INSTITUTE OF INTERNATIONAL RELATIONS PRAGUE

Think Visegrad
V4 Think-Tank Platform

MAPPING DIGITAL TRADE REGULATIONS IN CENTRAL EUROPE: REGIONAL TRENDS AND THE CZECH CASE

TOMÁS ROGALER

Summary

The regulatory environment for digital trade in Czechia, Hungary, Poland, and Slovakia shapes how these economies integrate into the regional and global digital economy, yet the relevant systematic comparative evidence remains limited. This paper maps the restrictive and enabling policies affecting digital trade across the Visegrad (V4) countries while following the Digital Trade Integration (DTI) Project methodology. It argues that EU-wide rules create a broadly similar regulatory baseline across the V4, while national policies and implementation choices still determine how enabling or restrictive the environment is in practice. The analysis shows the countries' convergence around the EU framework, but also their divergences in areas such as cross-border data policies and public procurement. The paper complements this regional assessment with an in-depth case study of Czechia combining legal analysis with qualitative insights from stakeholder interviews. The findings indicate that Czechia is broadly open and enabling in the areas of tariffs on ICT goods, FDI, and telecommunications, yet faces bottlenecks linked to data-related compliance costs and the legal framework for digital contracts and copyright, which weigh disproportionately on SMEs and digital services firms. By linking formal frameworks with practical outcomes, the study offers evidence-based recommendations to support more proportionate regulation in Czechia and foster deeper digital trade integration across the V4.

INTRODUCTION

The rapid expansion of digital trade[1] has reshaped the global economy, with digital activities now estimated to account for approx. 15–25% of global GDP (World Bank, 2022; López González, Sorescu, & Kaynak, 2023; OECD, 2025). The growth of digital technologies has enabled the remote delivery of services that once required physical proximity, lowering transaction costs and opening new opportunities for firms to participate in global markets (Freund & Weinhold, 2002, 2004; López González & Ferencz, 2018). At the same time, this evolution has exposed the limits of traditional, offline-oriented trade rules and drawn attention to regulatory areas such as data governance, privacy, and cybersecurity, which now play a central role in shaping online transactions (Burri & Chander, 2023; Burri et al., 2024).

In response, economies have adapted their regulatory frameworks, but their approaches differ, as they reflect diverse policy priorities and levels of institutional capacity (Evenett & Fritz, 2022; Ferracane, González, & Rogaler 2025a). International organisations and research initiatives, including UN-ECLAC, UN-ECA, UN-ESCAP and the DTI Project, LINK have worked on assessing these legal frameworks from the perspective of "digital trade integration", which refers to fostering cross-border flows of information and communication technology (ICT) goods, online services, data and the related investment by removing regulatory barriers and adopting enabling measures (Ferracane, 2022; ESCAP et al., 2024; Ferracane & Rogaler 2025a). Drawing on the DTI Project's methodology (Ferracane, 2022), these initiatives have offered a comprehensive picture of regulatory trends and produced comparable results that support empirical research on how regulation impacts digital trade flows (Ferracane & van der Marel, 2023; Ferracane, González Ugarte, & van der Marel, 2025).

These assessments are particularly relevant in the EU, where an extensive body of supranational rules coexists with national regulations and shapes domestic policy choices. Understanding how this multi-level governance influences member states' regulatory frameworks, and how it affects smaller economies in particular, is therefore crucial. In this context, the Visegrad countries (V4) – Czechia, Hungary, Poland, and Slovakia – offer a pertinent example: despite the centrality of their digital trade regimes for regional and global integration, systematic comparative assessments of their regulatory approaches remain scarce.

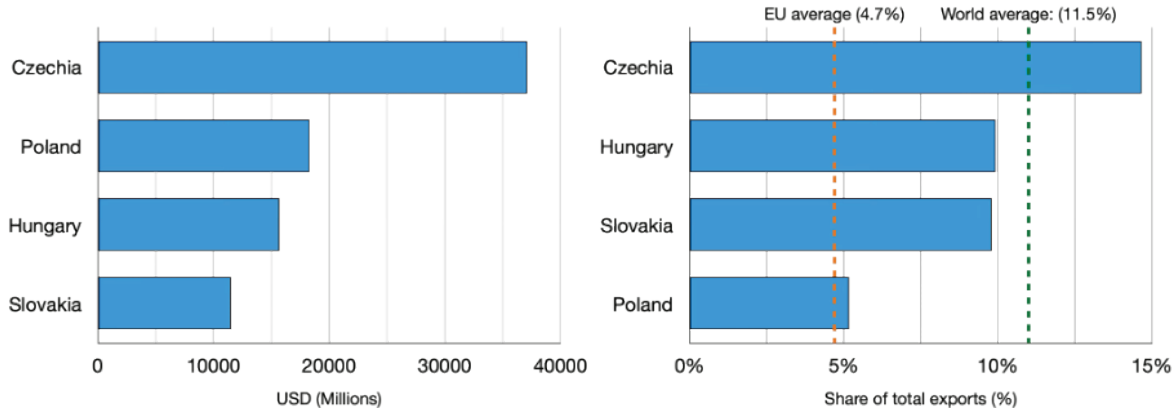
This policy paper addresses that gap by mapping the key restrictive and enabling measures affecting digital trade across the V4, using the DTI Project methodology, and examining the extent to which EU legislation creates a common baseline or leaves room for national divergence. Section I outlines the digital trade landscape in the V4, while Section II maps the countries' regulatory frameworks using DTI indicators, and Section III discusses some selected EU-wide measures that are particularly relevant for the region. Building on this comparative analysis, Section IV develops a detailed case study of Czechia combining legal and documentary analysis with qualitative insights from semi-structured interviews to identify the main regulatory bottlenecks and enablers as perceived by firms and other stakeholders. For Czech policy-makers, Sections IV and V constitute the heart of the paper, with Section V distilling the main findings into concrete policy recommendations for Czechia.

I. DIGITAL TRADE IN THE V4 COUNTRIES

In 2023, the Visegrad Group countries recorded high export volumes of ICT goods, ranking above many EU member states and, in some cases, above global averages in this regard. Out of the four countries, Czechia exported the highest value of ICT goods, with a total of USD 37.1 billion (Figure 1). By contrast, Slovakia had the lowest value of ICT goods exports of the V4 countries, with a total of USD 11.4 billion. Poland and Hungary ranked in the middle, exporting volumes of ICT goods with values of USD 18.2 billion and USD 15.6 billion, respectively.

Moreover, when examining the shares of these products in total exports, Czechia also records the highest proportion at 14.65%. This figure is not only well above the EU average of 4.7% but also exceeds the global average of 11.5% (Figure 1). Conversely, Poland registers the lowest share: 5.16% of its total exports. In between are Hungary and Slovakia, with almost identical shares of 9.9% and 9.8%, respectively. It is noteworthy that although Czechia is the only V4 country whose share surpasses the global average, all the V4 countries report values above the EU average (4.7%), indicating that these products represent a significant component of their export structures.

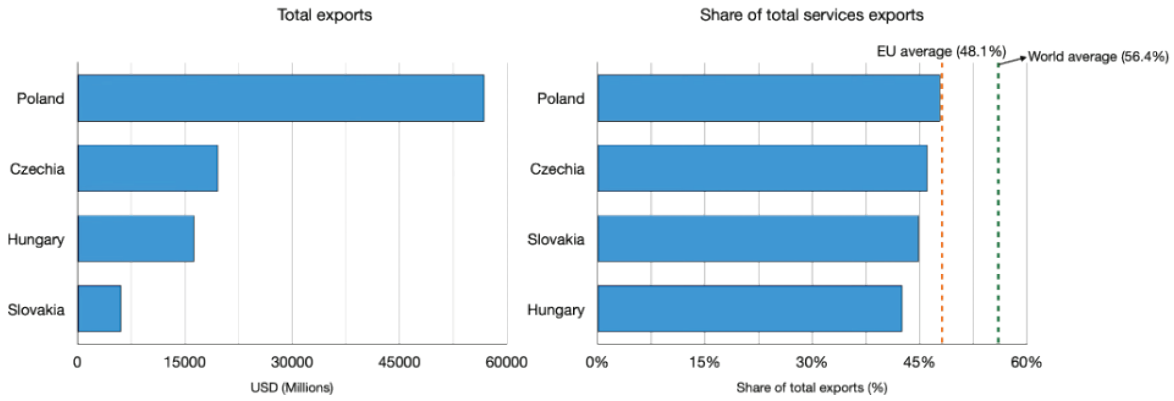
Figure 1: ICT goods exports: total volumes and shares in total goods exports in 2023



Source: UNCTAD (2025). Note: The data for the world and EU averages refer to the year 2023.

