Adopting a Pro-Innovation Agenda for Europe: 10 Key Policy Recommendations for the EU Czech Presidency
1 July – 31 December 2022

On 1 July, the Czech Republic will take over the Presidency of the Council of the European Union. To support the new Presidency’s development and implementation of its digital agenda, ITI identified several key policy areas that are crucial for communities and companies in the EU and will further drive Europe’s leadership in the global digital economy.

The upcoming Czech Presidency has the opportunity to take a clear stance for an open and trade-oriented approach to EU policy. Now more than ever, Europe needs to lead a pro-innovation, global and transatlantic agenda. ITI acknowledges the sincere public interest objectives that the EU is pursuing with its tech policy agenda. However, we believe that strategic autonomy should not mean protectionism, data localisation, disrupted data flows, preferential or otherwise differentiated regulatory treatment of global, non-European headquartered businesses, or fragmented approaches to standardisation policy. Rather, open, collaborative and international-minded approaches will be key to ensuring availability of critical technologies in Europe in the context of highly integrated global supply chains and contributing to the EU’s digitalisation goals. It is also crucial that legislative and regulatory initiatives seek consistency and avoid overlapping or conflicting requirements, whose cumulative effect would have a negative impact on innovation and competitiveness in Europe. Alignment with global partners and broad stakeholder engagement on these initiatives is a crucial component for success. In this context, we strongly support the upcoming Presidency’s open dialogue and the early signals of its intention to be closely involved in initiatives that are indirectly related to the traditional presidency’s role, like for example the EU-US Trade and Technology Council, and the evolution of the Trans-Atlantic Data Privacy Framework (TADPF).

Below you find ITI’s specific recommendations for these and other key initiatives and legislative proceedings. ITI looks forward and stands ready to support the Czech Presidency in its pursuit for digital policy which preserves an enabling environment for innovation and ensures the EU’s global competitiveness and security.

1. Artificial Intelligence – Ensure a Risk-Based and Innovation-Friendly Approach to AI Regulation

The wide variety of possible uses of Artificial Intelligence (AI) represents a huge opportunity for economies and societies around the world. Encouraging innovation in and uptake of these technologies is rightly a fundamental public policy goal. At the same time, in order to manage risks that may arise from some uses of AI, the EU has been a first mover globally in proposing horizontal AI

---

1 The Information Technology Industry Council (ITI) is the premier advocate and thought leader around the world for the technology industry. ITI’s membership is comprised of 80 of the leading technology and innovation companies from all corners of the information and communications technology (ICT) sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, and Internet companies.
regulation with the EU AI Act. In this context, it is important that the AI Act takes a truly risk-based approach, to address risks to fundamental rights and safety that some uses of AI can create, without burdening AI deployment in the majority of non-risky AI uses.

As the Presidency moves forward with the negotiations in Council, ITI has identified a set of key recommendations to ensure a pro-innovation and future-oriented legal framework:

- The definition of AI should be more targeted to differentiate between 1) traditional software that operates according to predictable and relatively static rules and 2) AI systems capable of self-learning or self-adjusting. The definition should also build on the Organisation of Economic Co-operation and Development’s (OECD) proposed definition of AI to ensure alignment with global partners.
- Target the list of high-risk AI use cases only to those that pose a risk to safety or fundamental rights and make a final decision that materializes that risk. This will help addressing risky AI without covering non-problematic uses.
- Subjecting all general-purpose software (i.e., software that can be adapted for a variety of tasks such as image or voice recognition, and thus does not have an intended purpose) to the requirements of the AI Act is not proportionate and does not follow the risk-based approach at the basis of the AI Act proposal. Only where general-purpose software is implemented into a high-risk AI use case it should be subject to the requirements of the Act.
- Requirements should be goal-oriented, rather than prescriptive, so that companies can apply to the different use cases in scope of the Act the most meaningful and appropriate measures to ensure compliance, without affecting the objectives of the regulation.
- The Act should allow responsible deployment of biometric identification for national security or law enforcement purposes under strict and meaningful safeguards. Use of biometric identification for other purposes should be subject to the provisions for high-risk AI systems.
- The proposal should better promote reliance on international industry-driven consensus-based standards to avoid fragmentation with global regulatory environments. Global industry-driven standards should also be used for demonstrating conformity to the requirements of the AI Act.
- The proposal should foresee greater acceptance of international testing outcomes. Considering that Conformity Assessment for AI is a nascent field, for which there is not a commonly understood practice or infrastructure available, this would help avoid backlogs in testing procedures and better account for the global nature of the technology.

