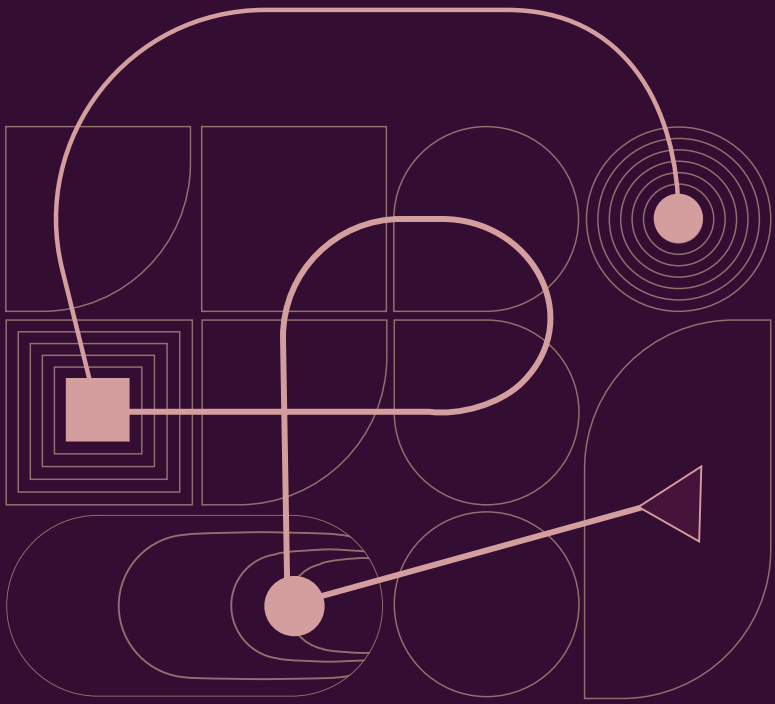
DIGITAL GOVERNANCE IN THE EU AND BEYOND

INSTITUTIONAL DESIGNS, STRUCTURES AND CAPACITIES COMPARED



IMPRESSUM

Executive editors:
Danilo Krivokapić and Andrej Petrovski

Editor:
Snežana Bajčeta

Authors:
Snežana Bajčeta, Jelena Adamović, Duje Prkut, Duje Kozomara

Design:
Olivia Solis Villaverde

Language editing:
Milica Jovanović

Share Foundation, 2025

DIGITAL GOVERNANCE IN THE EU AND BEYOND

INSTITUTIONAL DESIGNS, STRUCTURES AND CAPACITIES COMPARED

CONTENTS

SUMMARY

The new generation of European legislation on digital services (DSA), digital markets (DMA), and artificial intelligence (AIA) is grounded in public values such as accountability, transparency, interoperability, and accessibility, which are increasingly challenged by technology, the BigTech industry, geopolitical dynamics, and profit-driven society. The ambitious goal of building a safe, open, competitive, and democratic digital ecosystem depends on complex, multi-stakeholder, and multi-level institutional mechanisms that involve national and European institutions, experts and independent bodies, the digital industry, and citizens alike. Without effective institutions and their intersectoral cooperation, enforcing the systemic regulations designed to address structures of the digital sphere remains unattainable. Within its territorial scope and comprehensive institutional framework, the European Union currently represents the highest standard of institutional safeguards against the challenges of the digital environment.

On the other hand, EU candidate countries such as Serbia and Montenegro, while striving to align their legislation with European standards, must not only adopt new regulations and laws but also develop appropriate institutional mechanisms for their enforcement. However, when it comes to major platforms and the largest digital industry giants, effective implementation remains almost impossible without the support and direct involvement of European institutions.

A possible pathway for integrating the Serbian and Montenegrin digital markets into the European normative framework could be through their accession to the Digital Single Market. On the one hand, such an arrangement would strengthen various sectors of countries' digital economies and help establish higher standards. On the other hand, it could serve as a valuable interim step toward EU membership, enabling the Union

to address systemic risks in Serbia's and Montenegro's digital markets and to prepare them for full integration.

Although these two countries are at different stages of European integration, they share much of the same transitional legacy that shapes their major social, political, legal, and institutional challenges – all closely intertwined with the digital ecosystem. Croatia, another South-Eastern European country with a comparable legacy, is now a full EU member, meaning that its national institutional framework for digital regulation should already be integrated with European mechanisms. Yet, even in such cases, aligning national legislation is not a straightforward process. Croatia continues to face numerous challenges, delays, and obstacles along the way.

The aim of this study is to explore the institutional preconditions for implementing digital legislation related to digital services, digital markets, and artificial intelligence (AI). Using the Most Similar Systems Design (MSSD), we compare the *institutional mechanisms* of Croatia, Serbia and Montenegro in terms of their design, structure, and capacity to implement digital rights standards. The key hypothesis is that contemporary, globally scoped digital challenges cannot be effectively addressed through regulation at the level of a single nation.

KEY FINDINGS: THE CONTESTED CAPACITIES FOR DIGITAL GOVERNANCE

CAPACITY DIMENSION	CROATIA (EU MEMBER)	SERBIA (EU CANDIDATE)	MONTENEGRO (EU CANDIDATE)
Institutional and Political Context	Key regulators (HAKOM, AZOP, AZTN) enjoy partial autonomy, though risks of regulatory capture persist. EU membership ensures formal independence and external oversight mechanisms.	High degree of political capture and executive dominance. Regulators operate with limited autonomy, particularly REM.	Institutional fragility due to repeated government reorganizations. Mandates and accountability remain unclear.
Technical Capacities	Moderate to strong. Agencies use EU-developed tools and maintain functional IT systems. Limited AI-monitoring capacity at AZOP.	Sector-specific capacity. RATEL is technically competent but isolated. REM lacks digital expertise. The IT sector is globally competitive but disconnected from public regulation.	Basic capacities. The AMU shows interest, but the EKIP avoids digital regulation. The technical base remains largely administrative.
Human Capacities	Staff are qualified but insufficient in number, with skill gaps in AI and data science. Strong EU-level participation and trainings.	Regulatory personnel remain bureaucratic, with few experts and weak ties to academia or expert communities.	Limited expert pool but an emerging younger staff eager to learn. Reliance on EU support and external expertise.

CAPACITY DIMENSION	CROATIA (EU MEMBER)	SERBIA (EU CANDIDATE)	MONTENEGRO (EU CANDIDATE)
Institutional Design and Independence	Stable institutional setup, though risks of informal influence persist. Transparency is higher due to EU oversight.	Delayed convergence and weak independence, marked by politicized appointments and lack of cross-sector coordination.	Institutional continuity disrupted by shifting mandates and restructuring during EU negotiations.
Operational Capacities	Incremental development of procedures. Agencies define new workflows for the DSA. Cross-agency cooperation is limited but functional.	Severe coordination gaps and overlapping competences. No operational protocols for digital-regulation enforcement.	Preparatory stage: awaiting legal mandates before internal restructuring. No operational systems yet established.
Enforcement Practice	Agencies (HAKOM, AZTN, AZOP) fulfil EU obligations but act cautiously.	Formal-compliance culture: low proactivity and heavy dependence on government directives.	Implementation expected post-accession. Early focus on awareness-raising and education.
Collaboration with EU Networks	Full participant in EU-level enforcement boards. Regular data exchange and capacity-building.	Observer or peripheral role. Learning mainly through donor-funded projects.	Emerging participation. EU-supported projects serve as primary learning channels.

CAPACITY DIMENSION	CROATIA (EU MEMBER)	SERBIA (EU CANDIDATE)	MONTENEGRO (EU CANDIDATE)
Civil Society & Academic Integration	Inclusion of CSOs and academia in legislative processes is limited, while cooperation with agencies is sporadic and not systematic.	Absent: REM and other bodies rarely cooperate with academia or CSOs. Low culture of consultation.	CSOs and academia are under-engaged but increasingly recognised as potential partners for capacity-building.
Financial Framework	Stable funding framework. Staff salaries remain constrained.	Adequate income yet poorly allocated. No dedicated funding strategy for digital enforcement.	New mandates require additional financing. Dependence on the state budget, though the Growth Plan offers potential earmarked funds.
Coordination Across Institutions	Developing but uneven. Some inter-agency cooperation (HAKOM–AZOP) on DSA.	Fragmented and poor communication among regulators.	Weak horizontal coordination. Frequent ministrial reorganizations cause discontinuity.
Public Trust and Accountability	Moderate trust. Some improvement through EU transparency mechanisms.	Low public confidence; regulators are perceived as politically captured and ineffective.	Transparency expected to improve through EU-alignment efforts.

CAPACITY DIMENSION	CROATIA (EU MEMBER)	SERBIA (EU CANDIDATE)	MONTENEGRO (EU CANDIDATE)
Digital Market Supervision Capacity	Effective for domestic actors. Lacks experience with VLOPs/ gatekeepers.	Not equipped to monitor gatekeepers or platform markets; lacks systemic market-surveillance capacity.	Oversight limited to traditional media and telecoms. Digital-platform supervision absent.
Data Governance and Privacy	GDPR fully enforced and data protection well-institutionalised. AZOP resources are increasingly strained.	Data protection law aligned but weakly enforced. The Commissioner lacks independence.	Basic data-protection framework in place but institutional authority still improving.
Legislative Coherence	Harmonised with EU law. Continuous updates.	Fragmented and outdated laws. Unclear links among digital, media, and competition regulations.	Laws aligned on paper weakly implemented; delays due to administrative inefficiencies.
External Technical Assistance	Strong EU engagement and extensive training programmes.	Relies on donor-funded technical projects; lacking permanent EU-linked mechanisms.	Dependent on EU-funded initiatives for capacity building and regional cooperation.

CAPACITY DIMENSION	CROATIA (EU MEMBER)	SERBIA (EU CANDIDATE)	MONTENEGRO (EU CANDIDATE)
Political Will for Digital Regulation	Stable but pragmatic. DSM compliance of large platforms is seen as part of EU membership benefits.	Politicised and focused on formal compliance without enforcement.	Growing but inconsistent, driven primarily by EU conditionality.
Overall Assessment	Functionally aligned. Moderate institutional autonomy and capacity gaps in AI.	Structurally captured system with strong laws but weak enforcement.	Institutionally fragile and reliant on EU integration for functionality.

KEY STRATEGIC RECOMMENDATION: INTEGRATING THE WESTERN BALKANS INTO THE DIGITAL SINGLE MARKET

The new European institutional framework for digital governance is marked by an increasing degree of centralisation, reflected in the strong role of European institutions, especially the European Commission, in enforcing the EU's digital market rules. This complex and demanding institutional arrangement requires not only the development of knowledge, competences, and skills, but also the capacity for coordination and joint participation within a horizontally and vertically interconnected governance structure.

Such a model presents challenges even for EU Member States. For candidate countries, the difficulty is compounded by the fact that this architecture was designed primarily for intra-EU application. While they are required to harmonise their legislation with the EU acquis, the question remains: how can they effectively implement the rules before membership? Integration into the Digital Single Market (DSM) thus appears as both a solution to this institutional gap and a strategic opportunity with broader benefits.

Towards the Digital Single Market

Integration of the Western Balkans into the EU Digital Single Market is not merely a technical question of standards or market access. It directly concerns how the European Union manages digital challenges that transcend its borders and how enlargement can be reimagined in concrete and functional ways.

The DSM constitutes the digital pillar of the EU Single Market. It is a regulatory and economic space encompassing twenty-seven Member

States governed by shared rules, common regulations, and a unified legal framework. Through it, the EU leverages the strength of its 450-million-consumer market to establish enforceable standards for digital services, platforms, and emerging technologies.

From the perspective of the Western Balkans, DSM integration is both a regulatory and strategic project. The region is not digitally isolated but tightly intertwined with the European digital ecosystem through infrastructure, communication networks, and cross-border markets. Yet this connectedness generates a dual effect of opportunities and vulnerabilities. Many digital challenges in the region do not remain confined within national borders – they spill over across the region and into the EU:

- Disinformation campaigns often originate within local media systems and spread easily into the EU through shared languages, diaspora networks, and overlapping political narratives.
- Weak enforcement of data protection and privacy standards undermines the security of cross-border data flows.
- Market fragmentation and regulatory inconsistency across the region discourage EU investment and constrain regional business growth.

From a European standpoint, this constitutes a regulatory gap – an unregulated digital zone geographically surrounded by the EU. Integrating the Western Balkans into the DSM would close this gap, reduce systemic risks, and strengthen the coherence and resilience of the European digital space.

The Institutional Gap: Alignment Without Implementation

Over the past several years, the European Union has adopted dozens of new digital regulations – including the DSA, DMA, AI Act, and EMFA. Candidate countries are expected to align with this evolving regulatory ecosystem. However, legal alignment alone does not guarantee implementation. These acts rely on multi-level European enforcement structures, including:

- the European Commission's supervisory powers over Very Large Online Platforms (VLOPSEs) and gatekeepers;

- » cross-border coordination mechanisms such as the European Board for Digital Services and the European Competition Network;
- » joint risk-assessment systems addressing systemic digital threats.

Outside the EU, these mechanisms cannot be replicated. National regulators, often understaffed, politically influenced, and lacking technical expertise, do not possess the authority or scale to enforce such complex frameworks. This creates a risk of "regulatory compression", in which national governments assume functions that, within the EU, belong to the European Commission.

DSM integration can bridge this gap by enabling shared supervision, joint enforcement, and direct participation of Western Balkan regulators in EU-level networks. This would transform digital alignment from a bureaucratic requirement into a functional accession tool, building institutional capacity through practice rather than law alone.

Mutual Strategic Benefits

Integration of the Western Balkans into the EU Digital Single Market would generate reciprocal benefits for both sides. For the European Union, it represents a strategic investment in security, stability, and regulatory coherence. By extending digital rules and standards to its immediate neighbourhood, the EU would reduce exposure to disinformation, cyber threats, and data-governance vulnerabilities that often originate or circulate across the region. Harmonised digital standards would also eliminate market distortions, ensuring fair competition for EU businesses operating in or with the Western Balkans, while simultaneously reinforcing the EU's global regulatory influence – the so-called *Brussels* Effect – and strengthening digital human rights.

For the Western Balkans, DSM integration would unlock substantial economic opportunities, providing a predictable regulatory environment and access to Europe's largest digital market for small and medium-sized enterprises and start-ups. It would also extend EU-level consumer protections and human rights safeguards to regional users, ensuring accountability of global platforms that currently operate beyond national jurisdiction. Within DSM structures, any regulatory asymmetries would be

removed, as platforms would be legally obliged to cooperate with national institutions. Finally, participation in DSM frameworks would strengthen institutional maturity across the region, professionalising regulators, expanding technical expertise, and establishing an early track record of acquis implementation as an essential benchmark for credible EU accession. In this sense, DSM integration makes the EU safer and the Western Balkans stronger – economically, institutionally, and democratically.

Policy and Legal Pathways

Integrating the Western Balkans into the DSM does not require new treaties, but rather innovative use of existing EU instruments. Three viable options include:

- Digital Annexes to Stabilisation and Association Agreements (SAAs): define which DSM provisions apply to candidate countries, providing a clear legal framework for gradual integration.
- EU-Only Agreements or Commission Decisions: adopted directly by EU institutions, bypassing Member State ratification, thus enabling flexible and faster participation.
- Sectoral or Pilot Integration: introduce selected DSM mechanisms (e.g. roaming, eIDAS 2.0, NIS2) through modular approaches already tested in the Energy and Transport Communities.

The EU Growth Plan for the Western Balkans offers an immediate opportunity to support such initiatives. It prioritises digital convergence and allocates resources for strengthening administrative capacities and regulatory expertise.

