Agenda – Nordic-Baltic coordination network on regulatory issues

21. -22. March 2024, (11:00 – 17:30, 09:30 – 15:30)

Venue: Eteläesplanadi 4, meeting room 5

Participants:

Denmark	Latvia (Digital)	Sweden
Finland	Lithuania (Digital)	Aaland Island
Iceland	Norway	

Thursday 21. March

Time	Annotation
Data Act: Competent Authority	**Introduction and Framing** The workshop focused on national implementation of the Data Act, which entered into force on 11 January 2024 and will be applicable from September 2025. The DA establishes rules on access to and use of data across sectors in the EU, aiming to promote fairness, innovation, and accessibility. The session was divided into two thematic tracks, with a primary emphasis on **Competent Authorities (CAs)**. The workshop used a **carousel method**, where participants rotated through stations to explore five core questions. The following sections summarise the carousel input and plenary discussions. **Track One: Competent Authorities** **Defining Eligible Entities** Participants identified a wide range of potential candidates for CAs within their countries. These included telecommunications and digital agencies, competition and consumer authorities, statistical agencies, data protection bodies, sectoral regulators, and several ministries. The brainstorming was exploratory and did not reflect formal national mandates. Some members noted the limited pool of potential entities in smaller countries, leading to recurring mentions of the same candidates. The possibility of sector-specific versus general CAs was debated. In Denmark, for instance, the DA is interpreted as general in scope, and a single CA (Digitaliseringsstyrelsen) may take on both CA and Data Coordinator (DC) roles. In Sweden, Digg is not under consideration, being seen as closer to the Post and Telecom Authority. Country-specific insights included: • **Finland**: Undecided; leading candidates are the Transport and Communications Authority, Data Protection Authority, and Consumer Protection Authority. • **Latvia**: Ministry of Environmental Protection and Regional Development designated as Data Coordinator; CA not yet chosen. A collegial body is being considered. • **Lithuania**: Multiple institutions involved; plan to form a collegial institution for coordination.

Time	Annotation
	The European Commission has encouraged Member States to consider using the same authority for both the DA and the DGA to streamline coordination and participation in the European Data Innovation Board (EDIB). This would also prevent overcomplication of the EDIB and encourage sectoral knowledge exchange. The EC also urged NCAs to take active roles nationally and ensure they are empowered to represent their countries in the EDIB. A key unknown is the **volume of complaints** the DA will generate—expected to differ from the DGA. This uncertainty complicates planning for CAs. **Technical and Organisational Competencies Needed** The DA implies wide-ranging technical needs for CAs. Participants highlighted required competencies such as: • **Cybersecurity, IoT, cloud services, IT operations** • **Data protection, interoperability standards, technical architecture** • **AI-related data extraction and documentation** • **Infrastructure for online publication of public sector data access requests** • **System integration between public and private sectors** Additional needs include: • **Communication and guidance skills** • **Understanding data markets, ecosystems, and business models** • **Capacity for cross-sector and international coordination** • **Human, financial, and infrastructure resources** The governance structure and internal culture of candidate authorities were also seen as crucial to successful implementation. **Legal Expertise Requirements** Legal knowledge areas required include: • **Data and communications law** • **GDPR and IP law** • **EU law and sector-specific regulations** • **Contract law, including international private law** • **Emergency legislation, consumer law, public administration law** • **Human rights protections and the value of data from a consumer perspective** "Soft skills" like communication of legal concepts, clarity on penalties, and the capacity to provide legal guidance were also mentioned. **Data Coordinator – Who and Why?** Participants reflected on suitable candidates for the role of **Data Coordinator (DC)** under the DA. Suggested options overlapped with those for the CA role, but additional attention was paid to cross-sectoral coordination capabilities and EU-level experience. Key considerations included: • **Technical and legal proficiency** • **Track record in managing EU regulations** • **Familiarity with IoT and data access contexts** • **Institutional mandate and neutrality** Specific suggestions: • **Finland**: Likely to appoint the same CA as for the DGA (though not yet final). • **Latvia**: Ministry of Environmental Protection and Regional Development.

