ITI Promoting Innovation Worldwide

May 2024

Paving the Way for a Competitive, Open and Innovative Europe

Technology Policy Recommendations for the 2024 Hungarian Presidency of the Council of the EU

On 1 July 2024, Hungary will take over the rotating Presidency of the Council of the EU. With EU elections taking place in June 2024, the Hungarian Presidency will have the chance to lay the groundwork for the next cycle of EU technology and innovation policy.

ITI - the Information Technology Industry Council is the global trade association of the technology industry, representing 80 of the world's most innovative technology companies. The technologies our members develop and the investments they make in Europe significantly contribute to the European economy as well as towards Europe's goals for digitalization and the green transition.

Supporting technological innovation and reaping the benefits of technology are crucial policy goals at a time of significant global challenges, including environmental and geopolitical instability. To do so, **the next EU mandate must prioritize boosting the competitiveness and resilience of Europe's economy** and building a more open and well-functioning Single Market as detailed in ITI's manifesto for the next mandate, ITI Vision2030. At the same time, the EU will be stronger and more resilient when tackling these challenges in cooperation and alignment with global like-minded partners.

Following the intense legislative and regulatory activity related to technology in the current mandate, **the Presidency should advocate for time and support for companies to adapt new regulation** and ensure greater attention is placed on coherent, predictable and fair implementation of these initiatives. New EU rules on AI, cybersecurity, data governance, cloud, sustainability, platforms and digital markets are complex and, in some cases, unprecedented. They also apply concurrently and in parallel with existing regimes, such as GDPR, and shared oversight between multiple regulators creates additional new complexity. Prioritizing legal clarity and coherent application of the new rules across the Single Market will boost competitiveness of businesses in the EU and attractiveness for investments.

As the first Presidency of the new mandate, the Hungarian Presidency can play a significant role in championing these objectives in the Council and ensure these will be strategically pursued throughout the next mandate. The below paragraphs contain strategic priorities for the next EU mandate and specific recommendations on active EU workstreams.

We look forward to partnering with the Hungarian Presidency in ensuring these ideas are brought to action.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Strategic Priorities Ahead of the Next EU Mandate

Strengthen the EU's competitiveness and resilience while remaining open:

In an increasingly challenging geopolitical and economic climate, it remains extremely important to strengthen Europe's resilience and ensuring that its fundamental values and interests are protected, while preserving free and open competition, supporting the EU's global competitiveness and enhancing its international leading role.

- The Hungarian presidency should **support an open, collaborative and international-minded approach** to current and future EU policies to support EU digitalization goals in the context of highly integrated global supply chains.

While the EU has sought to assert technological sovereignty to boost Europe's leadership, the EU's digital economy and resilience will be harmed by policies that trend towards protectionism, data localization, preferential or differentiated regulatory treatment of global firms, or fragmented approaches to standardization initiatives.

- The Hungarian Presidency should support the **strengthening of bilateral and multilateral open trade relations** with like-minded international partners, including in forums like the EU-U.S. Trade and Technology Council.

Focus on the implementation of legislative initiatives:

To support innovators in Europe and avoid complexity and fragmentation, the new EU mandate should ensure regulations are well understood by companies and regulators, implemented consistently across the Single Market and work well alongside existing EU rules applying to technology – such as the GDPR. To do so, the Hungarian Presidency should foster implementation and enforcement approaches that create a pro-competitive and stable environment for business in the EU and enable business transformation in line with the EU's economic and competitiveness goals, particularly:

- Support increased coordination between Member States, Regulators, and the Commission to **ensure consistent and predictable application of EU Regulations** across the Single Market.
- Call on the Commission to **launch a process to review potential inconsistencies and fragmentation** of EU and national legislations applying to technology.
- Ensure the Commission and regulators provide **sufficient guidance for businesses** to apply new tech regulations, such as the Data Act, the EU AI Act, Cybersecurity regulations and new repair, eco-design and sustainable finance regulations.