For digital services, the countries' trade performance contrasts dramatically with that in ICT goods exports, with Poland ranking first (Figure 2). In 2024, the country exported a total of USD 56.8 billion in digital services, which was more than the combined digital services exports of the other three countries. Slovakia once again appears as the country with the lowest export value in this variable, with a total of USD 6.1 million. Meanwhile, Czechia and Hungary have similar values, with totals of USD 19.6 billion and USD 16.3 billion, respectively.

Figure 2: Digital services exports: total volumes and shares in total goods exports in 2024



Source: UNCTAD (2025). Note: The data for the world and EU averages refer to the year 2024, and exclude Malta, for which such data is not available.

Similarly, Poland recorded the highest share of digital services exports in its total exports: 47.9% (Figure 2). The other peer countries followed closely, with shares of 46.1% for Czechia, 44.9% for Slovakia, and 42.6% for Hungary. However, in contrast to their performance in ICT goods exports, here none of the V4 countries surpasses either the EU average (48.1%) or the global average (56.4%), which indicates a scope for further policy efforts to stimulate growth in this segment of trade.

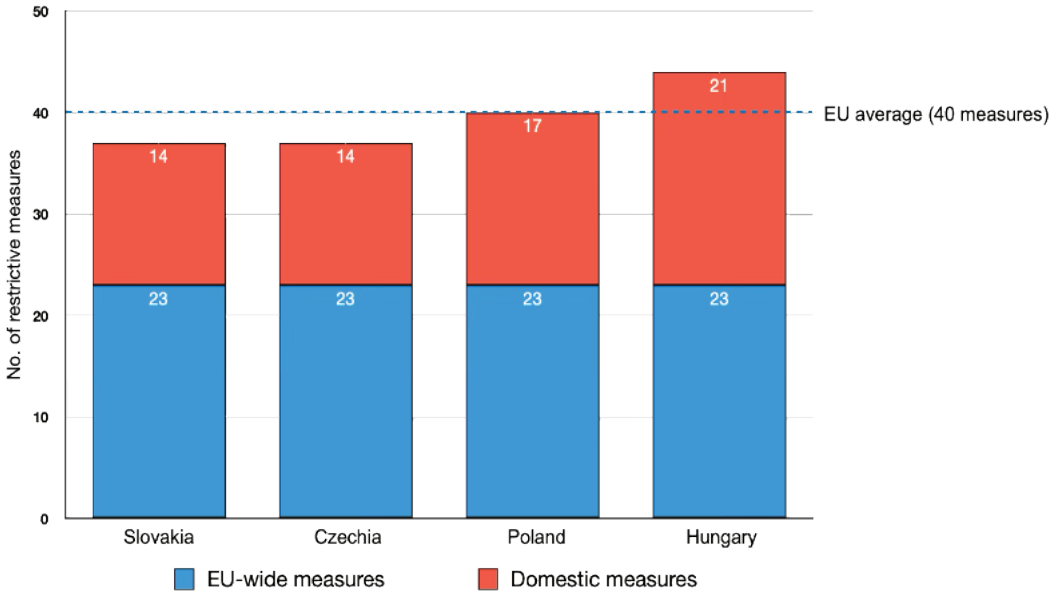
II. MAPPING THE DIGITAL TRADE POLICY LANDSCAPE OF THE VISEGRAD GROUP

This section examines the regulatory frameworks of the V4 countries as of 2024 based on desk research combining primary legal sources and secondary literature. Using the DTI Project methodology, LINK it identifies restrictive and enabling measures affecting ICT goods, digital services, relevant data and investment in sectors related to digital trade, and incorporates relevant multilateral commitments (Ferracane, González, & Rogaler 2025a).

Within this framework, a measure is classified as restrictive when it discriminates against foreign providers, imposes stricter conditions on online than on offline trade, or is particularly trade distortive in achieving its economic objective. It is considered enabling when it fosters trust in digital trade or reflects international commitments that enhance transparency and interoperability; the absence of an enabling measure is also treated as a restriction.[2] Figure 3 presents the total numbers of restrictive measures implemented by the

V4 economies. These measures are differentiated by two colours, red and blue, which respectively represent domestic measures and EU-wide measures – such as EU regulations, directives, trade defence measures, and signatures/adoptions of multilateral agreements within the EU framework – applied by these countries.

Figure 3: The total numbers of restrictive measures of the V4 countries



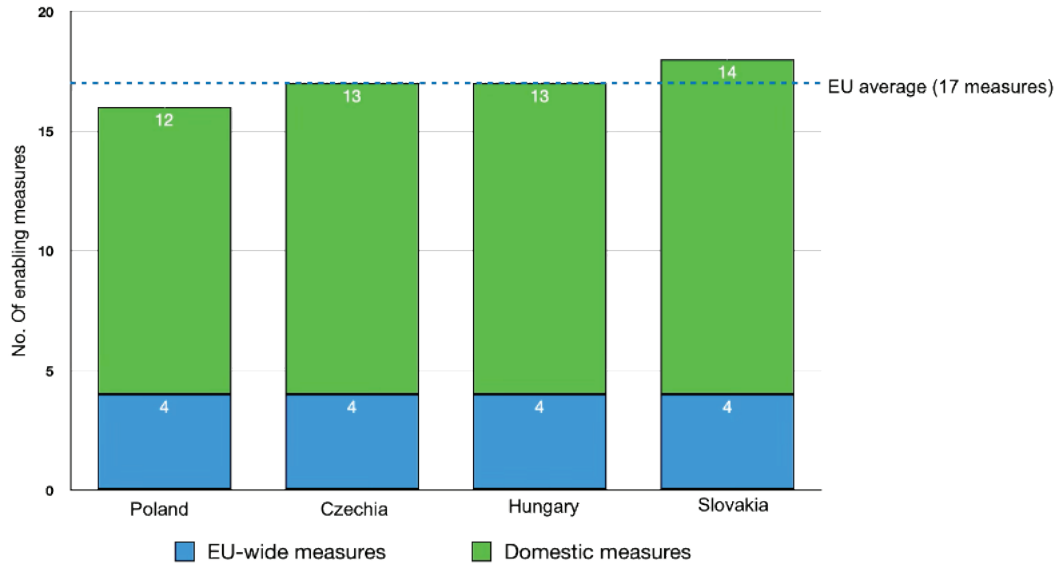
Source: Author. The average for European countries is based on 2023 data for all the EU Member States except for the V4 members. The data is available in the DTI database. LINK

Hungary records the highest number of restrictive measures (44, of which 21 are national), followed by Poland (40, with 17 national ones). Czechia and Slovakia each register 37 measures, including 14 national ones. The four countries display broadly similar levels of restrictiveness, both among themselves and in comparison with other EU Member States, with Hungary slightly above the EU average and Slovakia and Czechia slightly below it. The strong presence of EU-wide measures points to a shared baseline and a nominal convergence in digital trade governance.

On the enabling side, Figure 4 shows the numbers of measures that facilitate digital trade, again distinguishing domestic provisions (green) from EU-wide rules (blue). Slovakia stands out with 18 enabling measures (14 domestic and 4 EU-wide), which make it both one of the least restrictive V4 economies and the most enabling one, and place it above the regional average of 17 measures. Hungary and Czechia follow with 17 measures (13 domestic ones) each, while Poland registers 16. Once again, the countries all have relatively similar numbers of measures,

both among themselves and in comparison with other EU Member States; however, their adoption of measures at EU level does not have a major impact, as each of them has only four EU-wide measures.