Political motivations can be expected to differ across the region. Montenegro and Albania, already advanced in negotiations, may view DSM integration as a transitional step, while Serbia, North Macedonia, and Bosnia and Herzegovina could approach it as a strategic bridge to membership.

Finally, the next stage of European digital governance cannot depend solely on national adaptation. Its effectiveness will hinge on creating a European–national implementation framework in which candidate countries participate on an equal footing with EU institutions.

Integrating the Western Balkans into the DSM would transform a fragmented digital periphery into a coherent, rights-based European regulatory space. It would:

- reduce systemic and cross-border digital risks;
- extend the EU's democratic and human-rights standards to neighbouring societies;
- revitalise enlargement by delivering visible, everyday benefits to citizens and businesses before full membership.

The Western Balkans is already part of Europe's digital reality. DSM integration would make it part of Europe's digital future, demonstrating that the EU and the Western Balkans are moving forward together.

INTRODUCTION

The digital transformation is a cornerstone of the European Union's strategic vision, with A Europe Fit for the Digital Age designated as one of the European Commission's six key political priorities.[1] In March 2021, the Commission proposed the Path to the Digital Decade,[2] a policy programme grounded in the 2030 Digital Compass.[3] This initiative outlines a clear roadmap towards a human-centred digital ecosystem, emphasising the development of digital skills, robust infrastructure, digital business transformation, and the digitalisation of public services. By aligning with EU norms and standards, the programme seeks to reinforce Europe's digital sovereignty, supported by substantial budgetary instruments to ensure a resilient and inclusive digital future.

1 European Commission. *A Digital Single Market Strategy for Europe.* COM(2015) 192 final. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, 2015. Accessed Jun 24, 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015DC0192

2 European Commission. *Europe's Digital Decade*. Brussels: European Commission. Accessed June 24, 2025. https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade

3 European Commission. 2030 Digital Compass: The European Way for the *Digital Decade.* COM(2021) 118 final. Communication to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions. Brussels, 2021. Accessed June 24, 2025. https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=CELEX%3A52021DC0118

Building on the foundations of the 2015 Digital Single Market Strategy,[4] which promotes harmonisation, innovation, and economic growth across Member States, the EU is now extending its digital agenda to strategic partners. The Eastern Partnership (EaP) policy framework beyond 2020 reflects this ambition by prioritising investment in digital innovation, knowledge societies, cyber resilience, and secure digital infrastructure.[5] The EU4Digital Facility seeks to bring the benefits of the Digital Single Market to the Eastern partner countries (Armenia, Azerbaijan, Belarus, Georgia, Moldova, Ukraine), promoting a more integrated and competitive digital environment across the wider region.

The entire European Digital Single Market strategy is underpinned by a complex regulatory framework that sets the European digital space apart from other markets. This framework is embodied in a broad set of legislative acts adopted in recent years, including the Digital Services Act (DSA), the Digital Markets Act (DMA), the Artificial Intelligence Act (AIA), the Data Act, and the European Media Freedom Act (EMFA), alongside numerous other initiatives aimed at strengthening the governance of the digital environment.

This normative framework is supported by an equally complex institutional architecture that extends from civil society actors to the European Commission, encompassing national authorities as well. These stakeholders cooperate through both horizontal and vertical channels, forming a multi-level governance system that ensures coherent implementation across the Union.

Candidate countries such as Serbia and Montenegro hold a specific status in relation to the EU Digital Single Market. The greatest challenge in aligning with the EU's evolving digital regulatory framework lies in their institutional exclusion from the European governance system. Even so, institutional integration through various cooperation mechanisms could

4 European Commission. A Digital Single Market Strategy for Europe. COM(2015) 192 final. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, 2015. Accessed Jun 24, 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015DC0192

5 European Commission. ***Eastern Partnership***. European Neighbourhood Policy. Brussels: European Commission. Accessed June 24, 2025. https://enlargement.ec.europa.eu/european-neighbourhood-policy/eastern-partnership_en

create more favourable conditions for the full implementation of digital regulations and serve as a significant incentive in the broader integration process. At the same time, Serbia and Montenegro are digital markets, legal systems, and societies that share common regional characteristics typical of Southeast Europe. For this reason, this study includes the case of Croatia as a relevant and instructive reference point for a comparative analysis.

The aim of this study is to examine the institutional preconditions for the effective implementation of European digital legislation concerning digital services, digital markets, and artificial intelligence. Employing the Most Similar Systems Design, the research compares the institutional mechanisms of Croatia, Serbia, and Montenegro, focusing on their normative frameworks, structural composition, and capacity to enforce and uphold digital rights standards. By analysing these three cases, the study seeks to identify common challenges and opportunities in adapting to the evolving digital regulatory landscape. The central hypothesis is that contemporary digital issues, global in both scope and impact, cannot be effectively addressed through isolated national regulations. Instead, they require coordinated, multi-level governance and cross-border cooperation to ensure comprehensive and consistent application of digital legislation.

METHODOLOGY

This study begins with an analysis of the institutional design of three pivotal legislative instruments – the Digital Services Act (DSA),[6] the Digital Markets Act (DMA),[7] and the Artificial Intelligence Act (AIA)[8] – which establish the normative framework of the relevant institutional mechanisms. Beyond the European context, the national regulatory landscapes governing digital services, digital markets, and artificial intelligence in the candidate countries Serbia and Montenegro, as well as in Croatia, are also examined.

Subsequently, the study provides an in-depth review of the European institutional architecture established by these legislative acts, outlining the roles and responsibilities of key EU institutions within this governance framework. It also assesses the status of the most relevant national bodies identified as potential or designated regulators under the new legislative system.

The analysis further extends to the institutional capacities of these national authorities, focusing on their ability to effectively execute their mandated roles in compliance with legal provisions. This includes a comprehensive

6 European Union. 2022. *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act)*. Official Journal of the European Union, L 277/1–102. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A32022R2065

7 European Union. 2022. *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)*. Official Journal of the European Union, L 265/1–66. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925

8 European Union. 2024. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). Official Journal of the European Union*, L 168/1–185. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

examination of internal resources – technical, human, operational, and financial – and of their capacity to cooperate with other stakeholders within the newly established governance structures.

Methodologically, the study adopts a mixed-methods approach. It combines desk research, secondary analysis, and legal analysis to gather data and insights on institutional design and structure across the three sectors examined, at both the European and national levels. Complementing this, a series of eleven semi-structured expert interviews were conducted in June and July 2025 with specialists possessing in-depth knowledge of the institutions under review. The comparative analysis focuses on Serbia and Montenegro, with Croatia – an EU member state actively implementing the new regulations – serving as a reference point.

The overarching objective of this study is twofold: to provide a comprehensive analytical and comparative overview, and to formulate actionable recommendations that facilitate the effective implementation of the DSA, DMA, and AIA, primarily within candidate countries. This includes examining the conditions, prerequisites, and potential pathways for integrating Serbia and Montenegro into the Digital Single Market. To support the study's advocacy component, supplementary interviews were also conducted, building upon the findings of the initial research phase.

INSTITUTIONAL DESIGNS FOR DIGITAL GOVERNANCE IN THE EU AND BEYOND

EU INSTITUTIONAL DESIGN FOR DIGITAL SERVICES, DIGITAL MARKETS, AND AI

In recent years, the European Union has introduced a comprehensive regulatory framework for the digital environment within its territory guided by the principle that "what is illegal offline is also illegal online". This effort involves the adoption of several legislative acts aligning national laws with this framework and creating a new European institutional design for the digital sphere. The Digital Services Act (DSA), Digital Markets Act (DMA), and Artificial Intelligence Act (AIA) are the cornerstone regulations that normatively redefine the EU's digital ecosystem. By addressing the most pressing systemic challenges, these acts aim to establish a new value structure for the digital world.

GOVERNING DIGITAL SERVICES IN THE EU: DIGITAL SERVICES ACT (DSA)

The institutional design of the DSA aims to create an accountable digital environment. Rather than addressing individual pieces of content or specific online services, the DSA focuses on the structural factors that undermine digital rights and democratic values in the EU – factors that also underpin the business models of major digital platforms. This marks a significant institutional shift from a content-centric approach to structural solutions

targeting the systems and processes deployed by Big Tech. By adopting a systemic approach, the DSA introduces due-diligence obligations, together with risk assessment and mitigation measures scaled according to the number of users, thereby ensuring greater accountability in the digital space.

The DSA classifies intermediary service providers into the following categories:

- Mere conduits – services that enable access to and transmission of information within a communication network, without any intervention in the initiation of the transmission process, modification of the content, or selection of recipients of the services.
- Caching – services that provide automatic and temporary storage of information within a communication network to facilitate more efficient transmission of information to other service recipients upon request.
- Hosting – services that involve the storage of information provided by a service recipient at their request, without any intervention in the content by the service provider.
- Online platforms – services that not only store information upon request but also disseminate it to the public, making it potentially accessible to everyone.
- Very Large Online Platforms and Search Engines (VLOPSEs) – online platforms reaching at least 45 million monthly users, equivalent to 10 per cent of the EU's population.

A key feature of the DSA is the introduction of due-diligence obligations applicable to all digital intermediary services. However, these obligations are tailored to address specific risks and are proportionate to the category of the service.

OBLIGATION	VLOPSES	ONLINE PLATFORMS	HOSTING SERVICES
Transparency reporting	✓	✓	✓
Transparent terms and conditions	✓	✓	✓
Point of contact for users	✓	✓	✓
Point of contact for authorities	✓	✓	✓
Legal representative	✓	✓	✓
Notice and action procedure	✓	✓	✓
Reporting of crimes	✓	✓	✓
Statement of reasons for moderation decisions	✓	✓	✓
Internal complaint-handling system	✓	✓	
Out-of-court dispute resolution	✓	✓	
Cooperation with trusted flaggers	✓	✓	
Measures against misuse of the service and complaint mechanisms	✓	✓	
Reporting on number of users	✓	✓	
Transparency of advertising	✓	✓	
SoR Transparency Database	✓	✓	
Transparency of recommender systems	✓	✓	
Protection of minors	✓	✓	
Non-manipulative design	✓	✓	
Reliable trade	✓	✓	
Risk assessment and mitigation measures	✓		
Crisis response mechanism	✓		
Compliance function	✓		
Independent audits	✓		
Opt out of profiling option	✓		
Data sharing with authorities and users	✓		
Moderation transparency	✓		
Ads Database	✓		
Supervisory fee	✓		

Considering digital issues such as hate speech, disinformation, and manipulative content and design, the Act seeks to ensure the removal of illegal content and a clear distinction between promotion and information. It requires a reliable and non-manipulative technological infrastructure, as well as clear and unambiguous contractual agreements. Finally, full legal compliance is established as a fundamental requirement, all contributing to a more trustworthy and healthier digital environment.

Furthermore, the EU has incorporated transparency as one of the normative pillars of the DSA, requiring intermediary service providers to be transparent towards recipients, authorities, and independent stakeholders such as researchers, academia, and civil society. Transparency provisions are essential to ensure that recipients are fully informed about the rules and infrastructure governing the European digital ecosystem: terms and conditions, recommending systems, auditing, compliance, and content-moderation decisions, policies and practices.

Establishing a safe online environment is also among the key goals of the DSA, which seeks to ensure the safety of individuals, particularly minors, and the integrity of the broader digital ecosystem. The Act further establishes a framework that protects individuals and empowers them to participate in the regulatory mechanisms of digital services and the wider digital environment.

Finally, the DSA introduces a horizontal framework for institutionalised accessibility. In particular, Very Large Online Platforms and Search Engines (VLOPSEs), responsible for assessing compliance and systemic risks, are made specifically available for external monitoring and research activities.

GOVERNING DIGITAL MARKETS IN THE EU: DIGITAL MARKETS ACT (DMA)

While the DSA focuses on systemic platform accountability to directly benefit end users, the DMA targets the business operations of Big Tech. It seeks to promote fair and open market conditions, ensuring greater market democratisation. Specifically, the DMA regulates gatekeepers – dominant tech companies that monopolise key areas of the digital market – by scrutinising the advantages they gain through opaque practices. The Act addresses transparency through regular auditing and compliance

measures, guarantees fair and unrestricted access to third-party content on gatekeepers' services, and mandates verification and auditing of their advertising practices.

According to the DMA, the principle of accountability is crucial for maintaining free, open, and competitive market practices. Gatekeepers are required to obtain users' explicit consent for the collection, processing, and sharing of their data. This includes the right of users to withdraw consent at any time and to transfer their data to another company's services. Gatekeepers must also refrain from self-preferencing and ensure that all service providers enjoy equitable access to promote their own products and services on gatekeeper platforms.

A core principle of gatekeeper compliance under the DMA is interoperability, which ensures that end users can choose their preferred services rather than being locked into a gatekeeper's offerings by default. To prevent market dominance, the DMA introduces strict mechanisms encouraging smaller platforms and users to curate their own digital experiences. This means that all digital services must remain accessible under equal conditions. Interoperability also allows users to partially or fully disengage from a service, ensuring they are not confined to dominant providers. Non-compliance with these rules is considered interference with fair market competition and may result in severe financial penalties. Closely related to interoperability is the principle of data mobility, which is equally necessary for a democratic digital market. Smaller businesses must have continuous and real-time access to their user data to evaluate the products and services they provide on gatekeepers' core platform services.

The Digital Markets Act (DMA) establishes two categories of obligations for gatekeepers: self-executing obligations (Article 5), which are clear and precise enough to be implemented without prior consultation with the European Commission, and obligations susceptible to further specification (Articles 6 and 7), which may require dialogue between the Commission, gatekeepers, and third parties to determine appropriate compliance measures.

Among their obligations, gatekeepers must allow third parties to interoperate with their services in certain cases; enable business users to access the data they generate on the platform; provide advertisers and publishers with tools for independent ad verification; and permit business users to promote and sell their products outside the gatekeeper's platform.

Conversely, gatekeepers are prohibited from favouring their own products or services over those of third parties in rankings; blocking consumers from connecting with external businesses; restricting users from uninstalling pre-installed apps; and tracking users outside their core platform services for targeted advertising without obtaining proper consent.

GOVERNING AI IN THE EU: ARTIFICIAL INTELLIGENCE ACT (AIA)

The primary aim of the AI Act is to prevent and mitigate the adverse effects of artificial intelligence by introducing a cross-cutting, ex-ante risk-management framework. The Act seeks to safeguard health, safety, and fundamental rights in the development, deployment, and use of AI systems, complementing existing EU legislation such as the GDPR and product-safety rules. Its core pillars include transparency, risk prevention, and multi-layered oversight, supported by obligations tailored to the level of risk an AI system presents.

Harm prevention and mitigation are at the centre of the Act's risk-based structure. The regulation defines four tiers of risk: unacceptable, high, limited, and minimal. Unacceptable-risk systems, such as certain forms of biometric categorisation or social scoring, are prohibited. High-risk AI systems must comply with robust requirements covering data governance, cybersecurity, accuracy, robustness, human oversight, and resilience against unauthorized interference. Providers must establish quality management systems and post-market monitoring mechanisms to ensure continuous compliance throughout the system's lifecycle. Obligations also apply to deployers, distributors, and importers, while developers of general-purpose AI models face a dedicated set of responsibilities depending on the model's capabilities and associated risks.

Transparency requirements vary across system categories. Providers of high-risk AI systems must maintain comprehensive technical documentation, ensure record-keeping and logging, register their systems in the EU database, and inform deployers about the system's functioning, capabilities, and limitations. Users must be notified when they are interacting with an AI system, and AI-generated or AI-manipulated content must be clearly labelled. Developers of general-purpose AI models, particularly those with systemic risk, must also publish high-level information about the

training data used and comply with documentation and copyright-related obligations. Public authorities using high-risk AI systems must comply with additional transparency duties, including informing individuals affected by high-risk AI decisions.