Support better regulation and competitiveness checks:

We call on the Hungarian presidency to support **greater focus on a 'growth enhancing regulatory environment,'** in line with the March 2023 European Council conclusions, aimed at ensuring a proportionate and workable regulatory landscape for businesses in Europe by cutting administrative burden, streamlining reporting requirements and carrying out competitiveness checks on new and existing regulations.[1] To achieve that, we recommend:

- Reviewing how new policy is developed and create time and space early in the new mandate for a period of reflection. Steps should be taken to **revise the EU's better regulation framework** to better assess regulations' likely impact before they are developed and published. Particular attention should be paid to front-loading the process with evidence gathering and consultation in order to make the process open, fair, more transparent, equitable and inclusive for all parties.
- Introducing a **competitiveness check for tech regulations** to assess regulations' contribution to achieving the EU Digital Decade Targets; their human, technical and financial burden on firms;

[1] https://data.consilium.europa.eu/doc/document/ST-4-2023-INIT/en/pdf

their overlap with other regulations; their impact on growth prospects of firms in the EU; and the resources available for regulators to effectively implement regulation.

- Ensuring policies **reflect proportionality, scalability and affordability for businesses** in Europe. Challenges should be solved with an iterative approach that makes use of mixed policy tools such as dialogue with businesses and co-regulation.
- **Prioritizing quality of legislation over speed of any legislative negotiations.** We have seen in the past a tendency to quickly conclude certain negotiations without fully considering the impact of the proposed measures and without sufficient clarity of certain key concepts and terms being considered. This tendency is harmful to better regulation principles, it introduces ambiguous concepts creating additional fragmentation and it undermines the development of an agile and clear legislative framework.

Recommendations on Specific Workstreams

1. Artificial Intelligence (AI)

Support smooth and predictable implementation of the AI Act

As the landmark AI Act Regulation enters into force, it is imperative that policymakers focus their attention on its implementation. For the development of a robust, innovative and globally competitive AI ecosystem in Europe, it will be crucial to ensure legal certainty, guidance and predictable implementation across the EU Single Market.

- Member States are currently either setting up new bodies or appointing different existing regulators (such as telecoms, or consumer protection regulators) for the enforcement of the AI Act. More coordination is needed in this process to deliver a predictable and stable regulatory framework for investment and growth of AI in Europe. Divergent approaches between Member States could lead to different interpretations at national level, especially where authorities have different focus and expertise. This will harm legal certainty and complicate the ability of companies to swiftly operate within the Single Market. **We urge the Hungarian Presidency to promote exchanges and common understanding between Member States and ensure aligned approaches.**
- **The EU AI Act will coexist with several other EU policies applying to AI,** such as the GDPR, cybersecurity regulations, the newly adopted Digital Services Act (DSA), as well as sectoral regulations. **An ambitious assessment of the new body of EU laws applying to technology is needed,** with the aim of identifying and streamlining potential conflicts and overlaps, and guiding business compliance efforts. When it comes to AI, analysis and guidance on the interactions with GDPR is especially important. The Hungarian presidency should support calling on the Commission to pursue this objective.
- **Increased international coordination remains imperative.** AI is developed through global value chains and a common understanding of key concepts across jurisdictions and like-minded countries will be crucial to ensure availability of new technologies, facilitate trade and support the ability of companies to compete globally. To this end, the EU should continue its robust engagement within important multilateral work on AI taking place in forums like the OECD or the G7. For the same reason, **leveraging international standards**, including in upcoming secondary legislation, will be crucial to avoid global regulatory fragmentation which will harm innovation.

Carefully consider impact of potential new rules on AI Liability

The AI Liability Directive (AILD) Proposal remains on the table and the Hungarian Presidency may decide to advance negotiations in Council. We urge a cautious approach to inform the Presidency's decision to continue this work.