Time	Annotation
	• **Lithuania**: National Data Agency among the options. The role is expected to focus heavily on issues related to **IoT and switching** and not on the exceptional needs regime, which is viewed as a state-level matter. **Exceptional Need (Chapter 5 DA)** The group discussed what may constitute an "exceptional need" for public sector access to data: • The situation must be **specific, unforeseen**, and **non-personal**. • **Non-emergency cases** are included, but only when other means are exhausted. • Situations must be **limited in time** and often require formal national crisis declarations. • **Examples**: virus outbreaks (COVID-19), wars, and natural disasters. • The DA is primarily expected to apply in **cross-border contexts**, complementing national legislation. Members noted that most countries already have legal bases for crisis declarations, so the added value of Chapter 5 lies in enabling access across borders. **Data Innovation Board and Coordination** Members acknowledged that the **scale and approach to sanctions** under the DGA—and likely under the DA—differ considerably across countries. NoBaReg may play a valuable role in promoting **regional harmonisation**, especially in terms of coordination and interpretation. While such alignment is difficult without a formal mandate, NoBaReg offers a practical forum for mutual understanding and progress.

AIA – Track One: Competent Authorities (CA)

Setting the Context

As per Article 59(2) of the AI Act, Member States must designate at least one notifying authority and one market surveillance authority. According to paragraph 4 of the same article, these authorities must be equipped with sufficient technical, legal, financial, and human resources. Their staff should have expertise in AI technologies, data protection, cybersecurity, fundamental rights, and sectoral knowledge (e.g., health and safety risks).

T

he European Commission, according to *Euronews* reporting on 3 April, is actively encouraging national governments to appoint AI regulators ahead of full enforcement. Letters will be sent requesting these appointments, with a 12-month timeline for setup. The appointed bodies will form the **AI Board**, which is expected to harmonise AI regulation across the EU.

Nobareg proposes to begin by mapping the expected competencies for such authorities, followed by a discussion on the structural arrangements: Should there be one central authority or multiple sectoral ones? How should collaboration be ensured?

Miro Board Transcript

Notifying Authority

Eligible Institutions	**Competences Needed**
Norsk Akredditering	Development of software
Finnish Accreditation Service (Finas)	Deep understanding of the AIA
Icelandic Board for Technical Accreditation	Product safety legislation-ish
Swedac	Knowledge of AI, Health and safety risks, IT, fundamental rights
-	Data protection, cybersecurity, risk management and procedures

Market Surveillance Authority

Eligible Institutions	**Competences Needed**
Sectoral authorities, with one SPOC	Sectoral knowledge, public digitalisation, health, finance
Communication technology agencies	Imposing significant fines
Data Protection Authorities (when mandated)	Broad oversight of fundamental rights

Competent Authority

Eligible Institutions	**Competences Needed**
Equality/discrimination ombud	-
Data Protection Authority	Challenges noted with DPA role
	-
-	

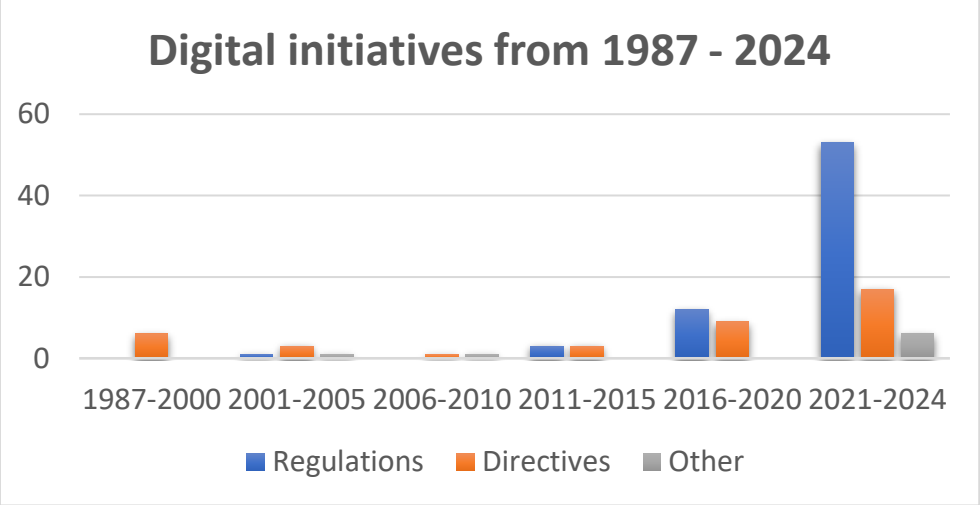
Time	Annotation
	Single Point of Contact **Eligible Institutions** — **Competences Needed** Nkom and/or DSB (also mentioned for Finland) — Public administration law - — Challenges noted with DPA role **Key Discussion Points** • The group debated whether **Data Protection Authorities (DPAs)** are suitable for broader AI oversight roles. While they are natural candidates for legal oversight, concerns were raised about whether they could support **responsible innovation**, which the AI Act encourages. Some members noted DPAs may default to stricter "approval/disapproval" approaches due to their current mandates. • A potential challenge was identified in **guidance to consumers**: if a citizen encounters a possibly illegal AI product, which authority should they contact? While some countries have mechanisms for redirection, this is not reflected in the AI Act. • **Resource allocation** emerged as a critical concern. Scarce resources must be strategically distributed among the authorities involved. The AI Act mandates that **Single Points of Contact (SPOCs)** be part of the market surveillance authority structure, adding further weight to their responsibilities.