Figure 4: The total numbers of enabling measures of the V4 countries



Source: Author. The average for the European countries is based on 2023 data for all the EU Member States except for the V4 members. The data is available in the DTI database. LINK

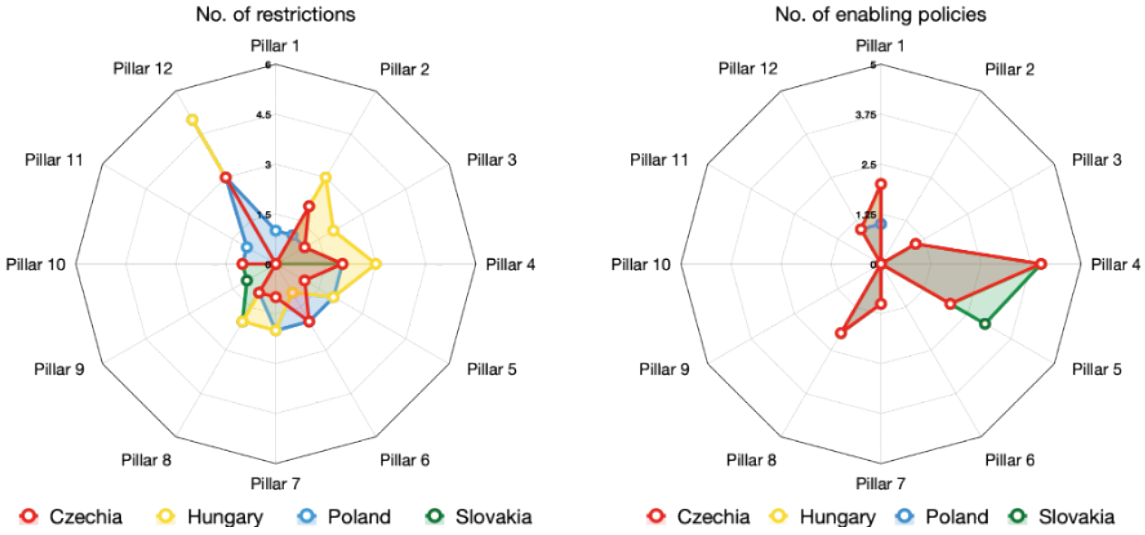
Yet, despite the common baseline established by the EU framework and the broadly comparable numbers of measures adopted across these economies, this does not necessarily imply that the Visegrad countries possess identical regulatory structures. Their divergence becomes evident when examining the distribution of measures across the different DTI policy pillars.

The DTI framework[3] groups measures into 65 indicators organised under 12 policy pillars covering tariffs and trade defence for ICT goods, public procurement, FDI, IPRs, telecom infrastructure and competition, cross-border and domestic data policies, intermediary liability, content access, quantitative trade restrictions, technical standards, and online sales and transactions. Figure 5 compares the numbers of domestic restrictive and enabling measures under these pillars.

The V4 countries apply relatively few restrictions on tariffs, foreign direct investment (FDI) in sectors relevant for digital trade, content access, quantitative trade restrictions and technical standards (Pillars 1, 3, 9, 10 and 11), while more restrictive environments emerge in the areas of public procurement, IPRs, cross-border and domestic data policies, intermediary liability and online sales (Pillars 2, 4, 6, 7, 8 and 12). Hungary shows the highest level of regulatory

intervention, particularly in public procurement, FDI, IPRs and online transactions (Pillars 2, 3, 4 and 12). Poland adopts a more balanced approach by spreading its restrictions across most of the pillars. Czechia concentrates its restrictions on cross-border data policies and online transactions (Pillars 6 and 12), whereas Slovakia is comparatively open but still introduced some limits on online transactions.

Figure 5: Numbers of domestic measures implemented by the V4 countries under the DTI pillar

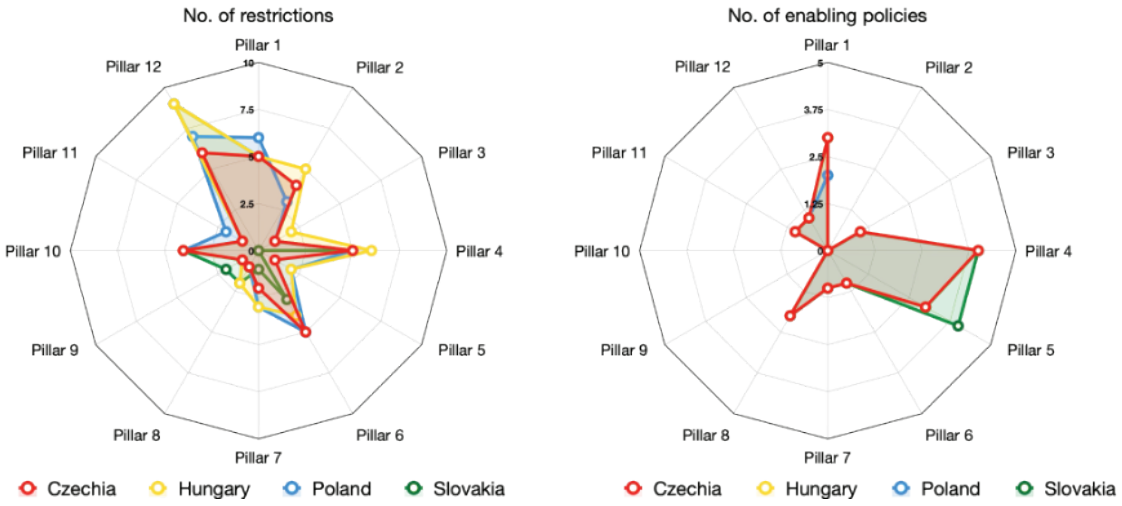


Source: Author. The data is available in the DTI database. LINK

On the enabling side, the right-hand panel of Figure 5 indicates that the V4 countries have identical or nearly identical numbers of facilitating measures under most of the pillars, with IPRs (Pillar 4) showing the highest concentration, and telecom infrastructure and competition (Pillar 5) and intermediary liability (Pillar 8) also recording moderate levels of facilitation. Slovakia marginally exceeds its peers in telecoms (Pillar 5), while otherwise the distribution of enabling measures remains similar across the countries.

When EU-wide measures are added to domestic ones (Figure 6), the regulatory landscape becomes denser and more homogeneous, which underscores the influence of supranational frameworks on national digital trade governance. The incorporation of EU rules substantially increases the number of restrictive measures in tariffs and trade defence for ICT goods, IPRs, cross-border data policies, quantitative trade restrictions and online sales (Pillars 1, 4, 6, 10 and 12). For enabling measures, EU-wide provisions reinforce alignment, with the four economies registering similar values in areas such as tariffs and trade defence (Pillar 1), IPRs (Pillar 4), telecom infrastructure and competition (Pillar 5) and intermediary liability (Pillar 8).