- The current EU mandate already finalized the revision of the Product Liability Directive (PLD), which now extends the EU's liability regime for defective products to include intangible elements like software and AI.
- **The combined application of the new PLD and the AILD,** together with the agreed AI Act, **will have an impact on the AI innovation ecosystem in Europe.** To avoid risks of overly complex legal frameworks and in line with the principles of pro-competitiveness regulation referenced in the previous paragraphs, **the Presidency should support a careful assessment of the interplay of the revised PLD and the AILD** before continuing the negotiations. The need for further assessment of possible legal overlaps was also recently referenced in the initial appraisal of the AILD's Impact Assessment made by the European Parliamentary Research Service.[2]

2. Privacy

GDPR Procedural Regulation – A balanced approach to GDPR cross-border enforcement

Consistent, stable and predictable handling of cross-border complaints under the GDPR is critical to enable organizations to innovate responsibly and with confidence. The proposed GDPR Procedural Regulation provides the opportunity to clarify and simplify processes and to consistently provide opportunities for early resolution of cases while reaffirming the One-Stop-Shop principle (OSS principle). While we recognize efforts in the Commission's proposal to streamline procedural rules, ITI is concerned over recent European Parliament amendments that would undermine the OSS principle and confidentiality and turn an administrative process into an adversarial one. In response, ITI urges the Hungarian presidency and the Council to focus on:

- **Reasserting the OSS principle.** The proposal should not dilute or undermine the "leading" competence of the lead supervisory authority (LSA) as maintaining its significant role under Article 56 of the GDPR is the most effective way to handle complaints. The proposals of the European Parliament will weaken the LSA's central role by shifting decision-making and administrative competence to concerned supervisory authorities (CSAs) and the European Data Protection Board (EDPB), thereby fostering fragmented and independent action. The LSA's role is a central pillar of GDPR and cannot be supplanted.
- **Safeguarding the investigated parties' right to be heard in practice at all stages**; in particular, the investigated parties' effective right to be heard before the EDPB during the dispute resolution mechanism procedure must be made explicit. It is crucial that the GDPR Procedural Regulation maintains and clearly articulates the fundamental right to be heard ensuring that it is not merely a formality but a substantive part of every phase of the investigation.
- **Ensuring robust rules on the protection of confidentiality with effective deterrent sanctions.** It is essential for parties involved in proceedings to recognize which documents in the file are confidential. Those who access this information should be prohibited from disclosing it to anyone who is not a party to the proceedings or using the information for any purpose other than the conduct of the inquiry. Keeping inquiry documents confidential is key to preserving the integrity of the decision-making process, and the proposal should strengthen safeguards to this end.
- **Ensuring that the process does not become an adversarial procedure.** GDPR investigations are not designed or intended to be an adversarial process; rather, they are regulatory and administrative in nature, with supervisory authorities representing the interests of the complainant and overseeing implementation and enforcement. These authorities have considerable competences, such as imposing fines under Article 58 of the GDPR, which places a heavier burden on the parties under investigation compared to the complainants. The proposal

[2] https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757810/EPRS_BRI(2024)757810_EN.pdf

should appropriately balance the involvement of the complainant and the investigated party in data protection cases, taking into consideration that the latter face greater repercussions.

- **Incentivizing early resolution and enhancing cooperation and amicable resolutions at all stages.** Parties under investigation should receive any complaint from their LSA without delay at the beginning of the process and be given the opportunity to address it through their internal complaint handling procedures first. The LSA should also be required to facilitate amicable resolution before initiating an investigation.

Support a swift conclusion of the EU-U.S. e-Evidence agreement

It will remain important to promote the swift conclusion of an EU-U.S. Agreement on e-Evidence that allows EU law enforcement authorities to obtain data directly from US technology providers for data stored outside the EU, under the appropriate privacy and human rights safeguards. An agreement would represent an important long-term solution enhancing transatlantic and global public safety, while better protecting customer privacy and increasing trust in cross-border data flows.