Oversight of AI systems operates through a combination of human supervision, national authorities, and EU-level bodies. Human oversight requirements ensure that high-risk AI systems remain subject to meaningful human control and intervention. National competent authorities oversee high-risk systems through market surveillance and enforcement, while notified bodies perform conformity assessments where required. The EU AI Office supervises general-purpose AI models—especially those posing systemic risks—and coordinates enforcement across the Union. Individuals and organisations may file complaints about suspected violations of the AI Act, and individuals must receive meaningful information when high-risk AI is used to make decisions that significantly affect them.

INSTITUTIONAL DESIGN FOR DIGITAL GOVERNANCE IN CROATIA

Croatia has been slow to implement EU digital regulations. It missed the deadline set by the AI Act for designating a market surveillance authority, and the working group tasked with drafting the implementing legislation had held only one meeting as of May 2025. In July 2024, the European Commission launched infringement proceedings against Croatia for failing to grant the designated Digital Services Coordinator (DSC) the necessary powers under the DSA.[9] The national law implementing the DSA was adopted only in April 2025. Presumably due to the limited role of national authorities under the Digital Markets Act (DMA), the legal framework for its implementation in Croatia consists of an executive order containing only one substantive article.

Meaningful stakeholder participation is severely undermined by Croatia's opaque, closed, and highly centralised legislative process. The composition of working groups is not systematically disclosed and is left to the full discretion of the minister, with no formal criteria or transparent procedure. Inputs from public consultations are largely disregarded, and the process serves a formal rather than substantive function.[10] While Croatia operates de iure under a ministerial cabinet system, in practice it resembles a chancellor model. When it comes to legislation, any document that a ministry intends to submit for public consultation must first obtain approval of the Prime Minister's Office. This is particularly the case for legislation and policy labeled as dealing with "EU matters", which are subject to a separate legislative procedure in the Parliament and attract little political interest or public scrutiny. Due to the centralised process for approving legislative drafts, there are strong institutional incentives to keep the substance of legislation unchanged from the public consultation phase through to the second reading in Parliament and final adoption. This dynamic is

9 European Commission. "Commission calls on 6 Member States to comply with the EU Digital Services Act". 25 July 2024. Accessed 24 June 2025. https://digital-strategy.ec.europa.eu/en/news/commission-calls-6-member-states-comply-eu-digital-services-act

10 "Savjetovanja o novim zakonima i dalje su kratka, neka traju samo pet dana" [Consultations on new laws are still short, some last only five days]. Faktograf, 13 May 2025. Accessed 24 June 2025. https://faktograf.hr/2025/05/13/savjetovanja-o-novim-zakonima-i-dalje-su-kratka-neka-traju-samo-pet-dana/

especially problematic for human rights organisations, which have limited opportunities to ensure that human rights considerations are meaningfully integrated into legislative and regulatory processes.

Despite the important role envisioned for civil society organizations (CSOs) in the enforcement of the DSA – particularly as Trusted Flaggers – Croatian CSOs have been largely sidelined by the Ministry of Justice, Administration and Digital Transformation. The persistent unwillingness to include civil society actors in crucial decision-making processes carries a significant risk that Croatia's emerging AI legal and policy framework will lack a human rights perspective. Furthermore, systemic deficiencies in state support for the work of CSOs severely undermine the likelihood that such organisations will be able to assume the roles and responsibilities envisaged for them under EU regulations.

INSTITUTIONAL DESIGN FOR DIGITAL SERVICES IN CROATIA

The Law on the implementation of the Digital Services Act was adopted in April 2025.[11] This piece of legislation can be considered a skeleton implementation law, containing only the bare minimum of provisions, most of which refer directly to relevant articles of the DSA. Excluding the provisions on sanctions, the law comprises 13 substantive articles.

The implementing law designates the Croatian telecom regulator, the Regulatory Authority for Network Industries (*Hrvatska regulatorna agencija za mrežne djelatnosti, hereinafter: HAKOM*), as the Digital Services Coordinator. Seven public bodies are explicitly listed as authorised to issue orders for the removal of illegal content (Article 9) and orders to provide information (Article 10). An additional blanket provision also authorises "other public bodies, in line with their competences defined by a special law which regulates their scope of work". The law defines the redress

11 Zakon o provedbi Uredbe (EU) 2022/2065 Europskog parlamenta i Vijeća od 19. listopada 2022. o jedinstvenom tržištu digitalnih usluga i izmjeni Direktive 2000/31/EZ (Akt o digitalnim uslugama) (NN 67/2005) [Act on the Implementation of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act) (OG 67/2005)]. Accessed 24 June 2025. https://narodne-novine.nn.hr/clanci/sluzbeni/2025_04_67_857.html

mechanism for challenging orders issued under Articles 9 and 10 of the DSA, designating the Zagreb Municipal Court as the competent authority. The maximum fines for legal entities are aligned with the thresholds set by the DSA: up to 6 per cent of annual global turnover for breaches of substantive obligations and up to 1 per cent for non-cooperation during investigations. Modest fines (EUR 1,000–6,000) are also foreseen for responsible individuals within companies, reflecting the national approach to personal liability in regulatory enforcement.

The broad blanket provision on national authorities is expected to pose significant challenges to the effective enforcement of the DSA in Croatia. The total number of public bodies authorised to issue content-removal orders or conduct inspections remains unclear, creating both legal and practical uncertainty. For example, the law does not explicitly designate the State Electoral Commission as the authority responsible for issuing removal orders related to electoral content; instead, this role is only implicitly assigned through the general blanket clause. Similarly, the law states that all listed public bodies – as well as those covered by the blanket provision – are tasked with implementing Articles 25, 26, 30, 31, and 32 of the DSA. Such diffuse and overlapping institutional design is likely to lead to coordination difficulties and a dilution of institutional accountability. As noted by the Office of Ombudsperson in public remarks, "It is...not sufficiently clear who is responsible for doing what and how".[12]

The law does not regulate Trusted Flaggers or out-of-court dispute resolution bodies. Instead, it defers these key elements to bylaws to be adopted by the Council of HAKOM – a collegial executive body – within three months of the law's entry into force. However, despite the expiry of this deadline, the relevant bylaws have not yet been submitted for public consultation, raising concerns about significant delays in operationalising key mechanisms under the DSA.

To mitigate the risk of Croatia falling short of its EU obligations and domestic expectations for legal certainty and user protection, it is essential

12 "Hakom već provodi EU akt o uklanjanju nezakonitog sadržaja na Internetu: kazne do 66.360 eura" ["HAKOM already enforcing the EU Act on removing illegal online content: Fines up to 66,360 Euros"] Lider Media, 16 October 2024. Accessed 24 June 2025. https://lidermedia.hr/info/hakom-vec-provodi-eu-akt-o-uklanjanju-nezakonitog-sadrzaja-na-internetu-kazne-do-66-360-eura-159502/

to establish clearer legal mandates, adopt the missing bylaws, and ensure the systematic inclusion of CSOs at all levels of implementation and policy development.

INSTITUTIONAL DESIGN FOR DIGITAL MARKETS IN CROATIA

Rather than adopting a dedicated law, Croatia has opted to implement the DMA through an executive order issued by the Government. This approach is grounded in Article 30 of the Law on the Government of the Republic of Croatia,[13] which authorises the Government to adopt executive orders for the implementation of EU law in cases where the adoption of a new law is not deemed necessary. This method appears to have been deemed appropriate, as national authorities are not granted an enforcement role under the DMA but are instead assigned a supporting function, primarily assisting the European Commission in complementary investigations.

The Decree on the Implementation of the Digital Markets Act (DMA)[14] was issued in November 2023, formally designating the Croatian Competition Agency (*Agencija za zaštitu tržišnog natjecanja, hereinafter: AZTN*) as the competent national authority for its enforcement.

Excluding the explanatory, introductory, and concluding provisions, only one article addresses the substance of the matter. Article 3 of the Decree designates the AZTN as the enforcement authority and assigns it the relevant tasks.

13 Zakon o Vladi Republike Hrvatske (NN 150/11, 119/14, 93/16, 116/18, 80/22, 78/24) [Act on the Government of the Republic of Croatia (OG 150/11, 119/14, 93/16, 116/18, 80/22, 78/24)] neslužbena pročišćena verzija (unofficial consolidated version). Accessed 24 June 2025. https://www.zakon.hr/z/170/zakon-o-vladi-republike-hrvatske

14 Uredba o provedbi Uredbe (EU) 2022/1925 Europskog parlamenta i Vijeća od 14. rujna 2022. o pravednim tržištima s mogučnošću neograničenog tržišnog natjecanja u digitalnom sektoru i izmjeni Direktiva (EU) 2019/1937 i (EU) 2020/1828 (Akt o digitalnim tržištima) (NN 131/2023) [Regulation on the Implementation of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OG 131/2023)] Accessed 24 June 2025. https://narodne-novine.nn.hr/clanci/sluzbeni/2023_11_131_1799.html

INSTITUTIONAL DESIGN FOR AI IN CROATIA

As of October 2025, Croatia has not yet adopted the law implementing the AI Act. The legislative working group of the Ministry of Justice, Public Administration and Digital Transformation held its initial meeting in May 2025. As expected, Croatia failed to meet the 2 August 2025 deadline to designate at least one market surveillance authority and one notifying authority.

Croatia submitted its list of public bodies designated to safeguard fundamental rights in relation to high-risk AI systems in December 2024 – one month after the deadline set by the AI Act. The list was submitted to the European Commission by the Ministry of Justice, Public Administration and Digital Transformation through Croatia's Permanent Representation in Brussels.[15]

In addition to the Public Ombudsperson and specialised ombudspersons – for children, gender equality, and persons with disabilities – the list of designated authorities also includes the Croatian Personal Data Protection Agency (*Agencija za zaštitu osobnih podataka; hereinafter: AZOP*), the State Electoral Commission, and the Agency for Electronic Media.

Nevertheless, human rights organisations have been entirely excluded from the legislative and policy-making process related to artificial intelligence, while representatives of industry interests are routinely included as standard practice.[16]

According to information received by the privacy watchdog organisation Politiscope, the Ombudsperson, AZOP, CroAI – a private industry association – all of whom are members of the legislative working group,

15 Ministry of Justice, Public Administration and Digital Transformation. "Objavljen popis nadležnih tijela sukladno Uredbi o umjetnoj inteligenciji" ["List of competent authorities published in accordance with the AI Act"]. 5 December 2024. Accessed 24 June 2025. https://mpudt.gov.hr/vijesti/objavljen-popis-nadleznih-tijela-sukladno-uredbi-o-umjetnoj-inteligenciji/29657

16 Ministry of Justice, Public Administration and Digital Transformation. "Radne skupine za izradu nacrta prijedloga zakona, drugih propisa i akata." [Working groups for drafting proposals of laws, other regulations and acts] Accessed 24 June 2025. https://mpudt.gov.hr/pristup-informacijama-6341/savjetovanja-s-javnoscu/radne-skupine-za-izradu-nacrta-prijedloga-zakona-drugih-propisa-i-akata/6230

supported Politiscope's request for inclusion of CSOs in the group. However, the request was ignored by the Ministry of Justice, Public Administration and Digital Transformation, which leads the process.

The exclusion of civil society is particularly problematic given the important role envisaged for such organisations under the AI Act – especially in areas such as the fundamental rights impact assessments (FRIAs), oversight of high-risk systems, and the representation of vulnerable groups.

INSTITUTIONAL DESIGN FOR DIGITAL GOVERNANCE IN SERBIA

Serbian legislation currently in force does not recognise most of the substantive rules or enforcement mechanisms introduced by the DSA, DMA, and AI Act. This creates a substantial gap between the comprehensive regulatory frameworks adopted in the EU and the far more limited provisions contained in Serbian law.

At the same time, Serbia's regulation of the digital sphere has, for more than a decade, been shaped by the need to align with an earlier generation of EU rules, both as part of the EU accession process and as a reflection of European regulatory standards. A clear example is the 2018 Personal Data Protection Law, which represents a domesticated version of the GDPR.

Still, certain Serbian laws address issues related to digital services, digital markets, and artificial intelligence. These provisions, however, represent only partial alignment with the EU acquis, establishing some foundations but falling far short of the comprehensive and systemic frameworks recently adopted by the EU. In practice, Serbia faces the significant challenge of harmonising with the DSA, DMA, and AI Act.

INSTITUTIONAL DESIGN FOR DIGITAL SERVICES IN SERBIA

Serbia does not yet have a legal framework that directly regulates issues addressed by DSA. Several general and sectoral laws partially cover certain DSA-related areas, although none replicate the scope or regulatory architecture of the DSA.

The most relevant general law is the Law on Electronic Commerce, harmonised with the EU Directive on Electronic Commerce, the predecessor of the DSA. It regulates information society services, including obligations related to transparency, liability of service providers, contracts in electronic form, and commercial communications. The law also empowers courts to restrict certain online services under specific conditions, which is conceptually aligned with DSA mechanisms, though considerably narrower in scope.

A more recent step toward DSA-related regulation is the Regulation on Mandatory Measures for Video-Sharing Platform (VSP) Service Providers, adopted under the Law on Electronic Media. It introduces obligations to protect users, particularly minors, from harmful content and to ensure transparency in audiovisual commercial communications. While these provisions represent progress, they remain limited to content harmful to minors and illegal audiovisual material, without addressing systemic risks, algorithmic transparency, or broader platform accountability.

Beyond these acts, other laws – such as the Consumer Protection Law, the Law on Information Security, and the Law on Electronic Communications – provide a potential foundation for future DSA-aligned regulation but currently lack direct provisions reflecting DSA principles and obligations.

Serbia's legal framework still relies primarily on judicial enforcement. Penalties under the Law on Electronic Commerce are imposed by the courts, and no specialised administrative bodies exist that are comparable to EU Digital Services Coordinators. Nor does the framework include requirements for periodic transparency reporting, mandatory legal representatives for platforms, or risk-based content governance mechanisms.

In 2024, Serbia adopted a bylaw introducing limited obligations for VSPs, signalling an initial step toward modernising the framework in line with the DSA. Nevertheless, this remains an isolated measure. Overall, while Serbia's existing laws establish certain foundational rules, key aspects, such as systemic platform accountability, algorithmic oversight, and coordinated enforcement, remain unregulated.

INSTITUTIONAL DESIGN FOR DIGITAL MARKETS IN SERBIA

There are no laws in Serbia that regulate DMA-related issues as such. Still, several general or sectoral laws address matters relevant to the scope of the DMA from different angles.

General fair competition rules applicable to all markets are set out in the EU-harmonised Law on Protection of Competition. Its relevance for digital markets has so far been modest, and its applicability to these markets has not yet been tested in the decision-making practice of the Serbia's Commission for the Protection of Competition. However, the Commission conducted

a sectoral analysis of competition in the market for digital platforms mediating the sale and delivery of restaurant food and other products during the period 2020-2021. In that report, it explicitly referenced DMA and recommended the adoption of further regulation in this area in Serbia, although no subsequent steps were taken by the Commission following the publication of the analysis.

Another relevant general law is the Personal Data Protection Law of 2018, harmonised with the GDPR. This law regulates personal data-related complaint mechanisms, the right to data portability, and the collection of personal data relevant to the provision of information society services, including those constituting core platform services under the DMA.

One of the most relevant sectoral laws in DMA context is the Law on Electronic Commerce. To some extent, it is based on the EU Directive on Electronic Commerce and regulates the provision of information society services in accordance with that directive's rules. While the definitions of information society services in the Law on Electronic Commerce and of core platform service under the DMA are not identical, the overlap is significant, indicating that Serbian law already recognises some fundamental concepts in this area of regulation. The Law on Electronic Commerce also contains provisions on contracts concluded at a distance or in electronic form, while additional rules in this regard can be found in the Consumer Protection Law and the Trade Law.