Figure 6: Total numbers of measures implemented by the V4 countries by DTI pillar

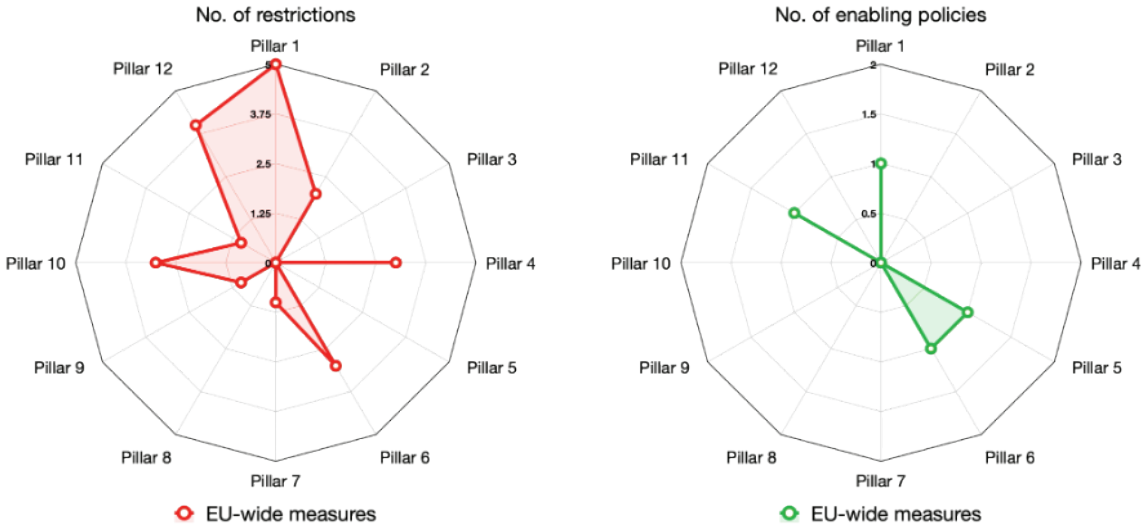


Source: Author. The data is available in the DTI database. LINK

III. EU-WIDE MEASURES AFFECTING DIGITAL TRADE

This section provides a detailed overview of the EU-wide measures mentioned in the previous section. Applying the DTI methodology, it assesses the EU's digital trade regulatory framework, which has a direct influence on the national frameworks of its member states. It also highlights how these measures affect all the EU member states, with particular attention to their implications for the V4 economies. Figure 7 provides an overview of the distribution of these measures across the 12 policy pillars of the DTI.

Figure 7: EU-wide measures by DTI pillar Regarding policies that affect trade in ICT goods, the



Source: Author. The data is available in the DTI database. LINK

EU is a signatory to the WTO Information Technology Agreement (ITA) and its 2015 expansion (ITA II), which eliminate tariffs on 402 ICT products, including computers, semiconductors and telecommunications equipment. This is particularly relevant for the V4 economies, whose export performance relies heavily on intermediary ICT components used in the production of final digital goods (see Section I). At the same time, the EU applies several trade defence instruments, such as anti-dumping and countervailing duties, which increase the prices of certain ICT inputs, including optical fibre cables and silicon metal. These measures, many of which target China, aim to protect EU producers but can raise costs for ICT manufacturing. This is especially significant for Czechia, which has emerged as a key semiconductor hub in Europe, with the "Semiconductor Valley" LINK around Brno positioning the country strategically within the EU value chain.

Other EU rules affecting ICT goods include export controls and relatively low de minimis thresholds for imports. Regulation (EU) 2021/821 imposes strict controls on dual-use items, and additional measures ban exports of selected ICT products, such as computer parts and memory chips, to Russia and Iran. On the import side, Council Directive (EU) 2017/2455 sets a de minimis threshold of USD 174, which is below the USD 200 level recommended by the International Chamber of Commerce, which means that small-value shipments entering the EU remain subject to customs duties and associated costs.

In the field of intellectual property, EU law simultaneously protects and mandates the disclosure of confidential business information, including algorithms and source code. The Trade Secrets

Directive (Directive (EU) 2016/943) safeguards confidential information but allows its disclosure in the public interest, while the Platform-to-Business Regulation (EU) 2019/1150 requires online intermediation services to explain the main parameters that determine classification (even if this may involve disclosure of trade secrets). The Digital Services Act (DSA) (Regulation (EU) 2022/2065) further allows regulators and vetted researchers to access specific platform data to monitor systemic risks. For many digital operators in the V4, especially smaller or fast-growing firms, these obligations can enhance transparency and trust yet increase compliance costs and concerns about the protection of proprietary technologies.

Policies on data flows and protection similarly combine enabling and restrictive elements. The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) offers a robust privacy framework and legal certainty but imposes stringent conditions on cross-border data transfers and extensive obligations on firms, which are particularly demanding for SMEs (Presidente & Frey, 2022). The Data Act (Regulation (EU) 2023/2854) complements the GDPR by governing access to and use of non-personal data; Article 32 restricts foreign government access to data stored in the EU and obliges providers, especially non-EU firms, to prevent unlawful transfers. Providers of "mixed data sets" must therefore comply with both regimes, which adds complexity for cloud and data service operators.

Additional requirements derive from local presence obligations under Directive (EU) 2016/1148, the GDPR and the DSA. Article 18 of Directive (EU) 2016/1148 and Article 27 of the GDPR require certain non-EU digital service providers and data controllers to appoint an EU representative, while Article 13 DSA adopts a similar approach for intermediary services. These obligations increase fixed compliance costs for foreign companies and may deter smaller providers from serving EU markets, including those of the V4.

Finally, the EU's multilateral trade commitments contain both enabling and restrictive features for digital trade. On the enabling side, the EU has incorporated the WTO Telecommunications Reference Paper into its commitments, adopting binding principles on competitive safeguards, independent regulation, transparent licensing and interconnection, which support an open and predictable telecoms market. Conversely, its commitments under the WTO Government Procurement Agreement (GPA) remain limited, as EU schedules exclude "telecommunications-related services" (CPC 754). Public contracts for telecom infrastructure and data transmission are therefore largely closed to foreign suppliers, which restricts competition in a sector that underpins the digital economy and potentially limits opportunities for V4 operators to integrate into wider supply chains or attract foreign investment in network development.

IV. CZECHIA'S DIGITAL ENVIRONMENT: DIGITAL TRADE POLICIES AND PRACTICES

This section analyses Czechia's legal environment for digital trade using the DTI Project methodology, which is complemented by qualitative evidence from eight semi-structured

interviews conducted between October and November 2025. The sample comprised eight founders and senior representatives of early-stage and growth-oriented firms, a fintech association, business and regional innovation organisations, and ecosystem intermediaries primarily based in Prague and Brno. The interviewed firms operate mainly in the fields of enterprise software, data processing, e-commerce logistics, and legal services, with their activities centred on the Czech market but often extending across Central Europe.

The interviews focused on two dimensions: (i) perceptions of the business environment and market conditions in Czechia, including the country's strengths, weaknesses, and similarities with other V4 countries; and (ii) how domestic and supranational rules affect digital business models and cross-border operations. The discussions addressed regulatory awareness among new entrants, the costs of EU-level compliance, data governance, consumer protection, and trust in the digital environment. The analysis concentrated on barriers and enabling measures that affect Czech firms supplying cross-border digital services. EU-level restrictions that differentiate between domestic and foreign providers were not addressed directly by the interviewees and remain an area for future research.

Before turning to the regulatory analysis of Czechia, it is worth noting that among the stakeholders interviewed, there was broad recognition of the high level of entrepreneurial activity and the opportunities for business growth in Czechia. On the public side, several highlighted the role of government-funded bodies such as CzechInvest, which manages programmes supporting incubators and providing grants for SMEs while enhancing the visibility and connectivity of firms in digital sectors. A notable initiative in this regard is the Fintech Regulatory Sandbox, LINK a CzechInvest programme offering regulatory guidance, technical testing, and business mentoring for selected fintech companies.

Likewise, private actors were emphasised as playing a pivotal role in fostering innovation. Regional associations, specialised media outlets, and community platforms operating across Central Europe contribute to strengthening the innovation ecosystem by enhancing the visibility of emerging firms and facilitating opportunities for networking and investor engagement.

Moreover, many of the interviewees identified talent retention as a major challenge for SMEs in specialised digital sectors. Several suggested that a clear legal framework for employee stock ownership plans (ESOPs) could help address this issue by aligning employee incentives with company growth and attracting investment. One community platform noted that such a regulation would enhance legal certainty and encourage investment in Czech firms, whereas its absence has led some companies to establish entities abroad to appeal to foreign investors.

