Latvia's non-paper on Simplification on the Digital Omnibus package

Latvia welcomes the European Commission's initiative to simplify and align the EU digital rulebook through the forthcoming Digital Omnibus. The aim of it should be to improve coherence and reduce unnecessary administrative burden while keeping the policy objectives and protection levels of existing legislation intact.

Simplification should concentrate on practical implementation, legal clarity and consistent interpretation across all Member States, avoiding potential conflicting interpretations and overlapping procedures among different involved authorities. The focus should be on improving how rules work in practice, not on reopening agreed political compromises.

Governance and coordination

Implementation of the digital rulebook has led to a growing number of boards, authorities and coordination formats. To reduce fragmentation, Latvia suggests:

- **Creating and maintaining a common glossary of digital terms** to be used across the acquis.
- **Using existing European coordination bodies (AI Board, European Data Innovation Board, Interoperable Europe Board, ENISA) to ensure consistent application** more effectively.
- **Allowing Member States flexibility to consolidate national competences and avoid parallel authorities. Ensure reasonable time for implementation.**
- **Organising regular technical exchanges between Member States before key implementation deadlines** to identify shared challenges early.
- **Ensure permanent coordination and proactive, timely guidance among authorities of the Member States and the European Commission, other EU institutions, bodies and competence centres** (AI Office, The European Data Innovation Board (EDIB), ENISA etc), to ensure consistent application and interpretation among Member States.
- **Introduce unified *"Digital Compliance Framework"* at the EU level allowing companies to use a single compliance and reporting mechanism to meet the requirements of multiple regulations**, strive to harmonize incident reporting and risk assessment formats, mutually recognize security and compliance measures across different regulations (for example, DORA and GDPR).

Artificial Intelligence Act

Latvia supports a proportionate, innovation-friendly implementation of the AI Act and the Digital Omnibus objective to simplify and harmonise EU digital legislation, especially where implementation creates unnecessary administrative burden. The Digital Omnibus should:

- **Clarify what counts as high-risk AI** to provide interpretative guidance on high-risk AI and the treatment of traditional (non-AI) algorithms. There is need for concise, practice-oriented guidelines, examples, checklists and templates for classification, incident reporting and related processes.

- **Provide EU model templates** to offer standardised templates for conformity documentation and post-market monitoring to reduce variability and complexity across Member States.
- **Support SMEs and low-risk public-sector use** to extend and clarify SME-specific flexibilities, including for public entities operating low-risk systems, so that compliance remains proportionate and does not discourage responsible innovation.
- **Recognise regulatory sandboxes** to accept results from regulatory sandboxes as valid evidence of compliance, rewarding early engagement with regulators and supporting safe experimentation.
- **Avoid parallel technical files and declarations** aiming for one modular technical file and one EU Declaration of Conformity per system, reusing common evidence across all applicable acts and fully preserving requirements on safety, robustness and cybersecurity. For example, a unified "AI + cybersecurity" technical file could underpin a single declaration avoiding fragmented procedures while keeping a high level of trust.
- **Make AI literacy practical** to implement AI literacy obligations through free online training and concise guidance with checklists, templates and example workflows – so organisations can build staff competences in a practical, low-bureaucracy way.
- **Ensure legal certainty when standards lag behind** to provide clear substitute mechanisms and a safe harbour for documented, good-faith operators, especially SMEs. Compliance timelines should remain realistic, and enforcement should be proportionate, considering genuine efforts to follow available guidance and alternative routes to demonstrate conformity.
- **Align the AI Act and the GDPR** to ensure a clear, unified interpretation of both acts (especially on risk classification and data use) and introduce a single, streamlined compliance process: one procedure, one impact assessment, one documentation set, covering both fundamental-rights and data-protection risks. This should be supported by a practical EU-level tool and simple checklists so that organisations, especially public bodies, start-ups and SMEs, can comply efficiently. Accelerate the review of e-Privacy rules to reflect current technological realities and ensure coherence with the AI Act and the GDPR, reducing legal fragmentation for AI-driven services.

Data legislation

We support the goal of harmonizing and simplifying existing data rules to create a clear, comprehensible, and effective legal framework that promotes secure and efficient data exchange between businesses and public sector institutions. Data protection and privacy are integral components of fundamental rights, and their observance must be ensured throughout the simplification process. Therefore, it is crucial to maintain a balanced approach between transparency, data accessibility, and personal data protection, ensuring that the regulation is not only effective and practically implementable but also fully compatible with human rights.

