Agenda – Nordic-Baltic coordination network on regulatory issues

24. - 25. February 2026, (09:30 – 17:00, 09:00 – 15:00)

Venue: Ministry of Smart Administration and Regional Development of the Republic of Latvia, Peldu Street 25, Riga, Latvia

Participants:

Denmark	Latvia	Sweden
Estonia	Lithuania	Aaland Island
Finland	Norway	Ukraine

Tuesday 24. February 2026	
Topic	**Annotation**
Achievements, challenges and opportunities in the digital in Ukraine	• Presentation by Ukraine's Ministry of Digital Transformation (Deputy Minister Zoriana Stetsiuk and Olha Krevska, Director for European and NATO Integration) • **Part 1: Ukraine's Digital Transformation achievements** • Mission and scale: The Ministry of Digital Transformation was created in 2019 with the mission "to build the most convenient digital state in the world." A wide portfolio of flagship projects is showcased (Diia, Diia.Business, Ukrainian Startup Fund, Дія.Відкриті дані, Army of Drones, UNITED24, Brave1, Diia.City, Diia.Engine, E-Court, E-Notary, Mriia, eExcise, Marriage Online, CDTO Campus, and others), positioning Ukraine as a broad GovTech ecosystem, not just a single app. • **Diia ecosystem — key numbers:** • Diia Portal: 150+ services, 6+ million users, including "Diya.AI" — described as the world's first national AI assistant • Diia app: 23+ million active users, 33 digital documents (including the world's first Digital Passport), 165+ portal services, 65+ mobile app services • Core ICT components: Diia app/portal (citizen-facing), Diia.Engine (backend for digitalizing public services — cuts service-creation time to under 3 months; used by 70+ registries/services, 22 ministries/state committees, 15 developer teams/100+ engineers), e-signature, Trembita (based on Estonia's X-Road, the national interoperability backbone — 196 connected resources, 1,179 web services, 17 billion exchanges over 5 years, 1 billion/month), and the e-ID system. Diia.Engine also offers low-code constructors (databases, business processes, forms, APIs, reports, extracts) to speed up development.

	• A new Personal Data Monitoring Subsystem is highlighted — citizens will be notified via Diia of every data exchange between government agencies (launching with Trembita 2.0, Q1 2026, full app integration mid-2026), framed around the "once-only" principle, cost efficiency, security, and data-driven governance. • Legal harmonization: Ukraine is drafting a Law "On Interoperability" based on the (EU) Interoperable Europe Act, with the Ministry running the process from drafting through peer review (with EU Commission DG DIGIT and the Interoperable Europe Community) to adoption and designation of competent authorities. • Open Data: 9 million unique users of data.gov.ua since 2016, 100+ services built on open data, ~13.9 million monthly users of those services, ~80,000 datasets (though some access is restricted due to the war), ₴103.4 billion estimated open-data GDP contribution (pre-war research), 70,000+ trained civil servants, and 3rd place in the European Open Data Maturity Assessment 2023. • eID and Trust Services: 22+ million Diia users including 10 million using qualified electronic signatures (QES); 36 million issued QES certificates; 60 million transactions and 26 billion data exchanges via the state identification hub id.gov.ua. Ukraine's implementation of eIDAS 1.0 is described as highly compliant; Ukrainian QES are recognized in the EU as AdES, and EU QES are fully recognized in Ukraine as equivalent to handwritten signatures. Ukraine is testing the EU Digital Identity Wallet prototype within the POTENTIAL consortium. A detailed roadmap runs 2017 → 2022-23 → 2025-27, aiming for full eIDAS 2.0/EUDI Framework alignment, internal market treatment, and full wallet interoperability with the EU by Q2 2027. • Bilateral milestone with Latvia: As of 6 January 2026, Ukrainian QES (on the EU's Third Country Trusted List) are legally recognized in Latvia as equivalent to handwritten signatures, following amendments to Latvia's Law on Electronic Documents — making Latvia the first country worldwide with full mutual electronic-signature recognition with Ukraine (EU QES was already recognized in Ukraine since 2023). • Digital governance leadership programs: CDTO Campus (1000+ graduates, 7000+ applications, 30 programs, 100+ lecturers); 45 CDTOs now embedded across ministries using OKR-based management and a results dashboard (13-ministry pilot underway); 15 regional CDTOs and ~1,400 digital community leaders, supported by the "Diia.Digital Hromada" platform and digital transformation indices for regions/communities. • **Part 2: EU Accession — Chapter 10 ("Digital Transformation and Media")**