Finally, it is worth noting that Serbia's Trade Law recognises the concept of an "electronic platform" as a means by which a person, acting as an information society service provider, enables electronic trading between parties. The person managing the electronic platform may also use it to sell their own goods or services. Yet, the only provisions in this law concerning such platforms address trade relations with end users, in their capacity as consumers.

INSTITUTIONAL DESIGN FOR AI IN SERBIA

At the time of writing, Serbia has a government-established working group tasked with drafting a national AI law. No public draft is currently available, although unofficial information suggests that the text should be finalised and adopted by Parliament by the end of 2025.

Although there are currently no laws or regulations governing artificial intelligence in Serbia, a significant piece of soft law exists – The Ethical Guidelines for the Development, Implementation, and Use of Reliable and Responsible Artificial Intelligence (hereinafter: Guidelines). The Guidelines were issued by the Serbian Government in February 2023 as an output of the Artificial Intelligence Development Strategy in the Republic of Serbia for the Period of 2020-2025 (Strategy, 2019) and its accompanying Action Plan for the Period 2020-2022 (Action Plan, 2020). The Strategy and the Action Plan contain a number of specific activities that were to be implemented during their respective periods of validity. Most of these activities do not appear to have been implemented yet, but it remains to be seen what new legal rules will be introduced once the AI law is adopted.

As expected for a soft-law instrument, the Guidelines provide general best-practice recommendations for companies that develop and/or use AI systems. They set out fundamental principles that should serve as a basis for creation, deployment, and use of AI systems – including explainability and verifiability, human dignity, prevention of harm, and fairness – and outline the conditions for reliable and responsible artificial intelligence. These conditions consist of verifiable parameters, both technical and non-technical, that confirm and demonstrate compliance with the stated principles.

Although not explicitly stated in the text, the Guidelines are grounded in the risk-assessment logic of the AI Act. They include a detailed explanation of what constitutes a high-risk AI system. While no AI systems are explicitly prohibited, the Guidelines specify that they do not apply to systems that are banned under some specific legislation.

INSTITUTIONAL DESIGN FOR DIGITAL GOVERNANCE IN MONTENEGRO

Montenegro is still in the early stages of developing an institutional framework for governing digital services, markets, and artificial intelligence. While no dedicated laws currently mirror the scope and requirements of the DSA, DMA, or AIA, several general and sector-specific laws touch upon relevant issues. These include legislation on electronic commerce, electronic communications, consumer protection, and competition. That said, regulatory provisions remain fragmented, uncoordinated, and in most cases outdated, lacking the comprehensive standards and safeguards introduced by the EU's digital regulatory package.

A working group established by the Ministry of Culture and Media marks an important first step in exploring how national laws could be harmonised with the DSA. In the area of digital markets, competition is regulated under a general legal framework that could support DMA objectives, although it lacks sector-specific rules addressing gatekeepers or systemic market imbalances. As for artificial intelligence, Montenegro currently has no legal framework, though strategic planning in this area is anticipated in 2025 or 2026. A coherent institutional design will be crucial for Montenegro to both participate in and benefit from the European digital regulation.

INSTITUTIONAL DESIGN FOR DIGITAL SERVICES IN MONTENEGRO

There is currently no law in Montenegro that directly regulates matters covered by the Digital Services Act (DSA). In the course of preparing this study, the Ministry of Culture and Media of Montenegro established a working group, marking the beginning of an initiative to align national regulations with the EU framework for digital services. Several general and sector-specific laws address some of the issues falling within the scope of the DSA, though not in a systematic or harmonised manner.

One of the most relevant laws in this context is the Law on Electronic Commerce, which is broadly aligned with the EU Directive on Electronic Commerce. Still, it does not incorporate the updated standards introduced by the DSA, particularly those concerning platform accountability,

systemic risk management, and transparency obligations. Nonetheless, the law establishes basic rules for service providers, including requirements for information disclosure and the identification of commercial communications.

The Law on Electronic Identification and Electronic Signature, together with the Law on Electronic Document, establish the legal basis for authentication and trust services, elements that could support the implementation of certain reliability standards envisioned by the DSA. For example, although Montenegrin law does not currently require platforms to verify the identity of traders, existing provisions on electronic identification and qualified trust services could serve as a foundation for introducing such obligations in the future.

Montenegro's Law on General Product Safety requires traders and distributors to notify market surveillance authorities if they become aware of risks associated with certain products. However, online platforms are not currently obliged to inform consumers about illegal or dangerous products sold through their services, nor are they required to take proactive measures to monitor such risks.

The Consumer Protection Law and the Law on Electronic Communications also contain provisions that are partially relevant to DSA-related issues. For example, the Law on Electronic Communications requires operators to provide data to the national regulatory authority – the Agency for Electronic Communications and Postal Services (*Agencija za elektronske komunikacije i poštansku djelatnost, EKIP*) – upon request, including certain financial and infrastructure-related information. Yet, there are no obligations for online platforms to publish transparency reports, disclose algorithmic decision-making processes, or provide information on content moderation policies, as prescribed by the DSA.

When it comes to user redress, Montenegrin law does not require hosting providers or online platforms to establish systems for reporting illegal content or internal complaint-handling mechanisms. Consumers may rely on general complaint procedures under the Consumer Protection Law, although these are not specifically designed for digital services.

In terms of safety, certain obligations exist under several laws, including the Law on Electronic Communications and the Law on Electronic Commerce. For example, service providers may be required to notify competent

authorities if users engage in prohibited or illegal activity via their platforms. Additionally, Montenegrin authorities are authorised to impose restrictive measures on EU-based service providers if their services pose serious risks to public order or consumer safety. Yet no provisions currently require online platforms to conduct risk assessments or implement specific mitigation measures, as envisaged by the DSA.

Montenegrin law does not require providers to appoint points of contact or legal representatives for communication with national authorities or users. Nor does it impose obligations related to interface design, recommender systems, or independent audits of very large platforms.

Supervision of the digital environment is currently divided among several institutions, including the Agency for Electronic Communications and Postal Services, the Competition Protection Agency, the Agency for Personal Data Protection and Free Access to Information, the Consumer Protection Council, and the relevant ministries. No single regulatory body has yet been empowered to oversee digital services in a comprehensive manner.

INSTITUTIONAL DESIGN FOR DIGITAL MARKETS IN MONTENEGRO

There is currently no explicit law addressing DMA-related matters in Montenegro. In general, competition issues are regulated by the Competition Protection Law, which regulates restrictive agreements and the abuse of dominant position on a general, non-sector specific basis. This law can serve as a legal foundation for supporting the DMA's objectives, as it enforces rules against anti-competitive practices that could hinder the freedom of information society service providers to set prices and conditions, thereby ensuring a competitive and fair market environment.

The Law on Electronic Commerce regulates several matters relevant to digital markets governance. From this perspective, it may indirectly contribute to achieving demonopolisation goals. For example, it sets out obligations for information society service (ISS) providers to ensure compliance with various regulatory areas – such as copyright, industrial property rights, and consumer contracts – as well as responsibilities and liabilities regarding data storage, transmission, and access to third-party data. These rules promote the freedom to provide services without unnecessary bureaucratic hurdles,

enhance market access and opportunities for service providers, and protect consumers from deceptive practices and unsolicited communications. The Law on Electronic Commerce also prescribes that every commercial ISS message must meet specific information requirements and regulates the use of electronic communications for sending unsolicited commercial messages.

The Law on Electronic Communications is another piece of legislation that addresses certain DMA-related issues, drawing inspiration from EU law. In particular, it includes provisions on users' rights to submit complaints to service operators concerning access, service quality, and billing matters, as well as rules governing the complaints procedure and applicable deadlines.

The Consumer Protection Law requires traders to adhere strictly to displayed prices and obliges them to advertise prices in accordance with the relevant legislation. It also sets out rules on price reductions and clearance sales, including related conditions and transparency requirements.

INSTITUTIONAL DESIGN FOR AI IN MONTENEGRO

At present, Montenegro has no legislation regulating the use of AI systems. A government AI strategy is planned for 2025 or 2026, but no draft or text of the strategy has yet been made publicly available.

COMPARATIVE DISCUSSION

Croatia, Serbia, and Montenegro occupy distinct positions in aligning their national frameworks with the European Union's emerging digital regulatory architecture. Croatia, as an EU member state, is legally required to transpose and implement these instruments, whereas Serbia and Montenegro, as candidate countries, face the more complex task of gradually harmonising their legislation and institutions with EU standards without being part of the Union's formal enforcement structures. These divergent trajectories highlight how differences in EU membership status, and policymaking capacities and practices, shape the pace and depth of digital governance reforms and, ultimately, the overall maturity of regulatory design in the three countries.

COMPARING INSTITUTIONAL DESIGNS FOR DIGITAL SERVICES

Croatia, Serbia, and Montenegro approach the DSA legal framework in different ways, yet all display specific forms of incompleteness when moving beyond the earlier Directive on Electronic Commerce toward a systemic model of platform accountability.

Croatia enacted a dedicated implementation law in April 2025, formally integrating the DSA into national legislation. The act is highly minimal, consisting largely of cross-references to the EU regulation and deferring key mechanisms, such as trusted flaggers and out-of-court dispute resolution, to future bylaws. Reliance on broad blanket provisions for designating competent bodies creates uncertainty about the precise allocation of responsibilities. Croatia has therefore achieved formal transposition without establishing the comprehensive normative framework necessary for effective DSA implementation.

Serbia has not yet adopted a dedicated DSA law. Its legal environment remains governed by the Law on Electronic Commerce, harmonised with the older Directive on Electronic Commerce, and by a 2024 bylaw on video-sharing platforms. These instruments regulate issues such as commercial communication and the protection of minors but omit the DSA's systemic

requirements. Serbia's legal design, therefore, represents a partial adaptation of outdated EU law rather than a substantive step toward the DSA model.

Montenegro illustrates a different trajectory. The establishment of a working group within the Ministry of Culture and Media in 2025 marks a constructive first step toward harmonisation with the DSA. Yet the existing legal framework dominated by the 2013 Law on Electronic Commerce and supplemented by provisions in communications and consumer protection laws, remains fragmented and outdated. It still lacks a dedicated legal basis for the DSA's layered obligations and platform accountability mechanisms.

In comparative perspective, Croatia exemplifies legal minimalism through skeletal transposition, Serbia continues to rely on obsolete frameworks, and Montenegro is only beginning its harmonisation process. Despite these differences, all three cases reveal a shared set of potential challenges. Their current legal designs do not yet reflect the DSA's ambition to establish a coherent and systemic regulatory regime for digital services. Unless forthcoming bylaws, new legislation, or strategic initiatives address these gaps, there is a significant risk that national frameworks will remain only partially aligned with the comprehensive legal architecture envisioned at the EU level.

COMPARING INSTITUTIONAL DESIGNS FOR DIGITAL MARKET

Since the most substantive regulatory powers under the DMA remain at the European level, national legislatures assume only a subsidiary role, focused on designating competent authorities and establishing procedural links to EU-level enforcement. This arrangement limits the scope for domestic legal development, leaving room for future adjustments once EU-level practice becomes more clearly defined.

Croatia has implemented the DMA through a concise executive order issued in November 2023, designating the Croatian Competition Agency (AZTN) as the competent national authority. This minimalist approach mirrors the DMA's design, in which national authorities primarily play a supporting role by assisting the European Commission in enforcement. While this ensures compliance with EU obligations, it leaves limited scope for developing a more detailed national regulatory framework.

Serbia does not have specific legislation directly regulating DMA-issues. Instead, it relies on the general Law on Protection of Competition, whose applicability to digital markets remains largely untested. The same holds for other relevant acts, such as the Personal Data Protection Law and the Law on Electronic Commerce, which address related aspects but not core platform services or gatekeeper regulations. While these laws provide a basis for tackling anti-competitive practices, their relevance to the DMA's focus on gatekeeper regulation is only indirect. Unless new legislation is introduced, reliance on these existing frameworks may constrain Serbia's capacity to regulate the contemporary digital market effectively.

Montenegro also lacks an explicit legislation addressing DMA-related matters, relying instead on its general Competition Protection Law and the Law on Electronic Commerce, which can only indirectly support DMA objectives through the enforcement of general competition rules. As these baseline provisions remain sector-specific and rooted in older regulatory models, Montenegro's legal framework would require significant adaptation to achieve alignment with the DMA in the future.

Therefore, while Croatia has a direct legal instrument for DMA implementation, aligning with the EU's centralised enforcement role, Serbia and Montenegro lack specific DMA legislation and rely instead on broader competition and e-commerce laws that do not target gatekeepers or the specific market imbalances addressed by the DMA. These legal acts have only indirect relevance for DMA compliance as they were not designed to meet the specific challenges of digital markets or the conduct of large online platforms. In both Serbia and Montenegro, existing laws provide only a conceptual foundation, serving primarily as a starting point for future alignment with the DMA framework.

COMPARING INSTITUTIONAL DESIGNS FOR AI

As of October 2025, Croatia has not yet adopted legislation implementing the AI Act, and further delays are expected in designating market surveillance authorities, despite the EU's deadline of 2 August 2025. Although Croatia has submitted a list of public bodies responsible for safeguarding fundamental rights in relation to high-risk AI systems, human rights organisations remain largely excluded from the legislative and policy-making process on AI.

Serbia has established a working group tasked with drafting an AI law, expected by the end of 2025, but currently has no specific AI legislation in place. It does, however, have the Ethical Guidelines for the Development, Implementation, and Use of Reliable and Responsible Artificial Intelligence – a soft law instrument prepared by the Serbian Government and based on the AI Act's risk-assessment logic, serving as a preparatory step.

Montenegro likewise has no legislation regulating AI systems. A government AI strategy is planned for 2025 or 2026, but no text has yet been made publicly available, indicating that the process remains at a very early stage of development.

Croatia's experience in implementing the AI Act illustrates the complexities of aligning national frameworks with ambitious EU digital legislation, offering valuable insights for Serbia and Montenegro. Despite the binding August 2025 deadline for designating market surveillance authorities, Croatia faces further delays, underscoring the significant technical and institutional challenges involved in such a transformative process. Furthermore, the continued exclusion of civil society organisations from Croatia's AI legislative and policy-making processes, as study highlights, exposes a major risk: the development of a legal framework lacking a human rights perspective.

For Serbia, which is currently developing its AI law and has already adopted ethical guidelines, Croatia's experience underscores the demanding legislative journey ahead and the importance of not only a robust legal text but also inclusive processes that incorporate diverse societal perspectives. For Montenegro, still in the early stages of strategic planning, the key lesson is the need for proactive engagement with all relevant stakeholders from the very outset of its AI strategy and subsequent legislation. Such an approach is essential to avoid the pitfalls of a centralised and non-transparent process that could undermine both the integrity and public trust in future AI governance.

INSTITUTIONAL STRUCTURES FOR DIGITAL GOVERNANCE IN THE EU AND BEYOND

EU INSTITUTIONAL STRUCTURE FOR DIGITAL SERVICES, MARKETS, AND AI

The institutional frameworks established under the DSA, DMA, and AIA comprise a range of bodies operating at both EU and national levels, designed to ensure consistent implementation of these new legislative acts. They encompass a combination of pre-existing and newly created entities with specific mandates. In addition to traditional public bodies, a variety of stakeholders – including service recipients, users, researchers, and experts – also assume institutional roles within the European digital governance ecosystem.

INSTITUTIONAL STRUCTURE UNDER THE DSA

The European Commission

The European Commission holds a pivotal role in the enforcement of the Digital Services Act (DSA). One of its key responsibilities is the designation of certain online platforms and search engines as Very Large Online Platforms or Very Large Online Search Engines (VLOPs and VLOSEs) where they have an average of at least 45 million monthly active users within the European Union (Article 33). At present, there is no official

EU methodology for calculating monthly active users, meaning that the designation process relies on self-reported data provided by the platforms themselves.