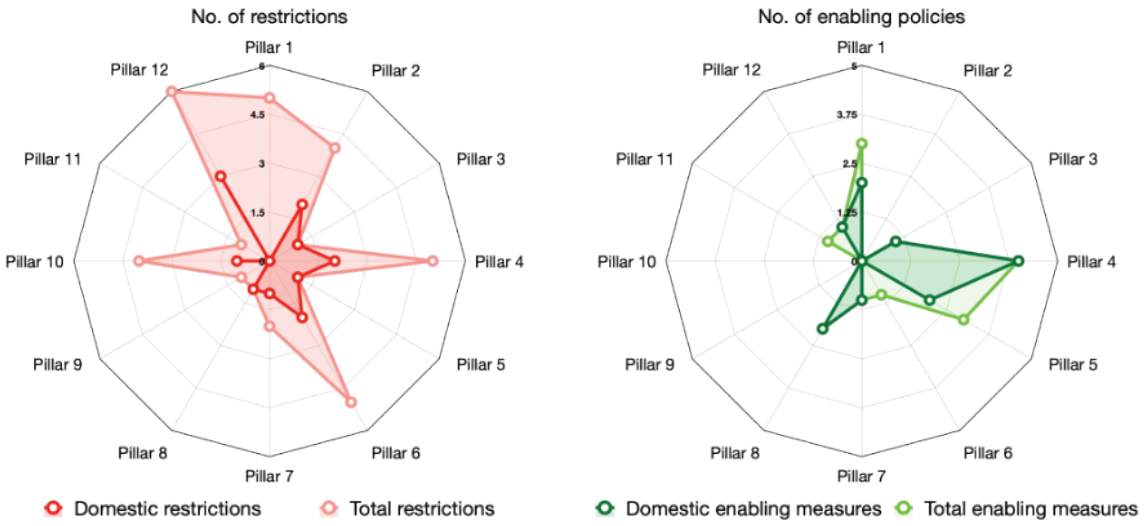
In this context, stakeholders are closely following the forthcoming reform of the Income Tax Act LINK and its potential benefits for firms seeking to implement ESOP schemes.

Additionally, one company highlighted how perceptions of trust towards companies established in Central Europe continue to affect their ability to provide services in other EU countries. In this regard, it referred to the proposed 28th EU regime, LINK suggesting that it could strengthen consumers' confidence when purchasing "European" services rather than specifically national ones. This proposal was highlighted by one community platform as a

potential means to strengthen investor confidence by enabling companies to operate under a unified EU legal framework rather than a national one.

Moving to the regulatory dimension, Figure 8 provides an overview of the Czech domestic regulatory framework for digital trade (in darker tones), which is benchmarked against the total numbers of measures – including the EU-wide policies (in lighter tones) – across the 12 policy pillars of the DTI methodology. The following section analyses the impact of these measures in greater depth, combining the quantitative findings with qualitative insights derived from the interviews.

Figure 8: Total numbers of measures implemented by Czechia by DTI pillar



Source: Author. The data is available in the DTI database. LINK

Regarding ICT goods, Czechia offers an enabling environment with low tariffs and limited national restrictions. The weighted average tariff on ICT products is 0.62%, which is below the global average of 0.9%, and 77% of ICT imports enter the country duty-free. Czechia has not introduced import bans or licensing requirements beyond those applicable at EU level, thus facilitating access to digital technologies and components needed for production and innovation.

In public procurement, there are no rules specifically targeting ICT goods or digital services, but general provisions have important implications for this area. Act No. 134/2016 on Public Procurement, which transposes Directive 2014/25/EU, allows contracting authorities to restrict participation in public procurement procedures by suppliers from non-EU countries not

covered by EU trade agreements and to give preference to EU-origin products in cases where two or more bids are otherwise equivalent.

Moreover, the lack of transparency in procurement procedures is reportedly a persistent problem in the country, particularly in relation to overly narrow tender specifications and potential biases favouring state-owned enterprises. One interviewed company noted that some tenders required specific data-handling and processing certificates even though the firms already complied with all the legal requirements for performing these activities. The cost of obtaining such certificates – which have a limited value outside the bidding process – discouraged SMEs from participating in the sector. Taken together, these measures and practices ultimately constrain the ability of smaller and foreign technology companies to compete effectively in public tenders.

Czechia maintains an open FDI regime with no sectoral restrictions on foreign investors, who generally operate under the same conditions as Czech nationals. However, the Foreign Investment Control Act implementing Regulation (EU) 2019/452 establishes a screening mechanism administered by the Ministry of Industry and Trade. This mechanism applies to non-EU investors acquiring significant holdings in sensitive sectors, such as dual-use products and critical data infrastructure. While this regime enhances oversight and aligns Czechia with EU standards, its scope may impact investment decisions in data-intensive industries and hinder the development of digital infrastructure.

In connection with this issue, one interviewed business centre noted that although the absence of clear rules on ESOPs remains the main reason why Czech firms establish operations outside the EU when seeking foreign capital, the investment screening process also reduces regulatory predictability for investors in these strategic sectors.

In the area of IPRs, online copyright protection is reportedly limited in the country. While business software piracy has declined, the entertainment software sector still faces challenges, mainly due to lengthy criminal proceedings. Offences involving copyrights and database rights continue to occur, often through unauthorised use of online repositories. Moreover, the Copyright Act does not include an open-ended "fair use" or broad "fair dealing" provision while restricting lawful unauthorised use to a narrow set of exceptions. On the enabling side, Czechia has ratified the WIPO Internet Treaties and the Patent Cooperation Treaty and has strengthened trade-secret protection by transposing Directive (EU) 2016/943.

During the interviews, the participants did not show any extensive awareness of the direct economic benefits these IPR frameworks provide to companies. Nevertheless, all the interviewees emphasised the relevance of trade-secret protection policies, which they considered particularly important for fostering trust between partners and investors. Moreover, none of the participants operated business models falling under the categories subject to trade-secret disclosure obligations in the Regulation on Relations between Platforms and Business Users or the Digital Services Act (DSA).

Czech telecommunications are regulated by the Electronic Communications Act, which ensures non-discriminatory market access and independent oversight by the Czech Telecommunication

Office. Obligations on passive infrastructure sharing and accounting separation for operators with significant market power support competition and reduce entry costs, contributing to the expansion of high-quality digital networks.

Regarding cross-border data policies, Czechia has introduced specific requirements that restrict cross-border data flows, particularly in the public sector. Decree No. 316/2021 Coll. requires certain operational data, including information relating to identifiable users, to be stored and processed within EU or EFTA Member States when cloud-computing services are used by public bodies. In addition, the VAT Act requires invoices to be stored in Czechia, although their storage abroad is permitted if the tax authority is notified and granted remote access. According to the interviewed companies and business associations, these provisions enhance data security and administrative control but increase operational costs for foreign cloud providers and SMEs that rely on cloud-based systems, especially in relation to VAT invoice retention.

Both the companies and the business associations expressed similar perceptions regarding cross-border data policies. There was broad agreement that these regulations increase operational costs for companies as they often need to outsource compliance to specialised professionals because of them. The participants highlighted that collaboration with business associations and law firms helps mitigate these costs by providing shared resources and legal advice. Regional associations, media outlets, and community platforms also offer tools and training to help firms understand and apply these regulations. Still, it was noted that most companies are not fully aware of all the legal requirements until they are faced with them in practice, which indicates that regulatory complexity remains a challenge for smaller and less-experienced digital operators.

Domestic data protection rules are largely harmonised with EU law through the Personal Data Processing Act, which implements the GDPR. However, Sections 97(3) and 97(4) of the Electronic Communications Act impose mandatory data-retention obligations on electronic communications providers, including VoIP operators, requiring them to retain information on telephone, text, internet and email connections for six months. The interviewed providers indicated that although these obligations are justified by law-enforcement objectives, they significantly increase storage and cybersecurity costs and may deter smaller or foreign operators from entering the market, thereby limiting competition and innovation in digital services.