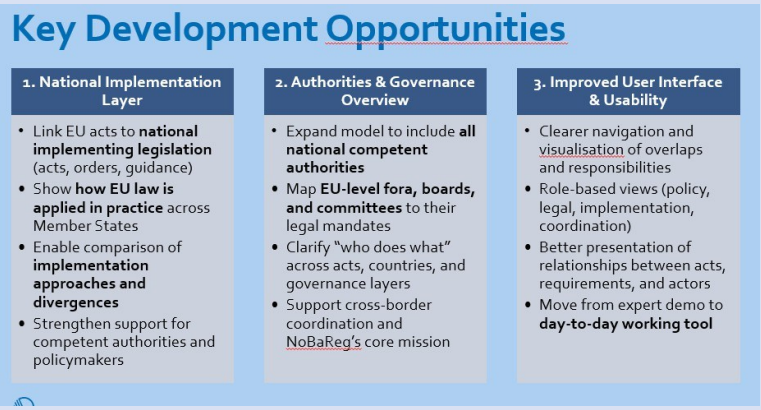
	• This section maps Ukraine's alignment against each thematic area of accession Chapter 10: • Overall Digital Strategy (Digital Agenda 2030): covers e-government, e-democracy, AI, digital economy, inclusivity, national cloud, infrastructure, skills, data management, and cybersecurity — KPIs synced with the EU's Digital Decade 2030/Digital Compass, with Ukraine working toward DESI and eGovernment Benchmark inclusion. • Electronic Communications & Spectrum: Partial alignment with the Gigabit Infrastructure Act; active 5G Toolbox development. A dense timeline of law adoptions runs Q4 2026–Q4 2027 (network deployment simplification, open internet rules, 5G security, regulator independence), with full spectrum alignment deferred until after martial law ends. • Roaming: Ukraine joined "Roam Like at Home" on 1 January 2026. • Digital Services (DSA/DMA/P2B): E-commerce Directive partially aligned (2015 law); DSA/DMA/P2B legislation in progress, alongside a concept for a future "Digital Regulator." Roadmap: draft laws 2026–27, regulator established 2028, full operational capacity and EU cooperation by 2028. Strategic goals include joining the AGORA platform and engaging VLOPs/VLOSEs/gatekeepers. • Data Governance & Open Data: Partial alignment across the Open Data Directive, Data Governance Act, High-Value Datasets, and Data Act. Key tension flagged: balancing open-data transparency against wartime security needs, plus DCAT-AP metadata harmonization. Detailed roadmap runs Q3 2026–Q4 2027, ending with a Data Sector Development Strategy 2028–2033. • eID and Trust Services: Covered in detail above (Part 1), restated here as the Chapter 10 accession dimension — high alignment with eIDAS 1.0, in-progress alignment with eIDAS 2.0/EUDI. • Cybersecurity: Original NIS Directive: high alignment (2018 law). NIS2: in progress — a new cybersecurity law entered into force 20 April 2025. Cybersecurity Act (certification) and Cyber Solidarity Act: partial/in progress. Institutionally, the National Cybersecurity Coordination Center and CERT-UA are fully operational. Notable section on lessons from active cyberwarfare — sustained high-intensity operations, hybrid kinetic/cyber threats, operational solidarity, supply chain/certification gaps, and institutional capacity constraints. Roadmap to Q4 2027 includes a new Framework Cybersecurity Law (Q2 2026) and full ENISA/CyCLONe compatibility. • Semiconductors: Early-stage alignment with the EU Chips Act; national strategy (2027–2030) will focus on "fabless" chip design and defense-related components (drones, robotics). Key challenges: investment gap, talent retention/brain drain, and physical security risk to manufacturing sites during the war. • Artificial Intelligence: High strategic alignment (Ukraine's 2020 AI Concept and 2024 White Paper mirror the EU AI Act's risk-based approach); legal alignment in progress via a "bottom-up," self-assessment/voluntary-code approach. Ukraine claims to be the first non-EU country localizing AI Act principles via a regulatory sandbox. Roadmap: observer status on the European AI Board