According to Article 43, designated VLOPs and VLOSEs are required to pay an annual supervisory fee to the European Commission, which is also responsible for determining the amount of that fee. The Commission is empowered to supervise and enforce compliance with the DSA in respect of VLOPs and VLOSEs (Article 56), as well as to monitor systemic risk assessments and rule infringements (Articles 64-66).

Under Article 57, the European Commission cooperates with the European Board for Digital Services (the Board). Together, they issue reports on major systemic risks (Article 35) and may activate crisis response mechanisms (Article 36). The Board may also refer disputes or communication issues to the Commission (Articles 59 and 60). Although the Commission chairs the Board, it does not hold voting rights, but provides administrative and analytical support. Additionally, any rules or procedures adopted by the Board are subject to the Commission's approval (Article 62).

The Commission also promotes the development and implementation of voluntary standards (Article 44) and codes of conduct aimed at supporting the objectives of the DSA (Article 45). It facilitates greater transparency in online advertising (Article 46) and promotes accessibility of online services for people with disabilities (Article 47). In addition, the Commission is empowered to activate crisis protocols in response to threats to public security or public health issues involving VLOPs and VLOSEs (Article 48).

Under the DSA, significant investigative and enforcement powers are vested in the European Commission. It may request information in cases of suspected infringements or non-compliance (Article 67), conduct interviews with relevant parties (Article 68), and carry out on-site inspections of VLOP and VLOSE premises (Article 69). Where necessary, the Commission may also impose interim measures to prevent the risk of serious harm (Article 70). Failure to comply with procedural obligations may result in fines of up to 1 percent of the provider's total annual worldwide turnover, while periodic penalty payments of up to 5 percent of the average daily worldwide turnover may be imposed for each day of delay in responding to requests for information or allowing inspections.

Beyond these procedural powers, the Commission is responsible for monitoring compliance by Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) (Article 72), adopting non-compliance decisions (Article 73), and imposing fines or periodic penalty payments in cases of substantive infringements. It may impose fines of up to 6 percent of the provider's total annual worldwide turnover for breaches of DSA obligations, non-compliance with interim measures, or breach of commitments (Article 74), and periodic penalty payments of up to 5 percent of the average daily worldwide turnover for each day of delay in complying with remedies, interim measures, or commitments (Article 76). VLOPs and VLOSEs retain the right to be heard during these procedures (Article 79), while enforcement actions are subject to a five-year limitation period (Articles 77–78). The Commission also adopts implementing acts setting out detailed rules for its investigative and enforcement procedures (Article 83).

Under Article 85, a secure and reliable information-sharing system must be established to facilitate communication between the Digital Services Coordinators, the Commission, and the European Board for Digital Services. The Commission is also empowered to adopt delegated acts, subject to the conditions laid down in Article 87.

Finally, the Commission is mandated to develop guidelines on several key aspects of the DSA's implementation, including the design and organisation of online interfaces (Article 25), the protection of minors online (Article 28), the methodology for calculating monthly active users (Article 33), and the structure and operation of advertising information repositories (Article 39).

European Board for Digital Services

Established under the DSA, the European Board for Digital Services acts as an independent advisory body composed of the Digital Services Coordinators (DSCs). Its mandate is to assist both the DSCs and the European Commission in ensuring the consistent enforcement of the DSA and in promoting effective cooperation among national and EU authorities. The Board contributes to the supervision of very large online platforms, helps coordinate the preparation of guidelines, and provides analyses on standards and emerging challenges (Articles 61 and 63). Pursuant to Article

62, it is composed of the national DSCs and chaired by the Commission, which participates without voting rights.

Court of Justice of the European Union

Pursuant to Article 261 of the Treaty on the Functioning of the European Union, the Court of Justice of the European Union has unlimited jurisdiction to review decisions by which the European Commission imposes fines or periodic penalty payments. Under Article 81 of the DSA, the Court has the power to annul, reduce, or increase the amount of fines or periodic penalty payments.

Digital Services Coordinators

Articles 49 to 51 define the functions, responsibilities, and powers of the Digital Services Coordinators (DSCs). These national authorities are responsible for supervising, enforcing, and monitoring compliance with the DSA within their respective Member States. Their tasks include managing enforcement at national level while ensuring coordination for the consistent application of the DSA across the European Union. DSCs cooperate closely with one another, with other national competent authorities, the European Board for Digital Services, and the European Commission. They have powers to access relevant data, conduct inspections, and impose penalties on intermediary service providers under their jurisdiction in cases of non-compliance. Furthermore, DSCs are responsible for certifying "trusted flaggers" and supervising mechanisms for out-of-court dispute settlement.

The term "Digital Services Coordinator of establishment" refers to the DSC of the Member State in which an intermediary service provider has its main establishment or its legal representative. In contrast, the "Digital Services Coordinator of destination" designates the DSC of the Member State in which the intermediary service is offered (Article 3).

Certified out-of-court dispute settlement bodies

Established under Article 21, independent entities accredited by national Digital Services Coordinators handle disputes arising from decisions taken by online platform service providers.

Trusted flaggers

Under Article 22, independent bodies designated by Digital Services Coordinators as trusted flaggers are recognised for their expertise and ability to detect, identify, and report illegal content. The notices they submit must be treated with priority, as they are presumed to be more accurate and reliable than those submitted by regular users. Trusted flaggers are also required to publish clear and detailed annual reports on the notices they have submitted.

Vetted researchers

Independent experts authorised under Article 40 to access platform data for the purpose of analysing systemic risks, content moderation, and platform operations are referred to as vetted researchers. They must meet strict criteria to guarantee their independence and compliance with data protection requirements. Accredited by the European Commission in cooperation with national Digital Services Coordinators, vetted researchers are granted access to anonymised and aggregated data from Very Large Online Platforms and Search Engines (VLOPs and VLOSEs).

Independent auditors

Under Article 37, entities tasked with assessing the compliance of VLOPs and VLOSEs with the DSA's requirements must conduct such audits at least annually. The use of standardised audit methodologies and implementation reporting templates ensures consistency and comparability across assessments. VLOPs and VLOSEs are required to facilitate the audit process by granting access to relevant data and premises, cooperating fully, and responding to all inquiries without compromising the auditor's independence.

Points of contact, legal representatives, compliance officers

Intermediary service providers must designate two separate points of contact to facilitate communication. The first point of contact, as outlined in Article 11, serves as the formal liaison between providers and national authorities, the European Commission, and the European Board for Digital Services. This ensures efficient and institutionalised interaction, addressing

challenges related to inaccessibility or evasion by providers. The second point of contact, established under Article 12, enables direct, user-friendly, and timely communication between service recipients and providers, thereby promoting accessibility and responsiveness.

Providers offering services within the European Union without a physical establishment in its territory must appoint a legal representative in one of the Member States where their services are available (Article 13). This representative acts on behalf of the provider in matters relating to compliance and legal accountability.

Furthermore, VLOPs and VLOSEs are required, under Article 41, to appoint a compliance officer responsible for overseeing adherence to the DSA. This officer monitors risks and potential instances of non-compliance, ensures the implementation of mitigation measures, and cooperates with the Digital Services Coordinator of establishment, and the European Commission.

INSTITUTIONAL STRUCTURE UNDER THE DMA

European Commission

Under the Digital Markets Act (DMA), the European Commission serves as a comprehensive oversight authority. The DMA establishes a "one-stop shop" enforcement model, granting the Commission exclusive competence to designate gatekeepers, adopt non-compliance decisions, impose interim measures against gatekeepers, and levy fines.

In practical terms, only the European Commission may designate an undertaking as a gatekeeper, either on the basis of quantitative thresholds or following a qualitative assessment conducted on a case-by-case basis (Article 17). The Commission is also empowered to adopt implementing acts specifying the methodology for calculating these thresholds (Article 3(6)). Once the thresholds are met, gatekeepers are required to notify the Commission, which then assesses the notification and adopts a formal designation decision.

Following the designation of a gatekeeper, the Commission monitors compliance with the core obligations set out in Articles 5 to 7 of the

DMA. Designated gatekeepers must submit detailed compliance reports to the Commission at least once a year, outlining the specific measures implemented to meet their obligations (Article 11). The Commission also receives and reviews audited descriptions of any profiling activities carried out by gatekeepers (Article 15). In addition, it conducts a regulatory dialogue with gatekeepers, enabling them to seek guidance on the practical application of their obligations. This dialogue, which may be initiated by a gatekeeper, can take an informal shape or lead to formal decisions specifying how compliance obligations are to be fulfilled (Article 8).

Where a gatekeeper fails to comply with its obligations, the European Commission may initiate enforcement proceedings. It possesses extensive investigative powers, including the ability to request documents, conduct interviews, and carry out on-site inspections, including unannounced dawn raids (Chapter V). These powers are comparable to those conferred on the Commission under the EU competition rules.

The Commission may adopt interim measures where there is a risk of serious and irreparable damage to competition (Article 24). When non-compliance is confirmed, it adopts a formal decision and may impose fines (Article 30). The Commission may also impose periodic penalty payments to compel compliance (Article 31). In cases of systematic non-compliance, it is empowered to launch a market investigation which may lead to the imposition of behavioural or structural remedies, including the possibile divestiture of parts of a business. Such remedies are subject to procedural safeguards, including the publication summaries, stakeholder consultation, and the opportunity for third parties to submit comments (Article 18).

Market investigations also enable the European Commission to identify digital services that may fall within the scope of the DMA but are not initially covered gatekeeper designations (Article 19).

Finally, the Commission holds wide-ranging powers to adopt secondary legislation regulating in greater detail specific aspects of the DMA's implementation, such as delegated acts under Article 12 and implementing acts under Article 48.

Through these extensive powers, the European Commission acts not only as an enforcer but also as a regulatory legislator. It interprets key definitions, provides implementation guidance, supervises compliance, and enforces penalties for non-compliance. This degree of centralisation reflects the EU's

objective of ensuring consistent enforcement and preventing regulatory fragmentation across Member States. The DMA therefore marks a clear shift towards supranational oversight of large digital platforms, with the Commission positioned as the pivotal authority within this framework.[17]

High-level group for the Digital Markets Act

Appointed by the European Commission, the high-level group for the Digital Markets Act comprises representatives nominated by the following EU bodies and networks:

- the Body of the European Regulators for Electronic Communications;
- the European Data Protection Supervisor and the European Data Protection Board;
- the European Competition Network;
- the Consumer Protection Cooperation Network; and
- the European Regulatory Group of Audiovisual Media Regulators.

Secretariat services for the high-level group are provided by the Commission, which also chairs it.

The high-level group advises the European Commission on the implementation and enforcement of the DMA, ensuring coherence across related regulatory instruments. It assesses the interaction between the DMA and sector-specific rules applied by national authorities and submits an annual report containing its findings and recommendations to the Commission. This report is also shared with the European Parliament and the Council. In addition, the group supports the Commission in market investigations by providing expertise on potential regulatory adjustments

17 Zanaki, Anna, and Julian Nowag. "The Institutional Framework of the DMA: A Novel but Thoughtful Experiment in Regulatory Design?" Journal of European Competition Law & Practice, forthcoming. SSRN Working Paper, posted 18 September 2023. Accessed 24 June 2025. papers.ssrn.com/sol3/papers.cfm?abstract_id=4574518

needed to preserve fair and contestable digital markets within the European Union.

The Digital Markets Advisory Committee

Established under the DMA, the Digital Markets Advisory Committee is composed of representatives from each EU Member State. It functions as a committee within the meaning of Regulation (EU) No 182/2011, which sets out the procedures governing committees assisting the Commission in the exercise of its implementing powers. According to the DMA's recitals, these delegations may include experts from the competent authorities of the Member States who possess the necessary expertise to address the specific issues submitted to the committee.

The Digital Markets Advisory Committee assists the European Commission in the implementation and enforcement of the DMA. Its primary function is to provide opinions and advice to the Commission on key matters related to the regulation's enforcement, thereby helping to ensure its consistent application across the EU. For example, the Advisory Committee is involved in the adoption of Commission decisions specifying the measures that a gatekeeper must implement under the procedure laid down in Article 8, or the suspension of such measures under Article 9. It also provides input on decisions concerning the designation of new gatekeepers under Article 17 and on the launch of market investigations into systematic non-compliance under Article 18.

European Data Protection Board and European Data Protection Supervisor

The European Data Protection Board (EDPB) is composed of the heads of the national supervisory authorities of each Member State and of the European Data Protection Supervisor (EDPS), or their respective representatives. EDPS serves as the European Union's independent data protection authority.

Under the DMA, gatekeepers are required to submit to the European Commission an independently audited description of any consumer profiling techniques they employ. The Commission must transmit this audited description to the EDPB. When preparing implementing acts – such as methodologies and procedures relating to these audited descriptions – the

Commission is obliged to consult the EDPS when drafting implementing acts i.e. methodologies and procedures for the respective audited description, and may also consult the EDPB.

National competition authorities

The composition of national competition authorities varies across Member States, depending on their respective legal frameworks.

Although these authorities do not possess direct enforcement powers under the DMA, they play a complementary role by conducting complementary investigations under national competition law and by cooperating with the Commission to ensure the coherent application of the regulation. National authorities are required to inform the Commission of any planned investigations or measures concerning gatekeepers, thereby facilitating coordination and avoiding overlap. The Commission may also consult national competition authorities on matters related to the implementation of the DMA, promoting a unified approach to enforcement across the European Union.

Other national authorities

Under the DMA, certain national authorities – such as consumer protection, regulatory and data protection authorities, as well as national courts – are required, in specific circumstances, to cooperate with the European Commission, thereby safeguarding the harmonised application and enforcement of the DMA.

INSTITUTIONAL STRUCTURE UNDER THE AIA

The enforcement framework of the Artificial Intelligence Act (AIA) is complex, as it seeks to regulate a broad spectrum of AI systems presenting different levels of risk across all sectors of the economy, from healthcare and law enforcement to education and transport. This diversity necessitates the involvement of multiple specialised authorities, each possessing expertise in distinct areas of AI governance.

At EU level, the AIA establishes two key institutional components: the AI Office, set up within the European Commission as an integral part

with specific structure and tasks, and the European AI Board, composed of representatives from the Member States. At national level, the AI Act requires Member States to designate national competent authorities - including at least one notifying authority and one market surveillance authority - alongside authorities responsible for fundamental rights, such as data protection or equality bodies. This multi-layered governance framework ensures that AI systems are not only technically compliant but also ethically sound and respectful of fundamental rights. It also enables the EU to maintain a consistent regulatory approach across Member States while accommodating their distinct legal and institutional frameworks.

European AI Office

Established within the European Commission in February 2024, this office is responsible for overseeing the implementation and enforcement of the AIA across all Member States. It supervises general-purpose AI models and works closely with national competent authorities to ensure the consistent application of the regulation. The AI Office is staffed with experts in AI and digital technologies and is organised to reflect its wide-ranging competences in AI governance and enforcement.

Under Article 64, the AI Office is tasked with strengthening the EU's expertise and capacity in the field of artificial intelligence. It fulfils this role by providing technical, legal, and regulatory guidance to stakeholders involved in the development, deployment, and use of AI systems. This office also ensures that best practices, technical standards, and regulatory knowledge are consistently updated and made accessible to all relevant actors.