3. Connectivity

Future of Connectivity – Regulatory Framework

The publication of the European Commission's White Paper on EU digital infrastructure needs has raised several questions from the tech sector, as it introduces certain ideas that could upend the open nature of the internet architecture and regulatory framework. Even though it recognizes that the IP interconnection market 'generally functions well,' the uncertainties around some of the scenarios in the paper could pave the way for future proposals or a revision of the European Electronic Communications Code (EECC) that introduces network fees in a disguised fashion, and as a result, have severe impacts to European consumers and businesses, competition and the EU's net neutrality principles.

As Hungary will lead discussions in the Telecommunications Council on connectivity, prepare Council conclusions, and work on related policy initiatives in this space we urge the upcoming Presidency to consider the following:

- **Recognition of a well-functioning market**. Legislators should objectively assess evidence of any market failures before considering any new regulatory intervention, drawing on the expertise of independent regulators like BEREC. The Presidency should firmly oppose disguised network fees via, for example, the introduction of mandatory dispute settlement mechanisms and resist destabilizing the current system of settlement-free peering operated by businesses of all sizes. This would make the peering and interconnection market significantly more regulated, and under traditional telecom law rather than the current IP-based model.
- **Smarter de-regulation rather than over-regulation**. A potential broadening of the regulatory framework with the inclusion of cloud service providers and unspecified 'private networks' could generate additional burdens without achieving the Digital Decade's connectivity objectives. We question the 'level playing field' argument that risks imposing traditional telecommunications regulation on different types of services. The EU should instead consider deregulating and harmonizing reporting obligations under the EECC to achieve a functioning Digital Single Market.
    - In addition, cloud and other application-layer services are already subject to a variety of legislative frameworks, for instance regarding interoperability and switching through the Data Act, regarding security through NIS2 and the Cyber Resilience Act, or regarding their obligations towards consumers through the Digital Services Act.

- **Need for clarity and specificity.** The rationale for potentially including cloud service providers and certain private networks in telecoms regulation should be justified and clarified. We urge for a clear explanation of the objectives and potential consequences of any specific regulatory interventions, evidence supporting any such interventions, and how unintended negative impacts on other EU policy priorities, market players, including new entrants, and innovation would be avoided.
- **Technology-neutral approach**. The upcoming Presidency should consider the importance of maintaining a technology-neutral approach to regulation and recognize the role and different ways in which market players contribute to the advancement of Digital Decade targets. For example, a number of technology companies already contribute to European digital networks by investing heavily in infrastructure, services, and products such as data centers, satellite connectivity, subsea cables, content delivery networks, and internet exchange points; products and services that play a complementary, not competing role to telecoms services.

4. Cybersecurity

Bolster Europe's Cybersecurity

To enhance firms' ability to address cybersecurity threats, **it is essential to focus on the implementation of the many new and existing cybersecurity legislations.** It will be particularly crucial to increase coherence of the regulatory framework while avoiding conflicting requirements between legislations such as the NIS2 Directive and the Cyber Resilience Act. The expected review of the Cybersecurity Act and the ongoing implementation of the EU Cybersecurity strategy will also be important to strengthen the EU's cybersecurity capabilities.
In engaging on these crucial workstreams, the Hungarian Presidency should take the following aspects into account:

- **The development processes of EU cybersecurity certification schemes** pursuant to the 2019 Cybersecurity Act **should be more collaborative**, **transparent** and ensure that different stakeholders are duly consulted.
- ENISA's mandate and objectives must also be properly respected so that it remains a technical and independent cybersecurity agency.
- The EU should ensure the various cooperation bodies and mechanisms foreseen under various pieces of legislation (e.g. the Cooperation Board under NIS2 and CRA's Expert Group on Cyber Resilience) are stood up in a timely fashion and their roles and interplay are made clear.
- These goals might be achieved more effectively by **creating more consistency with a Commissioner dedicated to security and cybersecurity** in the next mandate, who should also be entrusted with playing a centralized coordination role to ensure a coherent strategic approach and systematic consultation and involvement of ENISA and national cybersecurity agencies on relevant initiatives by default.