2. European Cloud Certification Scheme (EUCS) - Establish a Technical-based Cloud Certification Scheme

ITI appreciates the efforts from the European Commission and ENISA to protect data, systems and infrastructure from anomalous behavior and prevent unauthorised access. We believe that a harmonised European approach for a Cybersecurity Certification Scheme for Cloud Services (EUCS) would be most beneficial for users and service providers. However, it is crucial that the process of developing the EUCS is transparent and that there is no fragmentation among Member States on ENISA’s final proposal. In this respect, the Presidency can lead by crafting a unified position among Member States at a political level and to strengthen cybersecurity efforts by offering technical-based recommendations in the EUCS.

ITI has identified some recommendations that could support the Presidency and help reach the EU’s ambition to tackle cyber threats and increase trust and security in important products and services:

- Requirements that relate to legal aspects, organisational structure, and investment and ownership, are unrelated to technical-based certification of cloud services or improvement of cybersecurity and should be avoided in the EUCS.
• Considerations around foreign jurisdiction and control over data are more related to subjective considerations over “sovereignty” than to actual cybersecurity practices and should be discouraged.
• Cybersecurity certifications should focus on the objective and universal goal of keeping data secure from cybersecurity threats.
• The creation of (indirect) data localisation requirements in the EUCS would hurt the EU’s cybersecurity landscape as it would 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.
• Co-operation between ENISA and industry is essential, and the opinion of the Stakeholder Cybersecurity Certification Workgroup (SCCG) is highly relevant in the further development of the EUCS.

3. Cyber Resilience – Take a Horizontal Phased Approach that Avoids Fragmentation and Duplication
ITI supports the EU's efforts to improve cybersecurity resilience across all key economic sectors. As the Commission is expected to adopt the Cyber Resilience Act (CRA) proposal during the Czech Council Presidency, ITI would like to share some recommendations on how the CRA can help improve cybersecurity across the EU and protect digital products and ancillary services while aligning with and progressing further from existing cybersecurity legislation such as the Cybersecurity Act, the General Product Safety Directive, the Machinery Directive, the Radio Equipment Directive, the proposal for an AI Act, and the NIS2 Directive:

ITI's recommendations:
• To strengthen the entire cybersecurity system, the CRA should be able to overrule existing national legislation covering digital products and ancillary services and ensure coherence with existing and planned EU legislation, as means of avoiding fragmentation and duplication.
• The CRA must take a risk-based approach and encompass a clear scope and definitions, taking into account differences in the development, functionality and use of digital products. A risk-based approach should be introduced, comprised of a risk assessment, which would also include an assessment of the end-use of the product or service.
• The CRA should take a phased approach where it seeks to solve challenges iteratively, further developing and improving approaches as the rollout progresses.
• The proposal should align with industry-driven global standards, as these standards provide widely vetted, consensus-based information and guidance for defining and implementing effective security methodologies.
• The CRA should introduce a voluntary mixed policy approach with a horizontal regulatory intervention for a wide variety of tangible products and ancillary services in combination with soft measures for non-embedded software.

4. Data Act – Achieve a Balanced and Fair Framework for Data Sharing and Portability
ITI supports the overall goal of the Data Act to facilitate data access and use, and promote data sharing while preserving incentives to invest in data innovation and in the EU Digital Single Market and safeguarding individuals’ rights.

The objectives of the Data Act can be best achieved through ensuring legal, political, and policy alignment with existing EU data regulation, and encouraging sharing of data between companies on the basis of contractual agreements that can effectively protect businesses’ investments in data innovation. Efforts to improve cloud switching and data portability should be realistic, meaningful and
ITI’s Policy Recommendations for the Czech Presidency of the EU

ITI’s recommendations:

- The presidency should seek to clarify key concepts which are at the core of the new data access and sharing rules. Greater clarity and more targeted definitions of “data”, “data holder”, “data user”, “related service” and “product” would ensure legal certainty, foster trust, and avoid confusion regarding the products covered or the obligations of the different actors in the data value chain.
- Stronger protection for IP, trade secrets and against unfair competition vis-à-vis users and third parties should be ensured. Data holders should share trade secrets only on a voluntary basis.
- Provisions on government access to data should be clear, balanced and proportionate. This could be achieved by developing a more stringent definition of situations that would constitute an “exceptional need” and ensuring that companies’ data and rights of third parties are protected.
- Provisions on switching between cloud services should be better tailored to take into account the different scenarios, the variety of cloud services, the shared responsibility of the service provider and the customer, the data at play and its volume, the need of technical assistance, and the switching costs. Legislators should ensure that switching requirements are practical, feasible, and based on industry best practices.
- Current provisions on international transfers of non-personal data held by cloud providers are disproportionate and would unjustifiably restrict the flow of non-personal data across borders. Non personal data are rarely, if ever, the subject of government access requests and they should not be subject to restrictions similar to personal data, given their limited impact on fundamental rights. Concerns about government access to data should be dealt with in bilateral or multilateral conversations with global partners.