	(2025) → National AI Strategy 2030 (Q2 2026) → full AI Law transposition (Q4 2027) → Digital Regulator oversight (Q1 2028) → full implementation by 2030. • Digital Regulator vision: Proposed transformation of the NCEC (telecom/postal regulator) into a converged "Digital Services Coordinator" covering DSA, DMA, Data Act, AI Act, and P2B — funded by a market-participant regulatory fee model for independence. Three-phase roadmap 2025–2027 ending in AGORA integration. • Expert group participation: Ukraine already participates in several EU digital expert groups: European Digital Identity Cooperation Group, FESA, European Data Innovation Board, European AI Board, Radio Spectrum Policy Group (incl. a bilateral 700 MHz sub-group), Interoperable Europe Board, Gateway Coordination Group, and the Expert Group on Safer Internet for Children. • Tracking emerging EU legislation: The deck closes by flagging Ukraine's active monitoring of the new EU Cybersecurity Package, the Digital Networks Act (consolidating EECC, BEREC Regulation, Radio Spectrum Policy, and Open Internet Regulation into one framework), and the Digital Omnibus proposal.
Non-paper on the Cloud and AI Development Act by Denmark	Core argument: Denmark frames CADA as the concrete vehicle for delivering on the Commission's Tech Sovereignty Package, and pushes for a pragmatic, risk-based, low-burden approach rather than sweeping rules. The paper's central move is redefining "sovereignty" itself: not a binary or geography-based concept (i.e., not simply "EU-owned = sovereign"), but a continuum tied to resilience, freedom to choose, and the ability to switch providers without prohibitive cost — especially in crisis situations like cyberattacks, geopolitical shocks, or provider insolvency. Three priorities: 1. Risk-based, proportionate requirements. Stricter sovereignty requirements should apply only where risk and criticality are genuinely high; for everything else, the market should stay open and competitive, with interoperability, portability, and switching as the main safeguards rather than heavy-handed rules. 2. Remove infrastructure deployment barriers — but selectively. Denmark argues there isn't a general shortage of data centre capacity (they've attracted plenty of hyperscaler investment) — the real gap is in "sovereign and sustainable capacity" specifically for critical functions. They want fast-tracked permitting targeted at projects of clear public interest or strategic relevance, not blanket expansion, and specifically warn against this creating national silos that fragment the EU market. 3. Make sovereignty operational on the demand side. This is the most concrete section: citing a Danish Chamber of Commerce survey (88% of member companies use at least one non-EU cloud provider, roughly half want to reduce that dependency but lack clarity on viable alternatives), Denmark argues the barrier isn't intent but information and switching costs. They want CADA to introduce simple, evidence-based sovereignty criteria to prevent "sovereignty washing," plus stronger public procurement rules so the public sector can act as a strategic first mover for European alternatives — while being explicit that CADA should complement, not duplicate, the Data Act and Digital Markets Act.