Exclude sovereignty requirements from the EU Cybersecurity Certification Scheme for Cloud Services (EUCS)

ITI supports the development of a harmonized European certification scheme for cloud services, which will be beneficial both for users and service providers. In addition, **we support recent proposals removing the sovereignty requirements from the scheme and maintaining three assurance levels** - "basic", "substantial", and "high", as foreseen by Article 52 of the Cybersecurity Act as well.

The Hungarian Presidency can lead Member States at a political level towards adopting the scheme without the sovereignty requirements as those are discriminatory and politically motivated, and do not inherently enhance the security of cloud services. For instance:

- **Data localization requirements would be detrimental to the EU's cybersecurity landscape**, as they make it more difficult for organizations to exchange datasets stored outside borders, increasing the costs for maintaining state-of-the-art solutions and limiting opportunities for alternative storage in cases of data losses or network outage.
- **Ownership and foreign control criteria would unjustly restrict all non-EU cloud service providers' market access**, hampering competition and innovation in the European market by limiting cloud services options for users, including access to cybersecurity solutions from trusted and allied partners globally.

5. Sustainability

The tech sector plays a crucial role in promoting global sustainability efforts and in improving the environmental, energy, and performance characteristics of products, services, and infrastructure.

Digital technologies, including Artificial Intelligence, can significantly contribute towards achieving the EU's carbon reduction goals. The Hungarian presidency should consider the role of technological innovation as a key driver for achieving the EU's sustainability goals. To do so we make the following recommendations:

- **Streamline reporting obligations** derived from the Green Deal to allow companies easier operations and investments in Europe.
- **Be more ambitious on the digitization of information requirements** across environmental legislation to reduce logistical burdens and to reduce the need for paper-based information.
- Make sure EU legislation always considers the due **differences between B2C and B2B contexts**, especially when coming up with horizontal legislation.
- **Ensure consistency within existing and upcoming EU policies** and provide legal certainty and predictability by avoiding duplicative efforts and conflicting requirements. Any horizontal environmental legislation should remain coherent with the recently approved Ecodesign for Sustainable Products Regulation (ESPR).
- **Ensure coherence between green and digital policy initiatives at EU level**.
- **Address the green transition in cooperation and alignment with the EU's international partners**, reducing barriers to sustainable trade.

Green Claims: a burdenless framework to fight greenwashing

The Green Claims Directive should be aligned with and, where appropriate, defer to the Corporate Sustainability Reporting Directive (CSRD). For example, third-party validation conducted under the CSRD framework should be recognized as a valuable substantiation of any corporate claims made on that base. Moreover, we invite and encourage the upcoming Hungarian Presidency to:

- **Allow other Life-Cycle Assessment (LCA) methodologies** to substantiate environmental claims beyond Product Environmental Footprint (PEF). This is something fundamental as for certain product categories, like software and ICT, the PEF methodology is not appropriate.
- **Allow companies to make environmental claims that account for high quality removals, both technological and nature-based,** provided they abide by strict requirements for transparency,

verification, and certification. The Directive must consider the benefits for informed consumers while fostering investments for corporate climate action.

- **Reconsider the current Council's position on the certificate of conformity of a certain product**. This should be reviewed in case of changes to the product and not according to a set time validity as this would create unnecessary additional burdens for manufacturers.
- **Keep the Council's approach on the exemption from additional verification for traders using third-party environmental labels** (established in a third country) that comply with the requirements set by the Directive. This is fundamental to allow companies to continue using already established and reliable global environmental labels. Limiting environmental labels to EU eco labels only will limit the overall quantity of products rightfully awarded environmental labels.
- **Prioritize digital labelling over physical labelling**: Electronic labelling (e-labelling) via a data carrier (QR code or URL) is preferred over – and should replace where possible – physical markings, as it is the more sustainable alternative.

