Council of the European Union

Brussels, 2 June 2025
(OR. en)

9383/25

TELECOM 165

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	AOB for the meeting of the Transport, Telecommunications ans Energy Council on 6 June 2025 : Outcomes of the discussions on simplification activities in the digital field - Information from the Presidency

Outcomes of the discussions on simplification activities in the digital field

Balancing regulation and innovation in the technology -driven economy

Introduction

The Polish Presidency has prioritised regulatory simplification in the digital sector to support innovation and reduce burdens on businesses, particularly SMEs. This report summarises initiatives undertaken by the Polish Presidency, and key insights gathered from a wide range of stakeholders.

The consultation process generated a broad range of valuable feedback, with numerous organisations submitting detailed contributions. This report presents the most frequently raised and broadly supported recommendations, aiming to provide a representative overview of stakeholder perspectives and to inform the ongoing efforts in regulatory simplification.

As simplification in the digital area is an already agreed objective, both at the EU and Member States' level, it has been translated into several strategic documents, including:

- **Commission's political guidelines for 2024-2029** – these guidelines set the tone for the next institutional cycle, emphasising better regulation, competitiveness, and reducing burden on SMEs. They call for a smarter, less bureaucratic regulatory framework that supports innovation and digital transformation while ensuring high standards and protection of fundamental rights.

- **EUCO Conclusions - 20 March 2025** – the European Council prioritised urgent action to boost EU competitiveness through simplification of regulations and reduction of administrative burdens. The European Council called on the Commission and the co-legislators to work towards achieving the target of reducing the cost of all administrative burdens by at least 25%, and by at least 35% for SMEs, which could translate to €37.5 billion in business savings.
- **Competitiveness Compass** – presented a strategic vision for simplification and effective implementation of EU policies. It highlighted the need for better cooperation with Member States and the use of digital tools in regulation.
- **Single Market Strategy –** aims at enhancing the single market by removing remaining barriers, reducing red tape, promoting investment and ensuring fair competition.

Actions taken by the Polish Presidency

Considering the pivotal role that implementing and utilising new technologies plays in today's economy and economic development, a significant challenge lies in keeping pace with regulations that both provide robust protection and create favourable conditions for innovation and entrepreneurship. Taking into account the current geopolitical situation, it is crucial that Europe empowers digital companies to grow, scale, and innovate and in this way, effectively compete with other global players. **Given the importance of this issue, the Polish Presidency has launched several actions intended to add value to efforts being made at the European level in the area of simplification:**

- **High-level Roundtable**

On 10 April, the Presidency organised an event "*High-Level Roundtable on simplifying EU digital regulations and enhancing the business environment"*. The roundtable was attended by various industry associations and alliances[1] and representatives from the European Commission. The aim was to explore practical ways to reduce regulatory complexity and enhance the business environment for European companies (particularly SMEs) in the digital and industrial sectors.

- **A debate at the WP TELECOM meeting**

Polish Presidency addressed simplification also within the Council of the EU, including at the Working Party for Telecommunications and Information Society (WP TELECOM). On 14 March, the Presidency organised a debate on the interplay between the AI Act and the GDPR. The discussion was based on the discussion paper with guiding questions. The debate aimed to identify compliance challenges with both the AI Act and the GDPR, find best practices in cooperation between key actors and stakeholders, and discuss implementing regulatory sandboxes. The discussion explored the perspectives of both the entities subject to the two regulations, and the relevant national authorities: market surveillance authorities under the AI Act and data protection authorities under the GDPR. The outcomes of the discussion were gathered in the Presidency report.

[1] American Chamber of Commerce to the European Union (AM Cham EU), Association of Commercial Television in Europe (ACTE), Business Europe, Connect Europe (ex ETNO), Digital Europe, DOT Europe, EU Tech Alliance, European Data Centre Association (EUDCA), European Cyber Security Organisation (ECSO), European Digital SME Alliance, European Enterprise Alliance (EEA), European Roundtable for Industry, Information Technology Industry Council (ITI).

- **Digital tools to meet regulatory obligations and assist reducing the administrative burdens – questionnaire for Member States**

By issuing a survey among the Member States, the Presidency aimed to initiate a discussion on a possible set of recommendations on the methodology for using digital tools that facilitate harmonisation and coherence across the EU. The survey focused on the use of digital tools for better law-making and measures to facilitate compliance, data collection, data processing, reporting and interoperability at both national and European levels. It aimed at identifying and sharing good practices. Final recommendations, based on the results of the survey, could serve as a guide to better align usage of digital tools with the EU's vision for a unified digital and regulatory ecosystem.