The current data framework – the Data Act, Data Governance Act (DGA), the Regulation on the Free Flow of Non-Personal Data (FFDR) and the Open Data Directive would benefit from clearer interaction and simpler governance. Some of the issues to be resolved:

- The title of the DGA is quite misleading as it does not really cover the topic of data governance**.** In **the process of revising the regulations we propose that this aspect is integrated within the scope of the amended regulation**.

- The governance structure – there are lot of contact points and competent authorities established. **In the process of simplification this matter should be addressed also taking into consideration how will all these institutions interact with the EDIB.**
- With the Data Act, the EDIB's mandate has expanded beyond government data to also include private-sector data transactions. Both important responsibilities should be reflected in the EDIB's agenda.
- In terms of regulatory simplification, **we support the proposed** integration of the PSI Directive into the DGA, and the FFDR together with the private-sector–focused elements of the DGA (registration of data altruism organizations and data intermediary services) into the Data Act. **However, we are in view that aspects regarding data governance should be integrated to make data legislation easier to understand.**
- Regarding the INSPIRE Directive and the upcoming "GreenData4All" initiative, we believe it should be grounded in concrete use cases to ensure clear purpose and transparent links to other data regulations. **From a practical perspective, we recommend reviewing current data format requirements to make INSPIRE data more usable across sectors.** At present, the mandated formats are highly specific and, to our knowledge, not widely adopted outside the geospatial domain, limiting broader reuse.

Administrative burden on public administrations

Combined effect of several digital acts has created complex reporting and coordination duties for Member States. To ensure sustainability of implementation, issues to be resolved are:

- **Mapping and streamlining all reporting obligations** arising from the digital acquis.
- **Introducing common digitally enabled templates and reporting cycles** to reduce duplication.
- **Applying the one-in, one-out principle** also to obligations placed on national administrations.
- **Creating a single reference portal for definitions, templates and guidance** used under the digital rulebook.
- **Providing shared guidance and training material for officials involved in applying the AI Act, Data Act** and related instruments.
- **Setting up a simple channel for continuous feedback from Member States to the European Commission** on implementation issues.

Electronic Identity

It is essential to ensure regulatory and operational alignment with the upcoming EU Digital Identity Wallet and the EU Business Wallet.

By 24 December 2026, each Member State must ensure that its citizens have access to at least one European Digital Identity Wallet. Given that the functional and legal framework of the European Business Wallet is not yet defined, **the Digital Omnibus package should also assess the option of developing the European Business Wallet within the framework of the European Digital Identity Wallet.**

Cybersecurity

In the field of cybersecurity, we call for a harmonization of incident reporting. At present, incident reporting obligations overlap across GDPR, NIS2, DORA, and CER frameworks. Incidents often cross regulatory borders, for example, many personal data incidents are also

cybersecurity incidents. Companies would prefer to submit a single consolidated report in such situations rather than separate ones to each supervisory authority.

The European Commission has recognized the need for measures to minimize the complexity of incident reporting, to simplify compliance requirements, and the use of cybersecurity incident reporting tools, while maintaining a high level of cybersecurity. When evaluating the possible creation of a unified reporting platform to ease the obligations of cybersecurity incident reporting, it would be important that such a platform is designed to be easily administrable and user-friendly for all its users –companies (e.g., NIS2 entities), supervisory authorities, and EU institutions – and is interoperable.

We also call for a need to develop a mechanism which would harmonize cybersecurity regulations between EU Member States. States currently interpret the regulations in different ways and apply them to entities of various sizes, turnovers, sectors and levels of criticality. Due to differing national legislations EU-wide cybersecurity regulations are often applied unevenly across certain sectors. This creates a risk of interfering with a fair competition between companies of different states. In order not to affect the free market across all the EU States a unified application of cybersecurity regulations is needed. We believe this could be achieved through an improved coordination, information sharing and experience exchange between Member States.

GDPR and ePrivacy Directive

The regulation on cookies needs to be streamlined, as it relates to both GDPR and the ePrivacy Directive. The requirement for a consent should be simplified, for example, when it concerns to low-risk cookies used for analytics or statistics.
In the context of GDPR and data sharing, greater clarity is needed. Currently, the conditions for transferring data to third countries are quite burdensome, while in reality, data flows continuously. Mechanisms should be developed to facilitate such exchanges and make compliance tracking easier.