	Underlying tension worth noting: the paper wants CADA to avoid duplicating the Data Act on switching/portability, while also admitting the Data Act's effects on switching "have yet to materialise in the market" — implying CADA needs to do real additional work here even as Denmark insists it shouldn't overlap. That's a needle they don't fully thread in the text.
Latvia's National Interoperability Framework	Presentation by Monta Balode (Ministry of Smart Administration and Regional Development) Timeline: Latvia's digital government architecture work spans 2014–2026: architecture principles and conceptual architecture were developed 2014–2024; the ICT Construction Board was established in 2022; a domain architecture approach was piloted in 2023 (starting with electronic identity and trust services); 2024 focused on building the regulatory framework, making domain architecture a mandatory prerequisite for ICT investment projects; 2025 saw development of domain architectures across "6+14" domains; and 2026 is focused on reviewing and improving the regulatory framework, including giving domain lead architects a greater supervisory mandate. The "missing governance level" problem: Latvia identifies a structural gap between two existing levels — the national level (architectural principles, requirements, and governance frameworks, owned by the Government CIO office, Ministry of Defence/cybersecurity, and data protection authorities) and the project level (architecture of individual project solutions, owned by project promoters). Between them sits a gap with no clear owner. Their solution is a new domain level (L2), governed by domain authorities and programme promoters, responsible for domain-specific principles, requirements, target architecture, and oversight of how individual projects in that domain are architected. Domains structure: Latvia organizes its digital government architecture around a stack: national-level architecture principles and requirements at the top, then 14 vertical domains (Construction, Energy, E-Case, Education & Science, Culture & Language Technologies, Welfare, Transport [listed 3 times, possibly sub-areas], Taxes, Health, Voting & Legal Acts, Environment & Regions, Civil Protection), sitting above four horizontal cross-cutting layers: Data Analysis / Government Modernization / Public Services Delivery & Governance, then Data Governance & Sharing / Identification & Trust Services, and finally ICT Infrastructure & Cybersecurity at the base. Governance roles: A structured hierarchy: a State Lead Architect (based at VARAM, the ministry) sits within a State Architecture Forum (part of the broader ICT Managers Forum), alongside Domain Lead Architects for each domain (A, B, C shown as examples) and Subject Matter Experts. Each domain also has its own Architecture Governance Team and multiple Domain Architects reporting into the domain lead. Methodological grounding (slide 7): Latvia frames this explicitly as digital government architecture, not just ICT architecture — covering legal, organizational, semantic, and technical views (the latter highlighted as this presentation's focus). It's built on European interoperability frameworks (EIRA, EIF), the TOGAF standard adapted with

	private-sector practices, national-level principles compliant with EIF, and ties architecture directly to investment planning by domain. Key takeaways: • What's working: gradual institutionalization of governance, engagement of domain stakeholders, and integration with investment portfolio planning. • Challenges: limited institutional capacity and insufficiently coordinated domain architecture governance, dynamic/shifting target architectures, and legacy complexity across existing solutions. • Closing note: the model has potential for application at both cross-sectoral and domain-specific levels.
Cloud in Latvia – National Federal Cloud, Commercial Cloud and Regulatory Framework	Toms Štālbergs (Ministry of Smart Administration and Regional Development, Latvia) presented Latvia's approach to developing a national cloud infrastructure and regulating the use of commercial cloud services in the public sector. The Latvian model combines a National Federal Cloud for public administration with the possibility for public institutions to procure commercial cloud services under defined security, procurement and data residency requirements. The overall approach is intended to strengthen resilience and cybersecurity, reduce fragmentation and duplication, and avoid vendor lock-in. The National Federal Cloud was formally established in 2025 and is based on a federated model involving several state-owned cloud service providers, with central governance and a designated state "Broker" responsible for supervision and acting as a contact point for public institutions. In parallel, Latvia has established a dynamic procurement system for commercial cloud providers, with pre-qualified providers and a standard contractual framework aligned with EU and Latvian requirements. Cloud migration is also being pursued as part of Latvia's broader ICT consolidation policy, including a cloud-first principle for new developments and requirements for ministries and sectors to prepare migration plans. This is accompanied by measures to prevent uncontrolled re-fragmentation of public ICT infrastructure and by increasingly detailed cybersecurity requirements for cloud and data-centre environments. Of particular relevance to NoBaReg was the relationship with the EU Data Act, especially its provisions on cloud switching and the prevention of vendor lock-in. Although the Latvian ICT management authority is not necessarily responsible for market surveillance under the Data Act, it has an important role in ensuring that public-sector procurement, contracts and cloud policies comply with the Act's requirements. This includes addressing switching barriers, data portability, transparency and functional equivalence. The presentation highlighted several challenges that are likely to be relevant beyond Latvia, including balancing digital sovereignty with competition, ensuring interoperability between national and European cloud infrastructures, and avoiding new forms of structural vendor lock-in.

<table>
<tr><th colspan="2">Wednesday 25. February 2026</th></tr>
<tr><th>Topic</th><th>Annotation</th></tr>
<tr><td>Deliverables</td><td>Adam and Thomas presented the results from the EU Law Explorer thus far, and the group discussed possible way forwards from this table:

It was decided that Digst follows up with different points from the three tables. Next stps will be followed up in future meetings.</td></tr>
<tr><td>DAGR – Data dissemination and governance platform</td><td>Presentation by Jānis Krakops, Head of the Data Governance Unit at Latvia's Ministry of Smart Administration and Regional Development (25 February 2026), plus an attached second deck on Latvia's broader Data Governance Strategy:

DAGR platform

What it is: A centralized platform for exchanging data between "evidence providers" (data-holding institutions) and "evidence requesters," built around a core (database, object, API), configurable connectors on both ends, a self-service portal, and integration with Latvia's VIRSIS access-permission system.