Challenges identified by stakeholders

The following challenges and areas of further reflection were identified by stakeholders in the consultations undertaken:

Regulatory overlaps and inconsistencies

- Multiple risk assessment obligations (for example the allocation of tasks using AI and algorithms is subject to regulation across various pieces of legislation, each with its own enforcing authority[2]);
- Clarity of definitions – lack of consistency in definitions across legislation complicates enforcement, market surveillance, and judicial decision-making; definitions were sometimes considered too broad by stakeholders;
- Reporting requirements – multiple reporting obligations across different regulations (e.g., Electronic Communications Code, cybersecurity rules, sustainability rules) with different deadlines, various points in the year, through various means and to various authorities;
- Exemptions – the long list of exemptions in EU regulations, leaving room for fragmentation in the single market (despite having in principle full harmonisation)[3].

Implementation challenges

- The same European legislation often implemented by Member States in 27 different ways, creating administrative burden
- Gold-plating at national level[4]
- Fragmentation in enforcement mechanisms - different authorities responsible for related legislation, lack of coordination and cooperation between authorities
- Extensive documentation obligations.

---

2 E.g. PWD requires an ex-post assessment every two years when using algorithms to allocate tasks. The AIA requires ex-ante risk assessment every year when using AI for task allocation.

3 An example for this is the age of consent in GDPR, which was left to EU MS, with all going for somewhere between 13 and 16, which creates significant friction for consumer-facing online services. Moreover, the spread of minor protection measures by EU MS - often under the justification of the AMSD implementation - risks fragmenting the EU market for online services.

4 The recent example which is impacting the data centre sector is the implementation of the EED. Some MS have gone beyond the requirements of the directive and introduced more transparency in the publication of the reported data, which threatens business secrets. Similarly, beyond the reporting, some MS have introduced minimum standards, which run the risk of being different to future EU standards.

Thematic challenges

Data regulation framework

- Clarity on the application of the GDPR principles-based approach, for example related to personal data, minimisation, anonymisation, proportionality, and consent, including when cross-referenced in other digital regulations, such as the Data Act, Data Governance Act, Digital Markets Act or the Unfair Commercial Practices Directive [5]
- Unclear scope of notion of "data intermediation services provider" (Data Governance Act)

AI Act implementation

- Risk-based approach interpretation difficulties
- Challenging interplay with sectoral legislation and standards – i.e. GDPR provisions on purpose limitation for processing, and data minimisation versus the ambition for the AI Act to stimulate AI development and training in the EU
- **Issues with implementation timelines**/challenging deadlines to comply with two parallel pieces of legislation (i.e. the AI Act and CER Directive in terms of critical infrastructure)

Cybersecurity

- Overlapping incident reporting obligations
- Various **risk management frameworks** – relying on internationally-recognized standards or nationally-developed ones
- Demanding compliance processes concerning **assessments and auditing** – audits using manual data inputs in dedicated software, spreadsheets
- **Supply chain** – lack of methodology to classify and manage third parties; mixed levels of security assurance

Ideas for simplification

According to stakeholders' input, the following main ideas to reduce complexity and support effective implementation should be recommended. It should be noted that the summary prioritises ideas that were repeatedly mentioned by groups of stakeholders. The summary of the ideas in this report is offered for further analysis.

BETTER REGULATION IN THE DIGITAL SECTOR
Publish **codified versions of the EU rulebooks, seeking also to** clarify the legal relationship between laws, including through clear guidelines, especially as to the hierarchy of laws – such as *lex generalis* vs *lex specialis* etc.
Ensure that **any impact assessment drafted ahead of the preparation of a new legislative includes a dedicated analysis on regulatory governance** – so as not to add unnecessary regulatory governance structures that further overlap and over-complicate the enforcement and implementation of the digital rulebook both for companies and regulators.

[5] Unfair commercial practices directive (UCPD) - less obvious overlap between consumer protection law and data protection laws. Stakeholders pointed e.g. the GDPR's "freely given, informed consent" vs the misleading actions prohibition under the UCPD – is this the same standard, can an online interface fulfil one law but not the other? Additionally, different authorities are in charge of enforcing this provision.

Consider **interoperability assessments as part of the impact assessment** of new or revised regulations. This would prove helpful when developing digital tools for law-making process at the national level. For example, digital tools supporting (1) preparation of regulatory impact assessment, (2) gathering data from public consultations, (3) legislation drafting, (4) transposition of directives, (5) evaluation of legislation (e.g. in order to identify regulatory burdens).
Introduce new, common statutory duties for all regulators and the European Commission to have regard to the impact of regulation and enforcement on competitiveness, innovation, and growth.