Tech Sector: the importance of environmental handprint

Emerging technologies have the potential to help Europe reach the decarbonization targets. However, it is fundamental to increase the cross-collaboration of tech companies with different industry verticals and with the institutions. For instance, AI can help mitigating 5-10% of global greenhouse gas (GHG) emissions by 2030, and digital enablement is fundamental to decrease burdens for SMEs. ITI strongly encourages the upcoming Hungarian Presidency to:

- **Make sure that enabling digital tools are considered extensively in the strategies and proposals aimed at reaching the climate objective of reducing GHG emissions** and improving energy performance.
- **Involve tech companies which develop digital solutions in institutional discussions with other industries** to facilitate the identification of challenges and the potential solutions.

6. Illegal Content

Prioritize targeted CSAM detection, upholding privacy and encouraging global coordination

The voluntary commitments to combating the dissemination of child sexual abuse material (CSAM) have been essential for creating a safer and more secure digital space, as well as enabling the detection and prosecution of crime. The recent extension of the derogation of the ePrivacy Directive was a welcome step to avoid any gap in CSAM detection. As the Hungarian Presidency continues the Council work on the CSAM Regulation proposal, ITI encourages the Presidency to work towards an agreement that enables voluntary targeted detection of CSAM as a mitigation measure, continues protecting encrypted messages from detection orders while avoiding generalized monitoring of online platforms and services. In addition, while ITI welcomes the latest proposals in Council for a risk-based categorization of services for issuing more precise detection orders, the Regulation must provide a legal base for mitigation measures for services at all risk levels. The Regulation must also address outstanding concerns about the proportionality of detection orders and potential cybersecurity impacts.

Moreover, ITI calls on the Hungarian Presidency to:

- **Make sure that detection orders are a last resort measure**: these detection orders should only be issued after finding that the provider has failed to take all reasonable and proportionate mitigation measures to address known CSAM risks on their services, including detection where relevant.
- **Limit detection orders to those with the ability to act**: clarify that detection orders should only be issued to those downstream providers with technical and operational ability to act.

The requirements imposed by the Regulation should respect the roles, responsibilities, and capabilities of various actors in the ecosystem.

- **Defend the rights to privacy and confidentiality of communications** through the specific protection of encryption: support exclusion of end-to end- encrypted services from an obligation to scan message contents, as encryption plays a key role in the provision of private and secure communications.
- **Encourage global coordination on reporting of CSAM**: while ITI is generally supportive of the proposed EU Center for Child Protection to help build expertise and capability in the EU and implement the proposed new rules, it is equally important for the EU to help sustain and grow existing international efforts; this includes coordination with U.S. authorities, particularly the NCMEC to ensure reporting requirements are streamlined. In any event, the obligation to report, block, or remove CSAM introduced by this Regulation should not create a conflict that organizations may have in other jurisdictions in which they operate.

7. Standardization

We encourage the upcoming Hungarian Presidency to strictly monitor the developments related to the evolution of the standardization system in Europe. ITI has consistently advocated for **global, open, transparent and consensus-based international standards**. However, in the last years we have witnessed a tendency in Europe towards a more and more regional approach to standards development that could undermine international trade and European competitiveness. Ahead of the **evaluation of Regulation 1025/2012**, and the implementation of recent EU initiatives where standards play a vital role (e.g. Data Act, AI Act, Cyber Resilience Act (CRA), etc.) we urge the Hungarian Presidency to consider the following:

- **Standards development processes should not exclude or limit participation of non-European headquartered stakeholders or non-European standards experts.** Inclusivity is crucial to develop standards that guarantee interoperability and reduce trade barriers across the world, ultimately favoring European SMEs.
- **It is crucial to maintain the central role that European Standardization Organizations** (ESOs) **have in standards development**, especially regarding sectoral knowledge. The role of the European Telecommunications Standards Institute (ETSI) in relation to telecommunications and ICT sector standardization is key and must be preserved.
- **Common or technical specifications should be used as a last resort** and not be utilized as a mechanism by the European Commission to impose standards unilaterally.
- Member States should advocate for consensus-based standards developed in collaboration with industry stakeholders. Excluding industry from decision-making processes may lead to a decreased market relevance of European standards and hamper their broad adoption, undermining competitiveness while trying to guarantee economic security.

***