Within the enforcement framework of the Artificial Intelligence Act, one of the European AI Office's key responsibilities is "supervision, investigation, enforcement, and monitoring in respect of providers of general-purpose AI models" (title of Section 5 of Chapter IX). It fulfils this mandate by taking the necessary measures to ensure that such models are developed and used responsibly and in accordance with the AIA. This includes monitoring the effective implementation and compliance with the AI Act, assessing alerts on systemic risks notified by the scientific panel, requesting providers to make available relevant documentation and information, and conducting evaluations of systemic risks and providers' compliance. The Office may also handle complaints concerning non-compliance and take corrective actions where necessary, thereby providing an additional layer of accountability. For

general-purpose AI models, enforcement is therefore centralised at EU level, with the European Commission – through the AI Office – empowered to impose administrative fines for non-compliance.

The European AI Office also plays a key role in facilitating the development of two complementary instruments under the AI Act. Codes of practice provide best-practice guidance specific to general-purpose AI models. They are developed with the participation of relevant stakeholders, coordinated by the AI Office, which also monitors adherence to these codes (Article 56). Codes of conduct are voluntary guidelines for non-high-risk AI systems and are intended to help developers and deployers align with ethical and data-protection principles and other recognised best practices (Article 95).

Finally, the AI Office provides secretariat support to the European AI Board. It organises the Board's meetings, facilitates communication among national competent authorities, and supports the development of coherent regulatory practices across the Union (Article 66).

European AI Board

Established under Article 65 of the Artificial Intelligence Act, the AI Board is responsible for ensuring the consistent application of AI regulations across all Member States. It is composed of representatives from each Member State and includes the European Data Protection Supervisor as an observer. Representatives of the European AI Office may also attend the Board's meeting without voting rights. In addition, the Board may invite representatives of other national or EU authorities, bodies or experts to participate in its meetings by the AI Board where relevant to the matters under discussion.

Competences of the Board are set out primarily in Article 66 of the AI Act and include advisory, coordination, and support functions.

In its advisory capacity, the AI Board is tasked with assisting the European Commission and the Member States in ensuring the consistent and effective implementation of the AI Act. This includes providing opinions, recommendations, and guidance on a broad range of issues related to AI governance, such as technical standards, ethical practices, and compliance measures. The AI Board may also issue opinions on complex legal and technical questions concerning AI systems, thereby contributing to

a uniform interpretation and application of the regulation across the European Union.

As a coordinating body, the Board brings together national authorities responsible for monitoring and enforcing the AI Act across the Member States. It facilitates exchange of information, promotes best practices, and supports the consistent interpretation of the regulation. The Board may also organise joint activities, such as coordinated inspections, investigations, and enforcement actions, to address cross-border issues arising from the development or use of AI systems.

The AI Board supports national authorities in developing joint methodologies, conducting joint training sessions, and exchanging expertise on emerging AI risks and technologies. This cooperation helps ensure that national authorities can enforce the regulation effectively and consistently, regardless of their individual capacities or expertise. The Board also participates as a stakeholder in the preparation of codes of practice for general-purpose AI models (Article 56).

Advisory Forum

To ensure a multi-stakeholder approach, Article 67 of the AI Act provides for the establishment of an advisory forum composed of "a balanced selection of stakeholders, including industry, start-ups, SMEs, civil society and academia", appointed by the European Commission. The Commission selects members drawn from stakeholders with recognised expertise in the field of artificial intelligence. In addition, several key EU bodies and agencies – such as the Fundamental Rights Agency and the European Union Agency for Cybersecurity –- ENISA – have permanent representation in the Forum.

The principal task of the Advisory Forum is to advise and provide technical expertise to the European AI Board and the European Commission in support of their respective functions under the AI Act. The Forum may also prepare opinions, recommendations, and written contributions at the request of either the Board or the Commission. The AIA specifies one instance in which consultation of the Forum by the Commission is mandatory – when the Commission decides to draft common specifications for the requirements applicable to high-risk AI systems and to providers of general-purpose AI models.

Scientific Panel of Independent Experts

While the Advisory Forum is established to secure stakeholder input in the implementation of the AI Act, the Scientific Panel of Independent Experts ensures the structured involvement of the scientific community. It is established through an implementing act adopted by the European Commission, which also determines the number of experts to serve on the Panel, taking into account the need for gender and geographical balance. According to the AI Act, members are selected on the basis of up-to-date scientific or technical expertise in the field of artificial intelligence required for the performance of their tasks.

Article 68 of the AI Act provides that the Scientific Panel shall advise and support the European AI Office, particularly with regard to tasks such as assisting in the implementation and enforcement of the regulation in relation to general-purpose AI models and systems, supporting market surveillance authorities upon request, contributing to cross-border market surveillance activities, and assisting the AI Office in fulfilling its duties under the Union safeguard procedures. Article 69 further allows Member States to access the pool of experts to support their own enforcement activities. In addition, the Scientific Panel may alert the AI Office to potential systemic risks posed by general-purpose AI systems, in accordance with Article 90.

National Competent Authorities

Article 70 of the AI Act requires each Member State to designate at least one notifying authority and one market surveillance authority, with the designation deadline set for 2 August 2025. These bodies are collectively referred to, under the definitions of the AIA, as the national competent authorities.

According to Recital 153 of the Artificial Intelligence Act, Member States retain the flexibility to designate any type of public entity to perform the functions of the national competent authorities under the AI Act – namely, the notifying authority and the market surveillance authority. This approach allows Member States to align these designations with their respective administrative structures and regulatory frameworks.[18]

18 Non-official list of national competent authorities. Artificial Intelligence Act – National Implementation Plans. Accessed October 2025. https://artificialintelligenceact.eu/national-implementation-plans

National Competent Authorities – Market Surveillance Authorities

Each Member State is expected to designate one market surveillance authority to act as a single point of contact, enhancing organisational efficiency and ensuring a clear channel of communication for the public as well as for other national and Union counterparts.

The tasks of market surveillance authorities include providing guidance to AI providers, monitoring compliance, and enforcing regulatory requirements, particularly in relation to high-risk AI systems. They also serve as single points of contact for stakeholders and cooperate with other national and Union bodies to maintain a coherent and coordinated approach across the European Union.

Market surveillance authorities have a broad and diverse set of responsibilities under the Artificial Intelligence Act. Pursuant to Article 73, providers of high-risk AI systems must report serious incidents to the authority in the Member State where the incident occurred. Under Article 74, market surveillance authorities, in exceptional circumstances, access documentation relating to high-risk AI systems – including training and testing data, or source code. Where access to information on general-purpose AI models is required for an investigation and cannot be obtained directly, authorities may request such access through the European AI Office (Article 75(3)). Market surveillance authorities are also responsible for ensuring that real-world testing of AI systems complies with the requirements of the AI Act (Article 76).

Further key functions include managing AI systems that present risks at national level (Article 79), addressing cases where AI systems have been incorrectly classified as non-high-risk (Article 80), and ordering corrective actions where a compliant high-risk AI system nonetheless poses risks to health, safety, fundamental rights, or the public interest (Article 82). In addition, market surveillance authorities act as complaint bodies for suspected infringements of the AI Act (Article 85).

Market surveillance authorities are responsible for receiving and handling complaints submitted by natural or legal persons who consider that their rights under the AI Act have been infringed (Article 85). They are also empowered to impose fines for non-compliance with the AI Act, complementing their enforcement powers under other relevant regulatory

frameworks, such as Regulation (EU) 2019/1020 on market surveillance and the compliance of products.

National Competent Authorities – Notifying Authorities

Notifying authorities are responsible for overseeing the assessment, designation, notification, and monitoring of conformity assessment bodies (also referred to as notified bodies) that evaluate high-risk AI systems. Although Member States retain discretion to designate any authority as the notifying authority, such bodies must operate independently and avoid any conflicts of interest with the conformity assessment bodies they supervise. Their activities must therefore be carried out objectively and impartially.

In the pre-implementation phase of AI systems, notifying authorities play a significant role. According to the definitions set out in the AI Act, they are responsible for overseeing the procedures for assessing, designating, and monitoring conformity assessment bodies in accordance with Articles 28-39. These bodies are tasked with evaluating high-risk AI systems before they are placed on the market or put into service.

They ensure that conformity assessment bodies meet the necessary requirements of competence, impartiality, and independence before being authorised to carry out assessments. Notifying authorities also maintain continuous oversight of these bodies to verify their ongoing compliance with the standards set out in the AI Act. They may suspend or withdraw a designation if a conformity assessment body no longer fulfils the required conditions.

Conformity Assessment Bodies – Notified Bodies

According to Article 31 of the AI Act, notified bodies must be established under the national law of a Member State and possess legal personality. These bodies are required to meet strict criteria set out in the AI Act:

- Organisational requirements include an appropriate internal structure, quality management systems, and sufficient resources to perform their tasks effectively.
- Independence and impartiality requirements stipulate that notified bodies must be independent of AI system providers

> and any other parties with an economic interest in the systems they assess. A conformity assessment body, its management, and its personnel must not participate in the design, development, marketing, or use of high-risk AI systems, nor represent any of the parties involved. They must refrain from any activities that could compromise their independence or integrity, particularly the provision of consultancy services.

Conformity assessment bodies are defined in the AI Act as legal entities performing third-party assessments – testing, certification, and inspection – of high-risk AI systems under Chapter III, Section 2. To obtain the status of notified bodies, these entities must apply to their national notifying authority (Article 29). Bodies established in third countries may also be notified where relevant agreements exist, provided that they ensure equivalent compliance with the requirements of the AIA (Article 39).

National Authorities Protecting Fundamental Rights

Each Member State designates one or more public bodies to oversee and ensure compliance with fundamental rights obligations in relation to high-risk AI systems. Such authorities may include data protection agencies, equality bodies, national human rights institutions, or other entities responsible for safeguarding rights such as non-discrimination, privacy, and freedom of expression.

Article 77 of the AIA empowers these bodies to access documentation related to high-risk AI systems in order to fulfill their mandates. They must inform the relevant market surveillance authority of any such requests. Where the available documentation is insufficient, they may request the market surveillance authority to carry out technical testing of the AI system. Under the national procedure for addressing AI systems that present a risk, these authorities may also intervene alongside the market surveillance authority where a system poses a threat to fundamental rights (Article 79).

National Data Protection Supervisory Authorities

The role of national data protection supervisory authorities under the Artificial Intelligence Act is not explicitly regulated and depends on national law. However, given their existing responsibilities under the General Data Protection Regulation (GDPR) and the Law Enforcement Directive,

national data protection authorities (DPAs) are integrated into the AI Act's institutional framework, particularly with regard to the impact of AI on personal data processing. For high-risk AI systems listed in Annex III – such as those used for biometric identification, law enforcement, border management, administration of justice, and democratic processes – Member States must designate DPAs as market surveillance authorities. In addition, national DPAs may act as notified bodies for conformity assessments when AI systems are deployed by law enforcement, immigration, or asylum authorities (Articles 43(1) and 74(8)).

INSTITUTIONAL STRUCTURE FOR DIGITAL GOVERNANCE IN CROATIA

Croatia's digital governance framework assigns the enforcement of EU digital legislation to sector-specific regulatory authorities. The Croatian Personal Data Protection Agency (Agencija za zaštitu osobnih podataka, AZOP) acts as the national supervisory authority for the General Data Protection Regulation (GDPR). The Croatian Regulatory Authority for Network Industries (Hrvatska regulatorna agencija za mrežne djelatnosti, HAKOM) has been designated as the Digital Services Coordinator under the DSA, while the Croatian Competition Agency (Agencija za zaštitu tržišnog natjecanja, AZTN) serves as the national authority under the DMA.

It still remains unclear which institutions will be designated as the market surveillance authority and the notifying authority under the AI Act, despite the expiry of the implementation deadline. Although AZOP is currently the only regulatory body with institutional expertise and experience in safeguarding fundamental rights against the adverse impacts of digital technologies, non-official information indicates that Croatia is considering a decentralised model, in which AZOP would serve as only one of several market surveillance authorities. Such a fragmented approach risks weakening enforcement capacity and diluting institutional accountability.

INSTITUTIONAL STRUCTURE FOR DIGITAL SERVICES IN CROATIA

The Law implementing the Digital Services Act establishes a diffuse institutional framework that is likely to create challenges for effective enforcement. The total number of competent national authorities remains unclear due to a broad blanket provision in the law, which enables additional public bodies – beyond those explicitly listed – to issue content-removal and information orders.

Article 6(1) of the Law lists seven public bodies authorised to issue orders under Article 9 and 10 of the Digital Services Act – relating to the removal of illegal content and the provision of information. These are:

- State Attorney's Office and the Ministry of the Interior – for content constituting a criminal offence or misdemeanor;
- Agency for Personal Data Protection (AZOP) – for violations of data protection law;
- Customs Administration – for breaches of intellectual property rights;
- State Inspectorate – for violations of inspection-related regulations;
- Ministry of Health – for health-related content violations; and
- Agency for Electronic Media – for breaches of electronic media regulation.

In addition to the authorities explicitly listed, point 7 of Article 6(1) of the national law also authorises "other public bodies, in line with their competences defined by a special law regulating their scope of work". This general clause effectively extends enforcement powers to a potentially broad range of entities. For example, it enables the State Electoral Commission to issue orders concerning illegal content that constitutes a breach of electoral regulations.

A similar blanket provision appears in Article 8 of the national law, designating the same group of authorities as responsible for a broader range of obligations under the Digital Services Act. These include oversight of transparency in advertising, online interface design, trader traceability, and compliance by design (DSA Articles 25-26 and 30-32).

However, the law does not specify which authority is responsible for each obligation, nor does it define how coordination among them will operate in practice. This lack of clarity significantly undermines the enforceability of these provisions at the national level. By contrast, AZOP is explicitly designated as the competent national authority for transparency of recommender systems and online protection of minors (DSA Articles 27 and 28).

The tasks and duties of HAKOM, as Croatia's Digital Services Coordinator, are briefly outlined in Article 4(2) of the national law and primarily consist of cross-references to the provisions of the DSA:

- coordinating all bodies responsible for enforcing the Act and serving as the national contact point for other DSCs (Article 49);
- acting as the competent authority under Articles 51 and 53;
- preparing the annual report referred to in Article 55;
- engaging in cross-border cooperation with other DSCs under Article 58;
- participating in joint investigations with DSCs from other Member States under Article 60;
- taking part, with voting rights, in the work of the European Board for Digital Services pursuant to Articles 62 and 63;
- exercising competences in relation to out-of-court dispute settlement (Article 21); and
- exercising competences regarding the designation of trusted flaggers (Article 22).

All public bodies responsible for enforcing the DSA must submit an annual report on their activities, including the number of orders issued under Articles 9 and 10. The Digital Services Coordinator compiles these inputs and submits a consolidated annual report to the European Commission and the European Board for Digital Services. Bodies certified for out-of-court dispute resolution under Article 21 and trusted flaggers designated under Article 22 are likewise required to provide annual reports to the DSC. In addition, the DSC may request interim reports where necessary to facilitate cooperation with other national or EU bodies.

Given that the removal of online content is frequently portrayed in public discourse as a form of political censorship, the inclusion of two ministries (the Ministry of the Interior and the Ministry of Health) among the authorities empowered to issue removal orders may heighten reputational and political risks. Any enforcement actions taken by these ministries against illegal online content are therefore likely to be perceived as politically motivated interventions or as attempts to capture the DSA enforcement framework.

INSTITUTIONAL STRUCTURE FOR DIGITAL MARKET IN CROATIA

In line with the Digital Markets Act (DMA), the European Commission retains the central role in enforcement, while national authorities perform only a limited supporting function. This allocation of competences is reflected in Croatia's comparatively modest national implementation framework.