The Law on Certain Services of the Information Society (No. 480/2004) establishes the primary rules governing intermediary liability in Czechia. It incorporates the EU E-Commerce Directive and grants "safe-harbour" protection to internet service providers, which means that they are not held responsible for illegal content shared by users if they act promptly to remove it once notified. The law also prohibits general monitoring obligations, so platforms are not required to check all user activity in advance. In contrast, the more recent Digital Single Market (DSM) Directive, transposed through Act No. 429/2022 Coll., has increased the responsibility of online content-sharing platforms such as YouTube or Facebook. These platforms must now take proactive measures, like using automated filters or licensing agreements, to prevent the unauthorised sharing of copyright protected material.

The fintech organisations consulted for this study consistently described their sector as "over-regulated," stressing that EU-wide frameworks strongly shape their operations in Czechia. Regulations such as the Markets in Crypto-Assets Regulation (MiCA), the forthcoming Financial Data Access (FIDA) framework and the Digital Operational Resilience Act (DORA) were cited as creating complex licensing, reporting and resilience requirements.

According to the interviewees, these obligations are particularly burdensome for smaller fintechs that lack the internal capacity to comply with the regulations, and as they are unfamiliar with these requirements, they often discover specific conditions only when applying for licences or entering new markets. At the same time, the stakeholders highlighted the Payment Services Directive (PSD2) as an enabling framework that opened the market to new providers and spurred innovation in online payments and open banking, even if overlapping rules still tend to favour larger operators with greater resources.

As for online sales, Czechia's framework combines both enabling and restrictive elements. On the enabling side, the e-commerce sector is open to foreign investment, and no licensing requirements impede market entry there. The domain-name registration system enables foreign entities to obtain ".cz" domains without requiring a local presence, thereby reducing administrative costs. Moreover, the Consumer Rights Directive has been transposed through the Consumer Protection Act, thus ensuring strong consumer safeguards for both online and offline transactions.

The EU Digital Markets Act (DMA) was also mentioned as a potentially enabling measure in this sector, although its enforcement remains limited. One interviewee noted that the vertical restrictions imposed on large digital platforms have a strong potential to promote fairer competition in the market but observed that the implementation so far has not met expectations. For instance, in March 2025, the European Commission issued preliminary findings LINK against Alphabet Inc. (Google's parent company) for allegedly failing to comply with its DMA obligations, which illustrates the early challenges of enforcing this new regulatory framework.

Moreover, the regulatory framework governing online sales remains affected by the absence of international instruments. Czechia has not ratified the United Nations Convention on the Use of Electronic Communications in International Contracts or adopted legislation based on the UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures. This limits the international recognition of Czech electronic contracts and signatures, thereby reducing legal certainty in cross-border digital transactions and constraining the competitiveness of Czech digital service providers.

V. CONCLUDING INSIGHTS AND POLICY RECOMMENDATIONS FOR DIGITAL TRADE IN CZECHIA

This comparative analysis of the V4 countries reveals a regulatory landscape that is broadly similar in each of them and shaped by the EU's overarching digital framework, yet national differences persist. Slovakia stands out as the most enabling environment, combining a few restrictive measures with a robust set of policies that promote competition and innovation. Hungary, by contrast, maintains a more interventionist approach, particularly in public procurement and investment. Poland and Czechia occupy more balanced positions that reflect moderate levels of both restrictiveness and facilitation. Overall, the EU-wide rules have created a common baseline for digital trade governance across the region, as the EU implements both facilitating frameworks and restrictive policies that have a direct impact on its members.

In particular, Czechia presents a largely enabling environment for digital trade characterised by low barriers for ICT goods, an open investment regime, and transparent telecommunications regulation. At the same time, Czechia's institutional and market foundations are strong. Its transparent telecom regulation, passive infrastructure sharing, and equal market access for foreign operators have fostered competition in network services. Czechia and the EU's robust protection of intellectual property and trade secrets enhances investor confidence. However, limitations persist in areas such as online copyright enforcement, public procurement transparency, and the absence of modern frameworks for electronic contracting and signatures.

The interviews reveal a dynamic yet uneven digital ecosystem. While the entrepreneurs appreciate the stability and predictability offered by the EU-wide legislation, many view the current regulatory framework as excessive, particularly in areas such as data protection and fintech, where SMEs are the most affected. This highlights the need for more proportionate enforcement and tailored support mechanisms. In this context, several participants recommended introducing subsidies to help cover licensing costs for fintech companies, as well as creating regulatory sandboxes to test lighter compliance conditions for SMEs handling personal data.

Moreover, the cumulative effect of the EU and domestic measures often increases compliance costs and administrative burdens for smaller firms that lack the resources to navigate complex regulatory obligations, as well as for foreign investors interested in supporting these companies. These challenges are compounded by the structural issues previously identified by the stakeholders, including difficulties in retaining skilled talent and attracting foreign investment, as well as persistent trust barriers that companies from Central Europe face. Together, these factors underscore the importance of ensuring that future policy reforms – such as the ESOPs related to the forthcoming Income Tax Act – are implemented in a way that will strengthen both investor confidence and the competitiveness of Czech digital firms within the EU market.

Before outlining the policy recommendations for Czechia, it should be emphasised that a supportive regulatory environment is only one of several conditions required for realising the full potential of the digital economy. Other relevant factors – beyond the scope of this study – include cultural and practical barriers that can impede cross-border digital trade. In this regard, one consulted business hub recommended developing a government or EU-level guide outlining the practical time and cost implications of the "non-optional" rules companies must comply with when providing cross-border digital services.

CZECHIA'S DIGITAL TRADE ECOSYSTEM: THE MAIN RECOMMENDATIONS

1. SME capabilities and incentives

(Lead: the Ministry of Industry and Trade, in cooperation with CzechInvest and business associations)

- Enhance awareness and capacity-building among SMEs by providing accessible guidance and training in compliance with EU and national digital regulations (both fintech and data) in cooperation with business associations and innovation hubs.
- Introduce or clarify regulations enabling the use of employee stock ownership plans (ESOPs) for SMEs to support talent attraction and retention in digital sectors.

2. Public procurement and certification

(Lead: the Ministry of Regional Development and the Office for the Protection of Competition, in cooperation with major contracting authorities)

- Enhance transparency and proportionality in public procurement by reviewing tender specifications to ensure that technical and certification requirements are directly relevant to contract performance.
- Introduce simplified or standardised certification procedures and guidance tailored to SMEs while allowing an equivalent compliance to be demonstrated without unnecessary costs and promoting fair competition in digital tenders.

3. Tax and data-reporting obligations

(Lead: the Ministry of Finance and the Czech Telecommunication Office, in coordination with the National Cyber and Information Security Agency)

- Review the requirements for transferring VAT invoice data to ensure that compliance obligations remain proportionate for SMEs that rely on such data in their daily operations.

- Assess the proportionality and costs of the mandatory retention of the "data packets" imposed on electronic communications service providers with a view to reducing unnecessary administrative and cybersecurity burdens.

4. Copyright and online enforcement

(Lead: the Ministry of Culture and relevant enforcement authorities

- Strengthen the enforcement of intellectual property laws online while focusing on improving the speed and effectiveness of procedures against digital copyright infringements.
- Consider introducing copyright provisions aligned with fair use or fair dealing models to support innovation and the lawful use of copyrighted materials for research, education and software development.

5. The legal framework for digital contracts and cross-border commerce

(Lead: the Ministry of Justice, in cooperation with the Ministry of Industry and Trade)

- Ratify the United Nations Convention on the Use of Electronic Communications in International Contracts to enhance the international recognition of digital transactions and improve legal certainty in cross-border commerce.

- Adopt a legal framework consistent with the UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures to promote interoperability and facilitate the use of secure digital contracts.

