility sector and public sector have all experienced a **major shift in threat actors and attacks.**

After the Russian invasion, clients have seen a **huge increase in attacks, attackers and the level of sophistication** of those attackers.

- Some companies within water and electricity especially have seen attacks increase by a factor of 20-30 in the last three years.
- We see attacks directed at public authorities, with the sole purpose of disrupting their services and cause fear in the population, as with the recent attacks on SVT.
- When state-sponsored actors or state- backed criminal groups attack based on political motives, sectors similar to the public sector and utility sector need to increase their threat-based security.

2. The challenges: Skills gap

Our clients often **lack the necessary skills and resources to establish and maintain the right governance** to implement and comply with NIS2, AI Act, CRA etc., and we need to support with ISO/IEC 27001 and ISO/IEC 2700x in general.

What we need, and what the clients need, **are more people with experience, including certifications.**

- It helps if you have a strong foundation for your security, so new regulation can be mapped into it and the gaps are easier to identify. Certifications in demand are:
  - ISO/IEC 27001/27002
  - ISO/IEC 27005
  - ISO/IEC 27031
  - ISO/IEC 27035

2. The challenges: OT-security

We see the biggest gap in OT-security; both when it comes to skills and level of security.

OT-security is in some ways rather different from IT-security, where the **focus is on safety,** as OT can physically hurt people, if the safety isn't in place.

- In Denmark the lack of OT-security professionals have made some big companies start their own OT-security education to make up for the lack of available hands in the area.
- We would really like to see a bigger focus on IEC 62443 and similar standards, and more people with certifications within the area.

3. The next big thing

Cloud sovereignty

And even more regulation

3. The Next Big Thing: Cloud sovereignty

The ICC-case has scared many decision-makers.

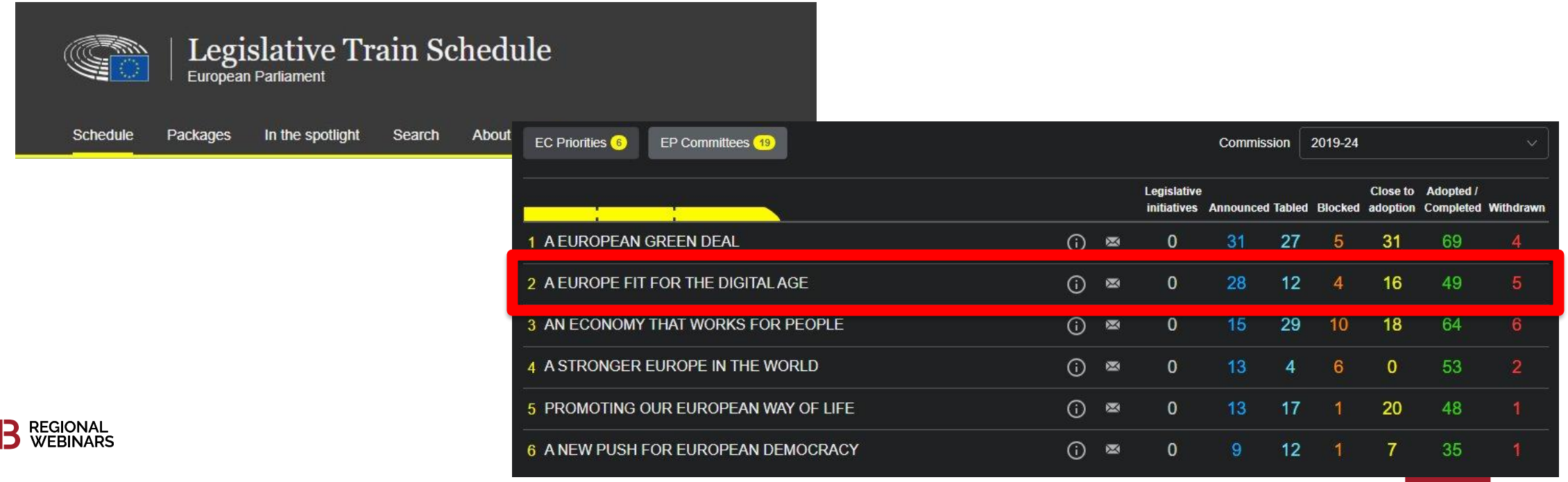
In Denmark, large companies and public authorities are focusing on:

- Vendor lock-in.
- How American software services can be used as leverage against European companies or states.
- Alternatives in infrastructure, platform and services – some can easily be replaced, others can’t.