The Government Ordinance implementing the DMA contains only one substantive article outlining the tasks of the designated national authority – the Croatian Competition Agency (Agencija za zaštitu tržišnog natjecanja, AZTN). These tasks include:

- informing the European Commission in writing of any intention to initiate proceedings against a gatekeeper concerning competition protection;
- notifying the Commission of its enforcement measures, including all factual, legal, and confidential information, via the European Competition Network;
- prior to imposing obligations on gatekeepers in relation to competition protection, submitting a draft of the proposed obligations with an accompanying explanation to the Commission; and
- in cases where interim measures are adopted in the field of competition protection, submitting the draft measures to the Commission as soon as possible or immediately after their adoption.

The listed tasks apply only in situations where the national authority takes proactive action or adopts measures against gatekeepers designated under the DMA. However, it appears highly unlikely that AZTN will undertake such activities on its own initiative in the near future. A formal inquiry with the agency confirmed that no DMA-related actions or investigations were initiated in 2024 or 2025. This is consistent with the AZTN's 2024 Annual Report, which contains no reference to gatekeeper oversight.

INSTITUTIONAL STRUCTURE FOR AI IN CROATIA

Croatia has not yet designated its market surveillance authority or notifying authority under the Artificial Intelligence Act. It also remains uncertain whether this will be achieved through the adoption of a dedicated national implementation law or by directly notifying the European Commission, as was the case with the designation of the Digital Services Coordinator and the identification of authorities responsible for protecting fundamental rights under Article 77 of the AI Act.

A total of seven independent institutions and regulatory agencies have been designated as authorities responsible for protecting fundamental rights in relation to high-risk AI systems. These include the Ombudsperson, the Ombudspersons for Children, the Ombudsperson for Gender Equality, the Ombudsperson for Persons with Disabilities, the Croatian Data Protection Agency (AZOP), the State Electoral Commission, and the Agency for Electronic Media.

The key provisions of the AI Act concerning high-risk AI systems will enter into force on 2 August 2026. Delayed national implementation will significantly shorten the preparation period available to competent national authorities ahead of this critical phase. This risk is likely to be further exacerbated if Croatia opts for a decentralised model with multiple market surveillance authorities, as such an approach could complicate coordination and undermine institutional readiness.

The absence of a designated market surveillance authority creates a substantial risk of non-compliance with provisions of the AI Act that have already entered into force – namely, the AI literacy obligation (effective from February 2025) and the obligations relating to general-purpose AI models (effective from August 2025).

The continued non-designation of a market surveillance authority is not expected to have an immediate impact on the development or deployment of AI systems in Croatia. Public institutions are expected to use the period until August 2, 2026 to prepare for the assumption of enforcement tasks related to high-risk systems. However, this interim phase may enable certain private sector developers and deployers to exploit regulatory gaps and avoid compliance, as high-risk AI systems placed on the market or put into use

before that date are not subject to the Act, unless they undergo substantial modifications.

While it remains unclear how many and which public bodies will be designated as market surveillance authorities, AZOP is expected to assume this role for high-risk AI systems related to biometrics, law enforcement, border management, justice, and democracy, as provided in Article 74 of the AI Act.

INSTITUTIONAL STRUCTURE FOR DIGITAL GOVERNANCE IN SERBIA

In relation to the institutional framework for digital governance and its alignment with EU standards, Serbia currently maintains only a set of institutions that are expected to assume specific regulatory roles once full harmonisation with the relevant EU legislation is achieved. This section therefore focuses on the institutions identified as prospective central national institutions under the DSA, DMA, and AIA.

INSTITUTIONAL STRUCTURE FOR DIGITAL SERVICES IN SERBIA

Serbia has two regulatory bodies responsible for market conditions, consumer interests, and electronic media services: the Regulatory Authority for Electronic Communications and Postal Services (*Republička agencija za elektronske komunikacije i poštanske usluge,* RATEL) and the Regulatory Body for Electronic Media (*Regulatorno telo za elektronske medije*, REM). Both are envisaged as independent national bodies tasked with safeguarding market competition and consumer rights, as well as promoting diversity and quality in media services and content. However, these institutions were established under an earlier generation of regulation and operate within mandates that do not encompass systemic oversight or structured mechanisms for inter-agency coordination, both of which are essential for effective implementation of the DSA.

RATEL was established in 2005 under the Law on Telecommunications as a national agency for telecommunications. Its initial mandate focused on implementing policies related to the national telecommunications agenda. Following the 2014 amendments to the Law on Electronic Communications, the agency merged with the national Agency for Postal Services, assuming its current form. Since then, RATEL's mandate has expanded to cover the broader field of electronic communications, including cooperation with competent regulatory and expert bodies from EU Member States to harmonise regulatory practices and support the development of cross-border electronic communication networks and services.

According to 2025 data, RATEL employs around 400 staff[19] and is structured around a Council and a Director, who jointly oversee six departments: Electronic Communications, Legal Affairs, Market Analysis and Economic Affairs, Postal Services, Cybersecurity and IT, and General Affairs.[20] The Director and members of the Council are appointed by the National Assembly for a five-year term, renewable once.

REM, formerly the national Broadcasting Agency, was established in 2003 under the Law on Broadcasting with the primary purpose of implementing national broadcasting policy. In 2014, the agency adopted its current name and expanded its mandate to include electronic media – covering online media portals and other audiovisual media services, including content distributed via video-sharing platforms. REM is responsible for granting broadcasting licences to media providers and for safeguarding the principles of freedom of expression and the public interest. It also has the authority to issue executive decisions, including measures against violations such as the promotion of hate speech, and to revoke licenses where appropriate. The agency's monitoring team oversees all registered media entities and tracks compliance with obligations set out in the Law on Electronic Media.

REM has the authority to impose a range of measures, from reprimands and warnings to the temporary or permanent revocation of licences in cases of serious violations. Decisions of the REM Council are final and not subject to appeal. All decisions are entered into the Register of Media Services, a public database of media service providers containing information on ownership structure, licence number, contact details, provider type, and licence validity.[21]

The regulator comprises a Council and a Director, supported by four technical departments: Monitoring and Analysis, Legal, General Affairs,

19 RATEL. "Podaci o broju zaposlenih i radno angažovanih lica" ["Information on the Number of Employees and Contracted Personnel"]. 29 June 2025. Accessed October 2025 https://www.ratel.rs/storage/upload/2025/07/Podaci-o-broju-zaposlenih-i-radno-angazovanih-lica-29_06_2025.pdf

20 RATEL. Overview of the Organizational Structure. Accessed October 2025.https://www.ratel.rs/en/organizational-structure

21 REM. Media Service Providers Register. Accessed October 2025. https://rem.rs/en/media-service-providers-register?q%5Bs%5D=tip_id+asc

and Finance.[22] REM's Council consists of nine members appointed by the National Assembly for a five-year term, renewable once. Council members are expected to be respected experts in fields such as media production, media studies, journalism, law, or other professions relevant to the agency's mandate.

INSTITUTIONAL STRUCTURE FOR DIGITAL MARKET IN SERBIA

Although Serbia does not yet have legislation equivalent to the DMA, its broader competition framework is closely aligned with EU law. In accordance with Article 73 of the Stabilisation and Association Agreement between the European Union and the Republic of Serbia, the country is committed to progressively harmonising its national competition rules with EU standards.

To support these objectives, the Commission for Protection of Competition was established in 2005 as an independent institution under the Law on Protection of Competition – Serbia's first modern legal framework addressing antitrust matters. The Commission is constituted as a legal entity with the status of an independent and autonomous organisation. It reports annually to the National Assembly on its activities and performance. Its structure, competence, and procedures are further defined by national legislation and by government regulations related to competition policy.

When adopting its decisions, the Commission for Protection of Competition takes into account not only Serbia's domestic legislation but also the relevant provisions of the EU acquis.

With regard to other legislation relevant from the perspective of the DMA, a key instrument is the Law on Electronic Commerce, which is aligned with the EU E-Commerce Directive. The competent authorities for its implementation and for the inspection of violations are government bodies – specifically, the ministry in charge of trade and services and the ministry in charge of electronic communications and the information society.

22 REM. Organizational Chart of the Regulatory Authority for Elecronic Media Accessed October 2025. https://www.rem.rs/uploads/files/PDF/Graficki%20prikaz%20organizacione%20strukture%2001.03.2024%20-%20e.pdf

INSTITUTIONAL STRUCTURE FOR AI IN SERBIA

On 3 June 2024, the first meeting of the Working Group for Drafting the Artificial Intelligence Law of the Republic of Serbia was held. However, as of the date of this study, no official draft of the law has been published. Consequently, there are currently no binding legal provisions regulating AI systems, models, or their use nor any designated bodies responsible for their implementation or oversight. The Ethical Guidelines for the Development, Implementation, and Use of Reliable and Responsible Artificial Intelligence, adopted by the Government of Serbia in February 2023, remain non-binding and contain no enforcement or sanctioning mechanisms.

Since July 2024, Serbia has had a Council for Artificial Intelligence, a strategic advisory body established by the Government of Serbia to coordinate and oversee national efforts in the development and governance of artificial intelligence. The Council does not hold regulatory authority but serves an advisory role in shaping legislative frameworks, aligning Serbia's AI initiatives with international standards, and facilitating cooperation among relevant stakeholders.

The Institute for Artificial Intelligence Research and Development of Serbia (AI Institute) was established by the Government in March 2021. Although it has no legislative or enforcement powers, the AI Institute serves as an important expert body within the national AI ecosystem. It brings together scientists, researchers, and industry experts from Serbia and abroad to conduct research and promote the application of artificial intelligence across various sectors.

With its extensive experience in Serbia's digital transformation projects, another key institution is the Office for IT and eGovernment (ITE Office). This central governmental body is responsible for developing and implementing the country's digital infrastructure and eGovernment services. Given its experience in designing, harmonising, and maintaining government information systems, as well as in developing and applying IT standards for public services, the ITE Office is well positioned to play an important role in supporting the development and use of artificial intelligence in Serbia.

INSTITUTIONAL STRUCTURE FOR DIGITAL GOVERNANCE IN MONTENEGRO

As in the case of Serbia it is currently possible to speak only of institutions in Montenegro that are expected to assume responsibilities for the implementation of harmonised digital governance in the future. These bodies already perform certain functions and have an institutional legacy in areas that are, to varying degrees, related to digital services, the digital market, and artificial intelligence.

INSTITUTIONAL STRUCTURE FOR DIGITAL SERVICES IN MONTENEGRO

Although the Agency for Audiovisual Media Services (*Agencija za audiovizuelne medijske usluge, AMU*) currently operates within the audiovisual media sector, its regulatory mandate and responsibility for overseeing video-sharing platforms make it a relevant institutional actor for the future implementation of the DSA in Montenegro.

The AMU is established as an independent regulatory authority for the audiovisual media sector, operating in the public interest. It functions as a legally autonomous entity under the Law on Audiovisual Media Services and maintains both functional and institutional independence from state authorities, administrative bodies, local self-governments, and all private or legal entities engaged in providing audiovisual media services. The Agency's governance is entrusted to its Council.

The Council consists of five members, one of whom serves as its chair. Council members are appointed by the Parliament of Montenegro. In addition to the Council, the Agency is organised into several key operational units: the Director, the Legal and Economic Affairs Sector, the Monitoring Sector, the General and International Affairs Sector, and the ICT Sector.

The Agency has a broad mandate encompassing regulatory, oversight, and promotional functions within the audiovisual media environment. It issues broadcasting and distribution licenses, maintains registries of broadcasters, on-demand audiovisual media providers, and video-sharing platforms, monitors compliance with legal obligations, enforces penalties for non-compliance, and publishes regular reports. In addition, AMU plays a key role in safeguarding media pluralism, protecting consumer

rights, promoting cultural and linguistic diversity, ensuring accessibility for persons with disabilities, and supporting the development of media literacy as well as co- and self-regulatory practices.

Importantly, AMU is also responsible for overseeing media conduct during electoral campaigns, including the monitoring of political advertising and the handling of related complaints. It has the authority to impose sanctions, request the initiation of legal proceedings, and adopt bylaws within its mandate. Its oversight functions also include the publication of regular reports and the conduct of public opinion research on audience trust and media consumption patterns.

The Agency for Electronic Communications and Postal Services (Agencija za elektronske komunikacije i poštansku djelatnost, EKIP) is another authority that may become relevant for the national implementation of the DSA, although its primary responsibilities are technical and market-oriented.

EKIP, established in 2001 by a decision of the Government of Montenegro under the name Agency for Telecommunications, is Montenegro's independent regulatory authority for the electronic communications and postal sectors. As an autonomous institution, EKIP operates independently of state bodies, operators, and other stakeholders, in line with the principles of independence, professionalism, transparency, non-discrimination, and reliability, as stated in its mission statement.

This agency's regulatory mandate is defined by the legal frameworks governing electronic communications and postal services in Montenegro. It supervises and regulates both sectors, manages the radio frequency spectrum, issues licenses and authorisations, and monitors compliance among service providers. The Agency plays a key role in protecting consumer rights, addressing complaints, and ensuring fair market practices. In addition, EKIP adopts bylaws and regulatory guidelines, oversees service quality, and regularly informs the public through market analysis and reports.

Institutionally, EKIP is governed by a Council whose members are appointed by the Parliament of Montenegro. Executive authority rests with the Director, who manages the Agency's operations. EKIP's internal structure is organised into specialised sectors covering electronic communications networks and services, radiocommunications, postal services, economic analysis and market supervision, legal and general affairs, as well as supervision and control.

INSTITUTIONAL STRUCTURE FOR DIGITAL MARKET IN MONTENEGRO

The Agency for Protection of Competition was established as an independent institution following the enactment of the Law on Protection of Competition in 2012 and its formal registration in 2013. Prior to its establishment, competition-related matters were handled by the Ministry of Economy. The law regulates free market competition as a key factor in economic development, investment potential, and product quality, with the overarching objective of fostering a modern market economy. A central aim of the framework is to align Montenegro's competition policy with EU standards, in line with Article 73 of the Stabilisation and Association Agreement and relevant provisions of the EU Treaties.

The Law on Protection of Competition incorporates European principles and seeks to harmonise Montenegrin regulations with those of the EU. The Agency for Protection of Competition operates as a public authority responsible for enforcing competition law, including the review of restrictive agreements, abuses of dominant positions, and mergers. It functions within a detailed framework of laws and bylaws adopted by the Government on the proposal of the Ministry of Economy. Among its core duties, the Agency monitors market conditions, conducts investigations, approves exemptions and mergers, and imposes corrective measures. It also issues opinions on competition matters, drafts legal proposals, and determines administrative fees. Additional responsibilities include initiating legal proceedings, advising on draft regulations affecting competition, forming expert bodies, and cooperating with domestic and international institutions. The Agency publishes statistical data, keeps records of mergers, oversees the implementation of its decisions, and reports to the Government.

INSTITUTIONAL STRUCTURE FOR AI IN MONTENEGRO

In the absence of dedicated AI legislation, the country currently has no institutions responsible for implementing rules related to artificial intelligence. The preparation of the announced national AI strategy falls under the competence of the Ministry of Public Administration.

COMPARATIVE DISCUSSION

From an institutional perspective on the DSA, Croatia, Serbia, and Montenegro represent three distinct stages of alignment with the EU model. Croatia has formally designated the The Croatian Regulatory Authority for Network Industries (HAKOM) as the Digital Services Coordinator and an undetermined number of public bodies authorized to issue orders under the DSA. Serbia continues to rely on the Commission for the Protection of Competition and the Regulatory Authority for Electronic Media, both of which operate under regulatory frameworks predating the DSA. Montenegro remains at a preparatory stage: a working group within the Ministry of Culture and Media is currently exploring options for future harmonisation, while existing regulators such as AMU and EKIP hold only sector-specific competences.

Taken together, these cases reveal a common institutional gap – none has yet established a coherent, fully articulated structure capable of implementing a new oversight model. Among them, however, Croatia stands out as the only country that has begun to conceptualise its national mechanism in relation to the EU's multi-layered governance structure.