IDENTIFIED CHALLENGE	IDEAS TO TACKLE CHALLENGES
GENERAL	
Dialogue and coordination between different authorities enforcing EU digital legislation	Enhance the ongoing cooperation and create, on the basis of **an existing structure**, a cross-regulatory forum of EU-level bodies and authorities coordinating the enforcement of rules, such as the AI Act, DSA, DMA, GDPR, GPSR and cybersecurity legislation. The forum should help to identify coordination challenges and issue **joint guidance on the interplay between regulations.**
Definitional inconsistencies	Create a centralised glossary, mandatory cross-referencing and align definitions. Align by using one definition across various regulations (e.g. "main establishment" across CRA, NIS2 and DORA, "remote data processing services" across CRA and NIS2, or “data processing service” under the Data Act).
Excessive and fragmented reporting obligations	Develop minimum harmonised, EU-level digital reporting standards. Establish single reporting obligation and national single entry points. Establish centralised EU reporting mechanism with harmonised templates. Consider introducing recognition of mutual fulfillment of notification obligations under NIS2 and CRA. Increase reporting thresholds for SMEs. Offer pre-filled templates, regulatory sandboxes and shared compliance services for SMEs.
Extensive documentation obligations	Develop Union level guidelines on documentation requirements in relation to risk assessments. Consider whether synergies are possible between various risk assessment duties. Streamline documentation requirements, especially when cumulative with sectoral or existing standards. Develop standardised documentation kits or pre-filled forms for typical SME devices (in open source or under EU license). Accept existing certifications or documentation to avoid duplication (e.g. for cybersecurity controls already certified under another framework). Allow pre-market compliance support through national authorities as an SME helpdesks.
Overlapping transparency obligations (for example under P2B, DSA, GDPR, EECC)	Consolidate and simplify transparency reporting into a single standardised framework for digital services.
Manual, fragmented, overlapping and outdated audit	Automate security audits (e.g. using Open Security Controls Assessment Language - OSCAL).

	Introduce single audits accepted across multiple frameworks based on internationally recognised standards. Adopt a systematic approach to presumption of conformity for cross-compliance (for example when an important or essential entity can prove compliance with the NIS2 requirements, this should be accepted as sufficient evidence that the entity has a satisfactory level of cybersecurity for the purposes of DORA audits as regards the corresponding obligations). Reduce the rigidity of independent audit requirements under DSA by changing the assurance standard in the delegated act.
Fragmented recognition of ICT certifications	Promote mutual recognition of sectoral and international certifications (ISO, CEN/CENELEC) across the EU.
Compliance complexity for access and portability	Introduce tiered (size-based) obligations or simplified compliance frameworks for SMEs. Promote sectoral and self-regulatory approaches - allow sector-specific certifications or self-regulatory initiatives that meet regulatory objectives and achieve equivalent results rather than mandating compliance audits.[6] Set minimum requirements for digital systems of businesses (Enterprise Resource Planning systems/ platforms) in the Single Market to promote automation for businesses and creating a level playing for companies. Establish Open Business Data Exchange Infrastructure to ensure a secure and seamless sharing of business data.
Expanding compliance timelines	Reuse the 'Stop-the-clock' mechanism applied in the Omnibus I sustainability package for the field of technology legislation (postpone the dates of application for laws if compliance tools like standards are not available, i.e. in the AI Act, the CRA).
Enhancing cooperation between Member States (e.g. ensuring interoperability across national systems)	Connect and use EU-level digital tools, especially the European Digital Identity Wallet and the upcoming European Business Wallet, which ensure that the same digital solutions and approaches are implemented in all Member States, to support compliance particularly for horizontal regulations, and for administrative simplification.
SPECIFIC	
Cybersecurity	
Cybersecurity Incident Reporting	Apply the "once-only" principle for incident reporting and ensure no duplicated notifications are required by Member States.

[6] For example, the EUDCA, a founding member of the Climate Neutral Data Centre Pact, is already setting industry targets to achieve climate neutrality by 2030. Similarly, industry-based certification schemes or self-regulatory initiatives in areas such as data protection, AI, and cybersecurity can help meet EU-level goals if they ensure equivalent levels of protection.