Time	Annotation
AIA – track two: Regulatory Sandboxes	**Setting the Context** Regulatory Sandboxes (RS) are covered under Article 53 of the AI Act. These may be set up individually or jointly by Member States. A forthcoming implementing act will establish rules on their structure and operations to avoid fragmentation across the EU. Nobareg hosted **Yordanka Ivanova**, policy officer from DG CNECT (Unit A2), for this session. Her presentation was followed by a brief Q&A. Open Questions and Legal Ambiguities A key issue raised by members was whether regulatory sandboxes must offer legal exemptions to be compliant with the AI Act. This question stemmed from different national practices. For instance, Norway has a sandbox for archives that explicitly includes legal exemptions. However, the AIA itself does not clearly state that sandboxes must function this way. An email to DG CNECT in advance sought clarification on this point, referencing the use of "comfort from enforcement" in the Commission's presentation. A second uncertainty relates to penalty regimes: If participants are exempt from AIA-related fines during sandbox participation, does this also apply to potential GDPR penalties? The answer could have substantial legal and financial consequences. Q&A with DG CNECT Q: How should differences between AIA Art. 3(55) and Art. 57 on RS roles be interpreted? A: The Commission does not perceive these articles as contradictory; Article 57 may have a stronger focus on legal uncertainty. Q: Do RS participants have legal immunity during or after participation if they follow guidance in good faith? A: RS offer a "safe space" from administrative fines if guidance is followed. Civil liability remains unaffected. Authorities must account for this when performing oversight. Q: Spanish RS only admit entities established in Spain. How does this align with Art. 53, which allows joint sandboxes? A: Common rules will be clarified through an upcoming implementing act. A working group with Member States is already active, including Norway. Q: How to manage confidentiality (e.g. IP) in RS while ensuring learnings are shared? A: Confidential business info must be protected, but exit reports are mandatory (AIA Art. 57(7)(8) & Art. 58(1)) to ensure knowledge transfer. Q: Should public sector bodies providing high-risk AI systems be deprioritised in RS? A: SMEs have priority due to resource constraints but must still meet eligibility criteria.