3. The next big thing: Regulation

While still working on implementing NIS2, DORA, and even GDPR, new regulations are coming our way, including:

- AI Act
- CRA
- … and more to come, especially within Digital and Compliance



3. The next big thing: Regulation

S = Strategy
R = Regulation
D = Directive

New “rules” since 2019 – from EU’s Digital Decade.

Cyber security

- **S: Cybersecurity Strategy**
- R: Cybersecurity Act
- D: NIS2
- R: DORA
- D: Critical Entities Resilience/CER
- R: Cybersecurity Regulation
- R: Cyber Resilience Act
- R: Cyber Solidarity Act
- R: Information Security Regulation

Data (access & sharing)

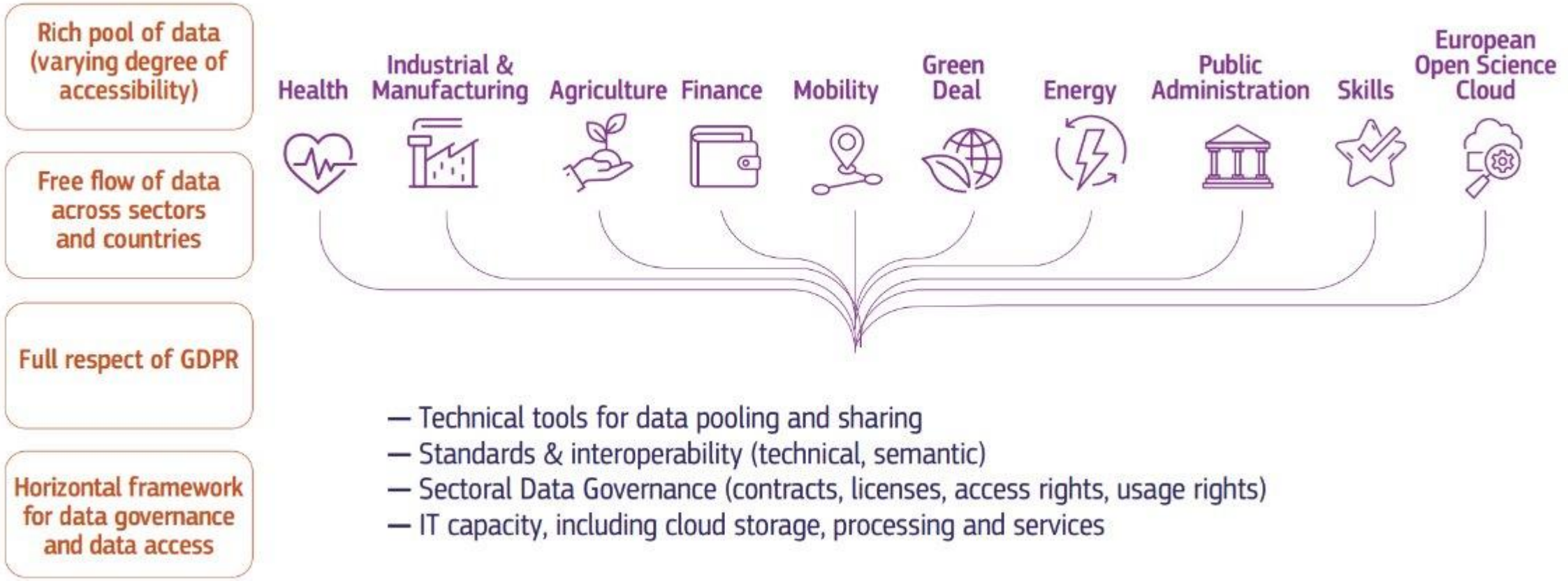
S: Data Strategy
R: Free Flow of Data
D: Open Data
R: Data Governance Act
R: Data Act
R: Interoperable Europe Act
R: Data Collection and Sharing Relating to Short-Term Accommodation Rental Services Act (!)
R: European Health Data Space
R: Financial Data Access

Tech & responsibility

S: AI Strategy + Blockchain Strategy
R: Platform-to-Business regulation/P2B
R: Digital Services Act
R: Digital Markets Act
R: MICA (crypto assets)
R: AI Act
R: European Identity Wallet (!)
R: Machinery Regulation
D: Product Liability Directive (revision)
F: General Product Safety Regulation

3. The Next Big Thing: Regulation

EU data spaces.



Q&A Session

Contact

- Website: www.globeteam.com
- Phone: +45 29 72 46 10
- Email: men@globeteam.com

For any questions or comments, you can contact us below:

- support@pecb.com