	Provide clear delimitation (e.g. NIS2 covers operational services, CRA covers products) to avoid double-reporting. Create a European incident reporting meta-platform managed via APIs linking national systems.
Lack of standardised supplier security assessment frameworks	Develop common baseline security controls and tiered supplier classification methodology.
Multiple conformity assessments for integrated products	Provide guidance on the format of conformity output and enable reusing the results for conformity assessments under different legislation Use a format that allows for automation. Consider data spaces where evidence can be stored and reused. Develop pre-approved compliance templates for SME product categories.
Harmonising public procurement requirements	Provide cybersecurity focused standard operating clauses for procurement contracts. ENISA and the ECCC could also play a role in raising awareness and promoting harmonization, helping ensure greater market openness and access to cutting edge cybersecurity solutions.
Data	
Potentially conflicting compliance requirements for actors subject to various legal frameworks	Clearer alignment of the rules, and, where relevant the scope alignment, across the Data Act, the GDPR, ePrivacy, potentially the DMA; transition from RED Delegated Act to CRA.
The AI Act and interplay with other regulations	
High-risk system obligations (AI Act)	Extend or modify modular compliance pathways or exemptions for SMEs (already partially introduced). Create regulatory sandbox routes to allow safe testing before full compliance kicks in (also for public administrations).
Conformity assessments and notified bodies (AI Act)	Allow for shared compliance services — e.g. using AI assurance providers or trusted third-party sandbox environments. Adopt waivers or fast-track assessments for low-complexity, low-volume high-risk systems. Develop EU or national voucher schemes for SMEs to cover conformity costs. Develop a compliance tool – the self-assessment could navigate users through a structured series of questions, categorizing AI systems into four risk levels. Upon completing the assessment, users receive a report containing valuable resources, information on their system's risk level, and advice on how to improve. This approach can be applied to other relevant legislation, including the CRA. Add guidelines for competent authorities to balance fundamental rights with regulatory goals such as enhancing competition, innovation and security.

Duplicative and inconsistent requirements for algorithm use assessments	Align risk assessment cycles and simplify enforcement across Platform Work Directive (PWD) and the AI Act.
The GDPR and the AI Act interplay	Provide joint guidance on areas of intersection between the AI Act and the GDPR. For example, clarifications are required on issues related to data minimisation, bias mitigation, sensitive data and accuracy. Create standardised templates for fundamental rights impact assessments (FRIA) that complement but don't overlap with GDPR data protection impact assessments. On regulatory sandboxes: - establish AI regulatory sandboxes with active involvement of both AI and data protection authorities - establish a common digital platform for sandboxes to facilitate cooperation between national regulators - publish regular sandbox insights, case studies, and success stories to assist organisations in understanding compliance requirements. Develop shared IT tools and coordination platforms for real-time, confidential data exchange. Create joint guidelines and a single auditing framework for holistic assessment of AI systems. Ensure cooperation between the AI Office, the AI Board, and the European Data Protection Board (EDPB). Consider involving European Digital Innovation Hubs (EDIHs) to provide advice to private entities. Provide clarification to allow adapting the GDPR principles for training on a large dataset (for example, that it is a permissible purpose to process personal data in order to anonymise it and include it in a large dataset; but other examples can also come later on). Provide dedicated resources and funding for joint training programmes and seminars for national authorities.

Conclusions

Regulatory simplification is a critical step towards boosting the EU's competitiveness and digital innovation. The consultations undertaken by the Polish Presidency provide a solid foundation for further political momentum. Simplification should result in the emergence of a coherent and clear system of digital law in the European Union and modern and effective digital tools to support the interactions between industry and authorities. We invite all actors to delve into and discuss key ideas and support the accelerated implementation of simplification measures across the EU's digital regulatory landscape.

The Polish Presidency recognises the importance of meaningful stakeholder dialogue and calls upon all future EU Presidencies to commit to regular high-level roundtable meetings with industry

representatives. Stress-testing regulations and adopting simplification measures should not be a one-time exercise, but an ongoing process essential to Europe's digital future and global competitiveness.

List of acronyms:

AMSD - Audiovisual Media Services Directive

AI Act – Artificial Intelligence Act

CER – Critical Entities Resilience Directive

CRA – Cyber Resilience Act

DORA - Digital Operational Resilience Act

DSA – Digital Service Act

GDPR – General Data Protection Regulation

ENISA – European Union Agency for Cyber-security

ECCC - European Cyber Competence Centre

EECC – European Electronic Communications Code

EED – Energy Efficiency Directive

NIS2 – Network and Information Security Directive

P2B – Platform-to-business

PWD – Platform Work Directive

RED – Radio Equipment Directive

UCPD – Unfair Commercial Practices Directive