5. Semiconductors – Swiftly Adopt the Chips Act Regulation to Increase Semiconductor Supply Chain Resilience

Semiconductors are the fundamental enablers of the digital and green transition, and they contribute to the advancement of new, world changing technologies like 5G and 6G; Internet of Things (IoT); Artificial Intelligence (AI); enhanced cloud services; and quantum computing.

ITI strongly welcomes the EU’s goal to strengthen the availability of semiconductor technologies, increase the EU’s global market share and support the resilience of supply chains in the newly proposed European Chips Act. The Czech Presidency should aim for a swift adoption of the European Chips Act to make sure we have the right tools in place to achieve these critical objectives. We highlight the following key points:

- Pillar I investments should target all technology nodes while investment and incentives should be available to all manufacturers who meet the agreed standards and guidelines. Furthermore, to increase IP protection, stronger legal safeguards are needed against any circumvention of technological protection measures and use of confidential data contained in chips.
- Clarifications on the designation process of “first-of-a-kind facility” under Pillar II would be useful.
- The monitoring and crisis response mechanism should be balanced, practical and proportionate. Industry stakeholders should be involved in the definition of early warning indicators and should be consulted by the Commission when it decides to take measures to
address a crisis scenario. Further clarity on the definition of crisis and the process to activate the crisis scenario are needed.

- Our industry is concerned with the provisions that would allow the Commission to impose the prioritisation of certain orders for certain sectors in Pillar III. This would create significant burdens for companies and risk disrupting complex manufacturing processes. Policymakers should not interfere in the market allocation of supply, even in the short-term.

- Further industry participation in the Semiconductor Board is fundamental given the Board’s competence on complex technical subjects like chip production, technologies, certification, identification of and action on potential shortage scenarios. Industry players should have permanent membership of the Semiconductor Board sub-groups, as well as voting rights on its proposed decisions.

- Given the global nature of the supply chain, the EU should work with like-minded partners and allies such as the U.S., Japan, South Korea, Taiwan, Singapore and others to ensure stability of the global semiconductor supply chain.

6. Data Flows - Swiftly Finalise the Transatlantic Data Privacy Framework (TADPF)
On March 25, 2022, U.S President Joe Biden and European Commission President Ursula von der Leyen announced in Brussels a political agreement on a new Transatlantic Data Privacy Framework (TADPF) to replace the 2016 Privacy Shield Framework. Cross-border data flows between the U.S. and the EU are the largest in the world, underpinning over 16 million jobs and more than $5.6 trillion in commercial economic activity annually. The TADPF will allow European citizens’ personal data to be transmitted to and stored on U.S. soil while safeguarding their privacy and civil liberties.

The incoming Presidency can have a great influence on the ongoing negotiations and foster greater alignments between the EU and U.S. As such, ITI offers specific recommendations that take into account privacy, security, and economic issues while encouraging transparent and appropriate enforcement. A draft adequacy decision by the European Commission making the agreement operational is expected during the Czech Presidency semester – as the decision will need to be approved by Member States, the Presidency will have opportunity to play a crucial role in coordinating and driving this forward. In this context, ITI recommends the following:

- A swift finalisation of the TADPF to restore business certainty and safeguard the continuity of commercial activities involving the movement of data across borders.

- The TADPF must address concerns regarding U.S. national security authorities access to data and offer an adequate redress mechanism for EU citizens, which is consistent with both EU and US law.

- It should contain provisions to address the necessity and proportionality of U.S. surveillance, which will form the basis of a durable agreement.

- The TADPF must recognize the potential implications of data flows, adopt approaches that facilitate data transfers while protecting data, and avoid data localization, which is harmful to transatlantic trade and reduces access to real-time data-backed services that can only be provided through seamless international data flows.

7. EU-U.S. Trade and Technology Council (TTC) - Promoting Ambitious Outcomes in the TTC
The months between the first and second ministerial meetings of the U.S.-EU Technology and Trade Council (TTC) yielded significant engagement across the 10 working groups of the TTC. ITI strongly supports the TTC as a forum to advance new and emerging technologies, mitigate climate change, and enhancing security, market access and resiliency, and looks forward to continuing partnering with governments to ensure the TTC’s ongoing success. As the TTC moves forwards and prepares for the
next meetings under the Czech Presidency, ITI offers the following recommendations to increase EU and U.S. competitiveness and promote democratic and market-oriented values:

- Accelerate research and development for 6G. The rapid pace of technological innovation and the intensity of investments in R&D by the private sector in next generation wireless communications provide an opportunity for the TTC to supplement this activity by supporting transatlantic R&D collaboration among private sector and academic institutions in the U.S. and EU.
- Commit to relying on internationally recognised, industry-driven, voluntary technical standards. This will be a powerful opportunity to model openness, reliance on global expertise, non-discrimination, and interoperability as core tenets of good governance.
- Support more resilient and secure supply chains for semiconductors and the broader ICT industry. As governments and the EU continue to develop and implement funding, incentives, and other programming for semiconductors, the TTC should commit to making schemes accessible to all technology companies that meet the agreed-upon standards and guidelines, without prioritizing domestic companies over non-domestic ones.
- Continue to collaborate on AI standards and AI governance and develop a set of common risk evaluation criteria. Such a set of criteria will ideally foster a common understanding of what sorts of characteristics might constitute a high-risk application.
- Enforce multilateral commitments that benefit U.S. and EU workers and companies.
- Coordinate engagement to address third-market policies of concern, such as increased data flow restrictions in privacy and data governance proposals.

8. Ecodesign for Sustainable Products Regulation (ESPR) - Improve Sustainability of Products while Preserving Innovation

The tech sector plays a crucial role in promoting global sustainability efforts and in improving the environmental, energy, and performance characteristics of products. ITI shares the goals of the ESPR proposal to improve sustainability and circularity of products and welcomes the harmonisation of ecodesign requirements at EU level, thus preventing fragmentation and ensuring legal certainty for manufacturers and other economic actors. Going forward, the Presidency should ensure consistency with existing and upcoming EU policies and preserve innovation. In particular:

- Legislators should clarify requirements in order to avoid the risk of duplicating efforts and burdens under existing sectorial legislation.
- Requirements related to the Digital Product Passport should be feasible and easy to implement for businesses and should ensure the protection of sensitive business information.
- We recommend broad stakeholder consultations and participation in the preparation of delegated acts setting ecodesign requirements for a specific product group.
- Simplifying information requirements on unsold consumer products and adopting a targeted approach, focusing on specific areas where a significant negative environmental impact was identified, would ensure achieving the EU’s environmental goals without creating unnecessary burdens for businesses.

9. Digital Decade – Advance the Digital Transition

The 2030 Policy Programme “Path to the Digital Decade” is an opportunity for the European Union to set the direction for its digital transformation by establishing clear objectives and a transparent monitoring mechanism. We believe that the digital transition is global and should be addressed in cooperation and alignment with the EU’s international partners. Open trade and cooperation with international partners can be crucial to ensure supply chain resilience and availability of key technologies. Moving forward with the Programme, the Presidency should focus on finding global
convergence in order to ensure that the Union reaches its goals in the areas of digital and cloud infrastructure, semiconductors, and artificial intelligence uptake, through the following:

- Strengthening the digital skills of the EU’s present and future workforce will contribute to strengthen the long-term competitiveness of the EU’s technology industry. Investments in STEM and computer education and training programmes, including for underrepresented minorities and women, is necessary in order to respond to the growing demand for highly skilled digital professionals.

- While we recognise and support the aim to ensure broad 5G coverage, we encourage the Presidency to broaden the scope of the digital infrastructure targets and include other technologies, such as WiFi. These technologies are complementary and respond to different needs, therefore, ensuring the right balance between them is important for achieving the connectivity targets.

- Increasing international cooperation with key like-minded partners such as the US, Japan, South Korea, Taiwan and Singapore will be fundamental to ensure long term availability of critical technologies and boost the EU digitalisation goals in the context of globalised supply chains. Digital partnership and dialogues should be sought with these key partners.

10. E-Privacy – Ensure Alignment with GDPR’s Risk-Based Approach
ITI appreciates the efforts that that were made during the e-Privacy Regulation (EPR) trilogue negotiations in promoting privacy for European users while seeking to promote innovation and the provision of digital services at the same time. However, further discussions remain needed to provide clarity and further alignment with the GDPR. Therefore, ITI is pleased to hear that the Czech presidency intends to make further progress. As a way of support, we recommend:

- Further improvement on the clarity and alignment between the GDPR and EPR is needed. This should be done by synchronizing Article 6 EPR with Article 6 GDPR legal grounds for processing, which includes harmonising the “performance of a contract”, and by introducing compatible further use for electronic communications metadata.

- The EPR should not hinder the goal of sharing data for good. Prohibitions on sharing electronic communications data and terminal equipment data is in practice incompatible with the way the digital economy operates and not proportionate to the risk associated with sharing it.

- Simplification of the EPR structure is needed to avoid overlapping requirements on different types of data.

- Clear enforcement structures are needed and should be modeled after the GDPR.