ENDNOTES

1 Although widely used, the term digital trade lacks a universally agreed definition. The most recognised one, set out by the IMF, the OECD, UNCTAD, and the WTO in the Handbook on Measuring Digital Trade, defines it as "all international trade that is digitally ordered and/or digitally delivered" (IMF et al., 2023)

2 For more information about the project and its methodology, see Ferracane, González Ugarte, and Rogaler (2025b).

3 Comprehensive information on the regulatory frameworks and practices discussed in this section is available in the DTI Database. For detailed data, see: Ferracane, M.F., González Ugarte, S., and Rogaler, T. (Eds.).

REFERENCES

Burri, M., & Chander, A. (2023). What are digital trade and digital trade law? *AJIL Unbound*, 117, 99–103.
https://doi.org/10.1017/aju.2023.14

Burri, M., Vásquez Callo-Müller, M., & Kugler, K. (2024). The evolution of digital trade law: Insights from TAPED. *World Trade Review*, 23(2), 190–207.
https://doi.org/10.1017/S1474745623000472

Evenett, S. J., & Fritz, J. (2022). *Emergent digital fragmentation: The perils of unilateralism* (GTA Report No. 29). Digital Policy Alert & Global Trade Alert; CEPR Press.
https://digitalpolicyalert.org/report/emergent-digital-fragmentation

Ferracane, M. F. (2022). *The Digital Trade Integration database: Description of pillars and indicators* (EUI RSC, 2022/70, Global Governance Programme-484, Global Economics, Digital Trade Integration project). European University Institute.
https://hdl.handle.net/1814/75011

Ferracane, M. F., González Ugarte, S., & van der Marel, E. (2025). The Brussels effect in Africa: Is it beneficial for intra-regional trade in digital services? *Journal of International Economic Law*, 28(1), 1–22.
https://doi.org/10.1093/jiel/jgae059

Ferracane, M. F., González Ugarte, S., & Rogaler, T. (2025a). Global Trends in Digital Trade Policies and Practices: Evidence from the Digital Trade Integration Database. *World Trade Review*, 1–25.
https://doi.org/10.1017/S1474745625100955

Ferracane, M.F., González Ugarte, S. and Rogaler, T. (Eds.), (2025b). Digital Trade Integration Database. European University Institute *et al.*
https://dti.eui.eu

Ferracane, M. F., & Rogaler, T. (2025). *Digital trade: An assessment of regulations and practices in Rwanda and Uganda* (Project Report RWA-24211, Global Governance Programme). International Growth Centre.
https://hdl.handle.net/1814/93666

Ferracane, M., & van der Marel, E. (2023). *Digital trade regulatory environment: Opportunities for regulatory harmonization in Africa*. United Nations Economic Commission for Africa.
https://hdl.handle.net/10855/49965

Freund, C. L., & Weinhold, D. (2002). The internet and international trade in services. *American Economic Review*, 92(2), 236–240.

Freund, C. L., & Weinhold, D. (2004). The effect of the internet on international trade. *Journal of International Economics*, 62(1), 171–189.
https://doi.org/10.1016/s0022-1996(03)00059-x

International Monetary Fund (IMF), Organisation for Economic Cooperation and Development (OECD), United Nations Conference on Trade and Development (UNCTAD), and World Trade Organization (WTO). (2023). *Handbook on measuring digital trade: Second edition*. OECD Publishing.
https://doi.org/10.1787/ac99e6d3-en

López González, J., & Ferencz, J. (2018). *Digital trade and market openness* (OECD Trade Policy Paper No. 217). OECD Publishing.
https://www.oecd.org/en/publications/digital-trade-and-market-openness_1bd89c9a-en.html

López González, J., Sorescu, S., & Kaynak, P. (2023). Of bytes and trade: Quantifying the impact of digitalisation on trade. OECD *Trade Policy Papers, No. 273*. OECD Publishing.
https://doi.org/10.1787/11889f2a-en

Organisation for Economic Co-operation and Development (OECD). (2025). *Measuring digital trade.*
https://www.oecd.org/en/topics/measuring-digital-trade.html

Presidente, G., & Frey, C. B. (2022, March 10). *The GDPR effect: How data privacy regulation shaped firm performance globally*. VoxEU.
https://cepr.org/voxeu/columns/gdpr-effect-how-data-privacy-regulation-shaped-firm-performance-globally

United Nations Conference on Trade and Development (UNCTAD). (2025). *UNCTADstat Data Hub*. Retrieved July 30, 2025.

https://unctadstat.unctad.org/datacentre/

United Nations Economic and Social Commission for Asia and the Pacific (ESCAP), Economic Commission for Africa (ECA), & Economic Commission for Latin America and the Caribbean (ECLAC). (2024). *Digital trade regulatory review for Asia-Pacific, Africa, and Latin America and the Caribbean. Bangkok*: ESCAP.
https://hdl.handle.net/20.500.12870/6848

World Bank. (2022). *Digital trust: How to unleash the trillion-dollar opportunity for our global economy.*
https://www.weforum.org/agenda/2022/08/digital-trust-how-to-unleash-the-trillion-dollar-opportunity-for-our-global-economy

ANNEXE I: HUNGARY'S NATIONAL REGULATORY FRAMEWORK FOR DIGITAL TRADE INTEGRATION

Regarding ICT goods, Hungary maintains an enabling environment supported by low tariffs and the absence of restrictive measures. The average tariff rate on ICT goods stands at 0.62%, which is below the global average of 0.9%, and about three-quarters of Hungary's ICT imports are tariff-free. The country imposes neither import bans nor licensing regimes, which facilitates access to digital technologies and components.

With regard to public tenders, Hungary does not have any rules that specifically refer to ICT products or digital services, although several Hungarian provisions indirectly affect them. The 2015 Public Procurement Law allows for the exclusion of bidders from outside the EU or the WTO from public procurement procedures and gives preference to European products in cases of equivalent bids, which reflects EU directives on public service procurement. In addition, persistent issues such as limited transparency, restrictive tender specifications and implicit preferences for local suppliers continue to concern foreign bidders and have been highlighted by the business community and foreign governments.

As for foreign investment, Hungary maintains an open regime under the 1988 Foreign Investment Act but operates two screening mechanisms covering strategic sectors of the digital economy. The first, introduced under Act LVII of 2018 on Controlling Foreign Investments Violating Hungary's Security Interests, requires ministerial approval for foreign acquisitions in sensitive industries such as cryptography and telecommunications. The second, the "Alternative FDI Regime" established under Chapter 85 of Act LVIII of 2020, applies to transactions exceeding specified thresholds in strategic sectors such as telecommunications, publishing, and IT services. Although designed to safeguard national interests, these regimes establish additional barriers to investment in sectors that are key to the development of digital trade, such as telecommunications, IT services, and cryptography. Therefore, they potentially hinder the development of these sectors.

In the field of IP, Hungary combines restrictive and enabling features. Foreign patent applicants from outside the EU or the EEA must appoint a local representative, while weak online copyright enforcement and limited exceptions under the Copyright Act restrict the lawful use of protected works. These constraints can raise compliance costs and limit the development of digital services. On the enabling side, however, the 2018 Trade Secrets Act, which is aligned with EU standards, provides strong protection for confidential business information, and Hungary's adherence to the WIPO Internet Treaties and the Patent Cooperation Treaty enhances predictability and investor confidence in this field.

Moreover, the telecommunications sector operates under an enabling framework overseen by the independent National Media and Infocommunications Authority (NMHH). The Electronic Communications Act ensures non-discriminatory licensing and mandates accounting separation and infrastructure sharing to foster competition and efficient network use. However, functional separation is not required, and the continued state ownership of major operators such as

Antenna Hungária and Vodafone Magyarország raises questions about market neutrality and long-term private investment.

Regarding data policies, Hungary's data policy framework implements the GDPR through amendments to the 2011 Data Protection Act. Yet restrictions remain regarding data retention and government access to personal information, as internet providers must retain connection data for at least twelve months and provide user data to authorities upon request. While these measures support security objectives, they raise concerns about proportionality, privacy, and compliance costs, and could potentially affect user trust and cross-border digital services.