Advantages highlighted:

• Data updates supported at up to every 10 seconds
• Configurable data connector integrating multiple endpoint providers
• Standardized, interoperable metadata
• High-availability SLA
• Centralized infrastructure reducing duplicated effort
• Usable by institutions with varying levels of technological capability
• Data providers retain full control over their shared data
• Support for cross-border procedures EDIW (European Digital Identity Wallet) and OOTS (Once-Only Technical System)

Usage as of February 2026: 71 data providers (including municipalities), 278 published datasets, 46 data users.

"Wrong way / Right way" framing: Without DAGR, each credential type (proof of residency, driving licence, business registration, disability status, etc.) would need its</td></tr>
</table>

	own separate integration into an EDIW provider — shown as failing/red. With DAGR, all these flow through unified DAGR connectors and a governance dashboard into the EDIW provider — shown as working/green. This is explicitly tied to the Once-Only principle, the EU Digital Identity Wallet, and the European Business Wallet. **DAGR summary (core value propositions):** Centralized data governance with unified access Reduced administrative and IT burden — institutions don't each need their own data exchange solution High-performance, unified data distribution Data access permissions concluded digitally via smart contracts **New key features, shown on a timeline:** • Data filters (Dec 2024): record-level access control — providers define exactly which data values are accessible; filtering happens automatically on DAGR's side rather than by the consumer • Dashboard (Feb 2025): a governance and reporting interface showing live statistics — active data providers/receivers, requests received, datasets offered/used, access permissions • From PDF files to structured data (Sept 2025): converting unstructured files (e.g., XLS) into structured data via DAGR • Data Consumer Connector (Dec 2025): cuts integration time from weeks/months to hours/days; acts as an agent writing records directly into the client's database, reducing upload errors; aimed particularly at institutions with limited IT resources • Data monitoring (April 2026): lets data consumers configure monitoring sets (which dataset, which fields to watch) for fast real-time change notifications, without using the consumer's own system resources to detect changes Comparison table — "Different Needs Require Flexible Solutions": DAGR is compared against four other Latvian tools (API manager, DIT, ĢDS, Open data portal) across 13 capabilities. DAGR's distinguishing strengths: high-performance data exchange, centralized computing power, and support for lower-ICT-maturity users — capabilities none of the other four tools share. It does not support data writing, exchange of large/geospatial data, anonymous access, or standalone web services — those are covered by the other tools instead. Data Governance Strategy 2026–2030 (in Latvian) A short strategy overview covering: • Strategy goals (Stratēģijas mērķi): implement a unified data governance culture across public administration; improve the quality of state data; expand public data accessibility; develop data competencies within public

	administration; foster data-driven innovation; reduce bureaucracy in data work • Benefits (Ieguvumi): less bureaucracy, higher-quality data, faster services, a one-stop agency for data dissemination, innovation and AI development, faster data exchange, more efficient public administration — with a cited €8,441,700 in estimated administrative-process savings • What is data governance? (Kas ir datu pārvaldība?): defined as a shared approach to working with data across the whole public administration — how data is described, shared, and used across institutions — improving cooperation, reducing bureaucracy, and strengthening innovation and AI development • Data lifecycle (Datu dzīves cikls): five stages — Creation (Izveide) → Storage (Glabāšana) → Use (Lietošana) → Dissemination (Izplatīšana) → Archiving (Arhivēšana) • Strategic foundation (Stratēģijas pamatā): data framed as a "valuable resource" that must be professionally managed across its full lifecycle; unified data governance practice ensures data is trustworthy and reusable in public administration work and decision-making
Next meetings/Latvia taking over NoBaReg from 1. November 2026	Next meeting decided to be in Brussels in June, and Latvia presented the main directions of the NoBaReg work plan that Latvia would like to focus on in the next period.