Friday 22. March

Topic	Annotation
Common values are a part of our mandate: How do we report back to the NMR on this topic?	**Common Values Shaping Cooperation** The session began with a thematic overview of the values shared by the Nordic and Baltic countries, highlighting the cultural, historical, and societal foundations that underpin cooperation in NoBaReg. While each country maintains its unique characteristics, the following values were identified as broadly common across the region: • **Social Welfare**: A collective commitment to healthcare, education, and social services. • **Equality**: Strong emphasis on gender equality and socioeconomic fairness. • **Democracy and Rule of Law**: Robust democratic institutions and governance based on legal accountability. • **Environmental Sustainability**: Proactive environmental protection and climate strategies. • **Education**: Prioritisation of quality education and lifelong learning. • **Trust and Social Cohesion**: High levels of mutual trust, both domestically and across borders. • **Work-Life Balance**: Policy support for parental leave, flexible work, and overall well-being. • **Tolerance and Diversity**: Inclusivity across ethnicity, culture, and identity. • **Independence and Self-Reliance**: A cultural preference for autonomy paired with social solidarity. These values contribute significantly to the way countries in the region govern, legislate, and interact, both internally and with one another. **Discussion Summary** The group explored how these shared values are reflected in NoBaReg's working culture and how they shape cooperation: • **Informality and Trust**: A defining feature of NoBaReg is the low level of hierarchy in interactions. Trust is not only strong within countries but also extends across borders. This relational trust supports collaboration on regulation and implementation, and enables the group to work effectively together. • **Transparency in Practice**: Members noted a distinct difference in approach to document access and process openness compared to other EU countries. While some EU practices tend toward formality and closure, NoBaReg countries operate by the principle of "only as closed as necessary", reinforcing both efficiency and accountability. • **Pragmatism and Solution-Orientation**: The group's identity is grounded in a shared culture of practicality. This results in a highly functional and collaborative working environment—one that would be difficult to replicate with a different geographical or political mix of countries.

Topic	Annotation
Strategic Outlook – Future of NoBaReg	The discussion also turned to the possible **third iteration** of NoBaReg. NoBaReg was decided established in April 2022, a decision the HNG made based on a project application from the Norwegian Digitalisation Agency. One of the direct procedural mandates in the project application, was that physical meetings should be the core of the project, run by one Project Manager. Since then, four more physical meetings have been held, and three digitals. Duew to a healthy financial situation, the first phase of Nobareg was extended until 31.07.2023. The second phase is planned to end 31.027.2024. Both within and outside of Nobareg, the project is viewed as successful and valuable. The PL indicated that if a new proposal were to be drafted, it would reflect the shared values described above and leverage the group's working culture. Key points included: • A new proposal may be initiated by a **single country**, **a group of countries**, or coordinated via **national lobbying** through the HNG (Horizontal Network Group). • Any new project must be **well-crafted** and **results-driven**, with **clear deliverables** aligned to existing frameworks such as the **European roadmap**. • A future NoBaReg might focus more on **implementation** of digital regulation (rather than the legislative work programme), possibly including the streamlining of **reporting obligations** to the European Commission. • It was also noted that any author of a proposal will bring their own strategic interests, which should be kept in mind when shaping the purpose and scope of a new initiative.

Looking back and taking stock: Where are we with Digital legislation?	The group reflected on the trajectory from the **Digital Single Market Strategy** through to the current **Digital Decade Strategy**, spanning nearly a decade of intense legislative activity in the digital space. As the EU enters a relatively quiet legislative period due to the 2024–2025 election cycle, participants saw value in pausing to evaluate what has been achieved—and where things are heading. The session was anchored by a visual timeline showing the rollout of EU digital legislation over time and by policy type.  *Figure 1 Digital initiatives from 1987 - 2024* For a broader and regularly updated view of EU digital legislation, participants were referred to **Kai Zenner's comprehensive timeline**, available here. **Discussion Highlights** • **Innovation vs Compliance Burden**: One concern raised was whether high administrative penalties, such as those seen under the **GDPR**, might unintentionally stifle innovation under the **AI Act** as well. The primary challenge may not be the intent of the laws, but the operational complexity and documentation burden involved in demonstrating compliance. • **Strategic Shift from Planning to Implementation**: The EU has long been in a **direction-setting phase**, but is now firmly entering the **implementation era**—especially in Member States, where regulatory frameworks are being tested in practice. This shift is seen more gradually in EEA countries. • **Evolving Data Governance**: The evolution from the **PSI Directive** to the **DGA** and **DA** reflects a policy transition from simply **making data available** to **governing how and by whom data is used**. This points to a maturing data economy that considers usage rights and control, not just access. • **Open vs Non-Open Data**: Despite the increasing focus on control and governance, participants noted a persistent divide in EU policy between **open data** and **non-open data** regimes. This tension continues to shape implementation strategies and stakeholder responsibilities.