The framework for online intermediaries aligns with EU law on intermediary liability. The E-Commerce Act transposes the EU Directive granting conditional liability exemptions to ISPs that act promptly to remove unlawful content. However, the implementation of the 2019 Copyright Directive introduced stricter monitoring obligations for content-sharing platforms, as it requires authorisation from rights holders and technical systems to prevent unauthorised uploads. Non-compliant providers lose their liability protection, which increases operational burdens.

Consumer protection is governed by the 1997 Consumer Protection Act, which incorporates the EU Consumer Rights Directive and establishes clear rights for online transactions. Nonetheless, several rules continue to raise compliance costs for e-commerce operators. The ".hu" domain registration policy requires a local presence within the EU, the EEA, or neighbouring countries, which limits foreign firms' visibility in the Hungarian market. Providers of video-sharing platforms must also notify the relevant authorities before commencing operations, which means that the process is effectively restricted to entities with a local registration.

Moreover, Hungary has not ratified the UN Convention on the Use of Electronic Communications in International Contracts or adopted the UNCITRAL Model Laws on electronic commerce and electronic signatures. The absence of these instruments limits cross-border legal interoperability and the international recognition of Hungarian digital contracts and signatures. Collectively, these conditions may reduce the competitiveness of foreign providers and the diversity of online services available to Hungarian consumers.

ANNEXE II: POLAND'S NATIONAL REGULATORY FRAMEWORK FOR DIGITAL TRADE INTEGRATION

Poland presents an overall enabling environment for ICT goods, which is supported by low tariff levels and the absence of restrictive measures. The weighted average tariff rate is 1.4%, which is slightly above the global average of 0.9%, but around 77% of Polish ICT imports are tariff-free. No import bans or licensing regimes apply in this case, which facilitates access to digital technologies and components.

Regarding public procurement, Poland follows the EU framework under the Utilities Directive, as reflected in the 2019 Public Procurement Act. The law allows contracting entities to exclude suppliers from non-EU countries not covered by the Union's international commitments from public procurement procedures and to grant preference to EU-origin products in cases of equivalent offers.

Poland's foreign investment regime is generally open in accordance with the 2018 Act on Entrepreneurs, which guarantees freedom of establishment and non-discrimination. However, the 2015 Act on the Control of Certain Investments establishes a screening mechanism aligned with the EU's investment screening regulation. Non-EEA or non-OECD investors must obtain prior approval when acquiring significant stakes in strategic companies, particularly those involved in critical infrastructure, telecommunications, or essential digital services. While designed to protect national security, this regime adds complexity for foreign investors intending to operate in key digital sectors.

In the field of intellectual property, Poland combines restrictive and enabling elements. The country's weak enforcement of online copyright and limited exceptions under the Copyright Act constrain the lawful use of protected works, thus raising compliance costs for digital firms. Conversely, Poland's ratification of the WIPO Internet Treaties and participation in the Patent Cooperation Treaty align it with international IP standards, while the 2018 Trade Secrets Act provides robust protection for confidential business information.

The telecommunications sector remains open and competitive. The Electronic Communications Law does not impose discriminatory licensing conditions, and the independent Office of Electronic Communications (UKE) supervises the market. Operators with significant market power are required to maintain accounting separation and share passive infrastructure, which promotes competition and efficient network use. However, functional separation is not mandated.

Poland's data policies include both enabling and restrictive aspects. Although the GDPR has been fully implemented in Poland, data retention and government access obligations persist. Telecommunications providers must retain user connection data for twelve months and grant access to it to authorised authorities such as the police and security services without prior judicial approval. While justified on national security grounds, these measures raise privacy concerns and add compliance costs for service providers.

In terms of intermediary liability, the Civil Code and the Act on Providing Services by Electronic Means establish a framework aligned with the E-Commerce Directive, limiting the liability of ISPs acting as conduits, caching, or hosting providers that act promptly upon notice of illegal content. Nonetheless, the transposition of the 2019 Copyright Directive has introduced partial liability for online content-sharing platforms, thus increasing their operational obligations.

For online transactions, the ".pl" domain regime imposes no restrictions on foreign applicants while supporting a non-discriminatory digital environment. The 2014 Consumer Rights Act transposes the EU Consumer Rights Directive, and ensures strong consumer protection for online commerce. However, Poland has not ratified the UN Convention on the Use of Electronic

Communications in International Contracts or adopted the UNCITRAL Model Laws on e-commerce and electronic signatures, which limits interoperability and potentially increases compliance costs for cross-border transactions.

ANNEXE III: SLOVAKIA'S NATIONAL REGULATORY FRAMEWORK FOR DIGITAL TRADE INTEGRATION

Slovakia maintains an enabling environment for ICT goods with a weighted average tariff rate of 0.75%, which is below the global average of 0.9%, and about 77% of its ICT imports are exempt from tariffs. No import bans or licensing regimes are applied in it, which facilitates access to digital technologies and components.

As for public procurement, Slovakia follows the EU framework under the Utilities Directive, which was transposed through the 2015 Public Procurement Act and complemented by related decrees setting monetary thresholds for compliance with EU procedures. However, following the regional trend, some persistent transparency issues remain, particularly those concerning the openness of tenders and perceived preferences for local suppliers.

Moreover, in line with EU Regulation 2019/452, Slovakia established a foreign investment screening regime under the 2022 Act on the Screening of Foreign Investments, which replaced the previous critical infrastructure system. The law requires non-EU investors to obtain prior authorisation for qualifying acquisitions, which is accompanied by compulsory, voluntary, or ex officio screening depending on the level of risk to national security or public order. A subsequent regulation then identifies strategic sectors in this regard such as infrastructure, cybersecurity, cloud services, encryption, broadcasting, and major online platforms.

The IP framework combines enabling and restrictive features. On the enabling side, Slovakia has ratified the WIPO Internet Treaties and the Patent Cooperation Treaty, and it strengthened trade secret protection through the 2018 amendment to the Commercial Code. On the restrictive side, weak online copyright enforcement and limited exceptions under the Copyright Act constrain the lawful use of protected works and may discourage digital innovation.

Slovakia's telecommunications sector stands out within the region for its pro-competitive structure. The independent Regulatory Authority for Electronic Communications and Postal Services (RÚ) oversees the sector, applying a non-discriminatory licensing regime. Functional and accounting separation, as well as passive infrastructure sharing, are mandated for operators with significant market power, which fosters openness and competition.

The data policies in Slovakia stand out for providing a less restrictive environment compared to their counterparts. The country has not introduced local storage or data localisation requirements, or mandatory retention periods for providers – beyond those imposed by the EU. The GDPR is implemented in Slovakia through the 2018 Data Protection Act, which ensures a comprehensive and harmonised privacy framework.

Intermediary liability is governed by the 2004 Electronic Commerce Act, which incorporates safe-harbour provisions for mere conduit, caching, and hosting services, and prohibits general monitoring obligations. However, amendments to the Copyright Act implementing the 2019 Copyright Directive make content-sharing platforms partially liable for copyright infringements committed by users. In the audiovisual sector, providers of on-demand media services must obtain authorisation from the Council for Media Services under the 2022 Media Services Act. The applicants must be based or registered in Slovakia, which effectively creates a local presence requirement. The authorisation decisions must be issued within 90 days, and are subject to a EUR 260 fee. The providers must also reserve at least 30% of their catalogue for European works and contribute 0.5% of their annual revenue to the Audiovisual Fund.

As for online transactions, Slovakia has transposed the EU Consumer Rights Directive through the 2007 Consumer Protection Act, thus creating a unified framework for offline and online commerce. However, registration under the ".sk" top-level domain is limited to individuals and entities with an address in the EU, the EEA, the EFTA, or the United Kingdom, which restricts the access to the Slovak market of foreign firms without a regional presence. Slovakia has also not ratified the UN Convention on the Use of Electronic Communications in International Contracts or adopted the UNCITRAL Model Laws on e-commerce and electronic signatures, which limits cross-border legal interoperability and increases compliance costs for foreign service providers.