COMPARING INSTITUTIONAL STRUCTURES FOR THE DSA

In the field of institutional arrangements for implementing the Digital Services Act (DSA), Croatia, Serbia, and Montenegro demonstrate varying approaches but share similar uncertainties regarding how to operationalise an effective national model. The DSA requires the establishment of Digital Services Coordinators (DSCs) as the central national authority, while the European Commission retains exclusive competence over Very Large Online Platforms and Search Engines (VLOPs and VLOSEs). This framework assigns national bodies primarily a supportive role. They are responsible for domestic enforcement and for maintaining procedural links with EU-level oversight mechanisms. Such a configuration, however, introduces a degree of ambiguity in national settings, particularly in non-EU countries, where the Commission's supervisory functions cannot be directly replicated.

Croatia has already adopted a law designating the The Croatian Regulatory Authority for Network Industries (HAKOM) as the Digital Services Coordinator, thereby fulfilling the EU's core institutional requirement. Yet, the law remains highly concise and defers some crucial functions – such as the accreditation of trusted flaggers and the establishment of out-of-court dispute resolution mechanisms – to future bylaws. This reliance on secondary legislation secures formal compliance but delays the development of a fully operational institutional framework, producing a degree of legal and procedural uncertainty.

Serbia, by contrast, relies on existing institutions, notably the Commission for the Protection of Competition and the Regulatory Authority for Electronic Media, whose competences are defined by earlier legislative frameworks in their respective fields. While these bodies can address certain aspects related to advertising transparency and the protection of minors, they are not formally mandated to serve as Digital Services Coordinators, nor are they integrated into the cooperation structures envisaged by the DSA. Serbia's institutional design remains incomplete and contingent on future legislative and administrative reforms.

Montenegro's current institutional landscape remains fragmented, though it signals a transitional phase. At present, responsibilities lie with the Agency for Audiovisual Media Services (AMU) and the Agency for Electronic Communications and Postal Services (EKIP), both of which operate under sector-specific mandates. Although these bodies could in principle be adapted to assume the role of Digital Services Coordinator, no formal legal designation has yet been made. Legislative harmonisation will therefore need to be accompanied by the establishment of a coherent institutional structure capable of supporting the systemic oversight model envisaged by the DSA.

In comparative perspective, Croatia has established a minimal formal framework by appointing a Digital Services Coordinator, Serbia continues to rely on pre-existing authorities without a dedicated institutional structure, and Montenegro is only beginning to prepare for harmonisation through a government working group. Despite these differences, all three countries share a common structural challenge: their current institutional arrangements remain insufficiently coherent and systemic to fully realise the DSA's model of digital services governance.

COMPARING INSTITUTIONAL STRUCTURES FOR THE DMA

The enforcement of the Digital Markets Act (DMA) is highly centralised at the EU level, with the European Commission holding exclusive competence to designate gatekeepers and impose fines. National authorities, including those in Croatia, perform a supportive role within this framework, which is designed to prevent regulatory fragmentation and ensure consistent enforcement across the Union.

Croatia's approach to the DMA institutional framework aligns with the EU's centralised model. The Croatian Competition Agency (AZTN) has been designated as the competent national authority, but its role is confined to assisting the European Commission in conducting complementary investigations. This minimalist arrangement can be effective for the time being, as it reflects the DMA's enforcement architecture, in which the primary responsibility rests with the Commission.

Both Serbia and Montenegro could, in theory, apply certain DMA-like rules only through their existing, fragmented national systems, as neither country has adopted specific legislation equivalent to the DMA. Instead, they rely on general competition and e-commerce laws that were not designed to regulate digital giants. The competition frameworks in both countries remain generic and do not address the specific challenges associated with gatekeepers or core platform services. Consequently, the applicability of these laws to digital markets remains largely untested.

In addition, neither country has a dedicated national body with the specific mandate, expertise, or legal authority to enforce DMA-like rules. To date, the existing competition agencies in Serbia and Montenegro have only limited experience in dealing with digital markets. This represents a major gap compared to the European Commission's robust and specialised enforcement structure and institutional expertise. From the perspective of DMA-related rules, the broader regulatory landscape in both countries remains fragmented and poorly coordinated, rendering it ineffective for addressing digital challenges of a global scale.

COMPARING INSTITUTIONAL STRUCTURES FOR THE AIA

To ensure both technical compliance and ethical soundness across sectors, the Artificial Intelligence Act establishes a multi-layered institutional framework that combines newly created bodies at the EU level with national authorities responsible for market surveillance and the protection of fundamental rights. Within this system, Croatia is in the process of aligning with the AIA's requirements, albeit with significant delays. The country has already designated several public bodies to safeguard fundamental rights in relation to high-risk AI systems, but it has not yet designated its market surveillance authority or notifying authority. The Croatian Data Protection Agency, with its established expertise in GDPR enforcement, is expected to assume one of the roles. However, its limited human resources and current legal status may pose a serious risk to the effective implementation of the AI Act complex rules. Croatia's experience illustrates that even where legal alignment has been achieved, institutional capacity remains a major challenge for EU Member States.

By contrast, Serbia and Montenegro are still at a very early stage of preparing for AI regulation, with no legislation currently in force. As of August 2025, neither country has adopted a law governing AI systems nor designated the bodies responsible for its implementation. A government AI strategy for Montenegro is expected in 2025 or 2026, while Serbia has established a working group to draft an AI law, reportedly due by the end of 2025, though no public information on this progress has been released.

As with the DSA and DMA, in the absence of a dedicated legal framework, neither Serbia nor Montenegro has established institutions with a specific mandate to enforce AI regulations. Existing bodies such as Serbia's Council for Artificial Intelligence and the AI Institute remain purely advisory, without legislative or enforcement competences. In Montenegro, the Ministry of Public Administration is responsible for strategic planning, but no enforcement or expertise body is currently envisaged or under development. This stands in stark contrast to the situation in the European Union, where the European AI Office is already operational, while the national-level landscape remains uneven. Some Member States have already established, or are in the process of establishing, dedicated AI authorities. Others, such as Croatia, have not yet designated the bodies that will be responsible for enforcing the AI Act.

INSTITUTIONAL CAPACITIES FOR DIGITAL GOVERNANCE IN AND BEYOND THE EU

This chapter presents the findings of an original empirical study based on semi-structured interviews[23] exploring the institutional capacities and broader structural preconditions for digital governance as introduced by the new European regulatory framework both in and beyond the EU.

Given the differences in national contexts, research scope, and the availability of expert input, Croatia's results are presented in an integrated chapter, while Serbia and Montenegro are examined in relation to individual legislative acts.

The aim was to provide a qualitative and descriptive interpretation of the findings in order to assess the state of institutional capacities in all three countries, identifying key similarities and differences, and paying particular attention to the technical, human, operational, and financial resources required for the effective implementation of new digital governance processes.

23 While respondents from Serbia and Montenegro agreed to be named, all Croatian interviewees requested anonymity; therefore, their quotes are attributed by institutional affiliation or professional role only.

INSTITUTIONAL CAPACITIES FOR DIGITAL GOVERNANCE IN CROATIA

We examine Croatia's institutional capacities for digital governance from the perspective of an EU Member State directly obliged to implement the new regulatory acts. At the same time, Croatia shares many of the socio-political, institutional, and systemic challenges typical of the wider Southeast European region. These are rooted in the relatively late development of independent institutions and regulatory bodies, which continue to face both internal and external constraints, including limited expertise and persistent risks of institutional capture.

CAPTURE OF INDEPENDENT INSTITUTIONS AS A KEY CHALLENGE

Regulatory agencies designated as national competent authorities for EU digital regulation are, in principle and as defined by relevant national legislation, independent and free from political or private influence. In practice, however, Croatia displays persistent features of state capture. Holders of executive power exercise personal political control over governing structures, including ministries, affiliated state bodies, public institutions, regulatory agencies, public enterprises, and non-public entities entrusted with public functions or competences.

This capture network, comprising institutional stakeholders and private actors, facilitates the exchange of influence, favours, and resources to advance private and special interests at the expense of the public interest. Consequently, Croatian institutions remain structurally weak and exposed to political pressure and private influence. Centralised political control over public funds, public goods, and appointments continues to be the dominant explanatory factor for understanding the broader governance context.[24]

24 GONG. "Naša zarobljena mista. Istraživački izvještaj studija kvalitete lokalnog javnog upravljanja u Hrvatskoj" ["Our Captured Places: A Research Report on the Quality of Local Public Governance in Croatia"]. Accessed 24 June 2025. https://www.gong.hr/media/uploads/nasa_zarobljena_mista.pdf

Political capture

The degree of political control over executive regulatory agencies in Croatia appears to be proportional to the extent to which their decisions affect the political and private interests of decision-makers and capture agents. One prominent example is the Government's complete political dominion over regulatory agencies in the energy sector, most visibly demonstrated in the scandal that the media and public dubbed "Gas for a Cent". Amid surging gas prices and full storage capacities, the Government sold excess gas at a symbolic price to a well-known businessman in order to balance the amount of gas in the system. Although the authorities described the incident as a sequence of unintentional oversights and unfortunate circumstances, the only official dismissed from any of the involved agencies or independent bodies was the one who internally and publicly disclosed key details of the case.[25]

Business capture

In contrast, when it comes to regulatory agencies responsible for market surveillance, the primary risk of institutional capture often arises from private sector influence rather than direct political interference. A notable example involves the Croatian Civil Aviation Agency, where a deputy director approved and signed a request by the private concessionaire operating Zagreb International Airport to increase the maximum price of airport services – a decision that directly affected carriers such as the state-owned Croatian Airlines. Shortly thereafter, the official resigned from public service and assumed a position with the same concessionaire.[26]

Another notable example is the rise and subsequent collapse of the Agrokor conglomerate, which sent shockwaves through the Croatian economy.

25 HRT. "Abramović odlazi s čela HROTE; Oporba: Zato što je govorio o plinskoj aferi" [Abramović Leaves the Head of HROTE; Opposition: Because He Spoke About the Gas Affair]. 22 September 2023. Accessed 24 June 2025. https://vijesti.hrt.hr/hrvatska/grbin-11049598

26 Jutarnji list. "Sporno rješenje najvećeg hrvatskog prometnog projekta – Francuzima na Zračnoj luci Zagreb osigurali 300 mil eura ekstra profita!" [Controversial Solution in Croatia's Largest Transport Project – The French Were Granted an Extra 300 Million Euros in Profit at Zagreb Airport!] 20 January 2016. Accessed 24 June 2025. https://www.jutarnji.hr/vijesti/hrvatska/sporno-rjesenje-najveceg-hrvatskog-prometnog-projekta-francuzima-na-zracnoj-luci-zagreb-osigurali-300-mil.-eura-ekstra-profita-88945

During the period of Agrokor's rapid expansion and growing market dominance – achieved through acquisitions and allegedly unfair trading practices – the Croatian competition agency (AZTN) remained notably passive. At the time, the agency was headed by the spouse of an Agrokor executive.[27]

WEAK INSTITUTIONAL STANDARDS AND PROCEDURES

Erosion of ethical standards

Meaningful ethical standards in internal bylaws and conflict-of-interest provisions in national legislation have not strengthened over time; on the contrary, they were weakened. While the heads of regulatory agencies are formally classified as state officials and therefore fall under the scope of the Conflict of Interest Act, this legal framework has proven insufficiently effective in practice. The competences of the enforcement authority were significantly curtailed by precedent-setting court decisions that annulled years of established enforcement practice.[28] As a result, state officials are no longer held accountable for inadequate management of their conflicts of interest. This erosion of enforcement capacity has undermined the law's intended purpose to influence political practice and to strengthen public trust and accountability in the exercise of public office.

Politicised appointment procedures

The perceived political dependence of regulatory agencies is further reinforced by their appointment procedures. It is widely acknowledged – and rarely contested – that the Prime Minister exercises broad discretion in the

27 Index.hr. "Todorić kupio Polikliniku Nemetova i za ravnatelja postavio supruga šefice Agencije za tržišno natjecanje" ["Todorić Bought the Nemetova Polyclinic and Appointed the Husband of the Competition Agency's Director as Head"] 20 June 2012. Accessed 24 June 2025. https://www.index.hr/vijesti/clanak/Todoric-kupio-Polikliniku-Nemetova-i-za-ravnatelja-postavio-supruga-sefice-Agencije-za-trzisno-natjecanje/621706.aspx

28 Dnevnik.hr. "Što će biti s odlukama Povjerenstva za sukob interesa: 'Past će one odluke koje je tek trebalo donijeti, a neke se odnose na Plenkovića i članove Vlade'" ["What Will Happen to the Decisions of the Conflict of Interest Commission: 'The Decisions That Were Yet to Be Made Will Fall, and Some Concern Plenković and Members of the Government'"] 2 February 2021. Accessed 24 June 2025. https://dnevnik.hr/vijesti/hrvatska/dalija-oreskovic-o-ukinu-toj-odluci-povjerenstva-za-odlucivanje-o-sukobu-interesa---638356.html

appointment of government members, heads of government offices, public companies, regulatory agencies, and independent bodies. This perception was recently reinforced by the Prime Minister's response to criticism from the Ombudsperson, who had condemned his failure to denounce a fascist salute at a concert with record-breaking attendance. Rather than addressing the substance of the critique, he remarked: "Should I, as the Prime Minister, listen to her? We appointed her. She is there thanks to me."[29] Appointments to regulatory agencies are most often guided by political loyalty and informal personal connections rather than by professional qualifications or demonstrated competence.

EXPECTED LOWER RISK OF CAPTURE IN DIGITAL REGULATION DUE TO ABSENCE OF VLOPS AND GATEKEEPERS IN CROATIA

While the risk of undue private influence over regulatory agencies in Croatia remains insufficiently mitigated overall, it is considerably lower in the context of the DSA, DMA, and AI Act. Enforcement of these regulations does not directly concern business actors that play a systemic role in Croatia's economy or form part of the existing capture network. Croatia does not have VLOPs under the DSA or gatekeepers under the DMA, and this situation is unlikely to change in the near future. Domestic companies subject to the DSA – predominantly hosting providers, e-commerce platforms, and media outlets – fall under simple obligations. As a result, the usual incentives for exerting informal or political pressure on regulatory bodies are notably weaker than in other sectors marked by entrenched links between political and private interests.

29 Mirovina.hr. "Plenković se obrušio na pravobraniteljicu zbog Thompsona: 'Da ja nju slušam? Mi nju biramo'" ["Plenković Lashed Out at the Ombudswoman over Thompson: 'Should I Listen to Her? We Are the Ones Who Elect Her'"]. 9 July 2025. Accessed 24 June 2025. https://www.mirovina.hr/novosti/plenkovic-se-obrusio-na-pravobraniteljicu-zbog-thompsona-da-ja-nju-slusam-mi-nju-biramo/

INSTITUTIONAL CHALLENGES AND RISKS

Lobbying risks

It can be reasonably expected that regulatory agencies will, in general, operate independently from political influence in matters related to the enforcement of EU digital regulations. However, undue political interference may still arise in exceptional cases of particular relevance to the political elite. This risk could materialise, for instance, if large IT companies were to engage in direct lobbying of the Government, thereby increasing political sensitivity and interest in the regulatory decisions and enforcement actions of the competent national authorities.

AZOP's institutional underdevelopment

As Croatia's data protection authority, AZOP plays an increasingly significant role in safeguarding digital human rights. Although its mandate centres on the protection of fundamental rights, its legal and institutional framework more closely resembles that of a regulatory agency than of an independent institution such as the Information Commissioner or the Ombudsperson. This is particularly evident in the absence of a cooling-off period for candidates applying to head the agency. Notably, the current director applied for the position while still serving as a senior political official in the Ministry of Physical Planning, Construction and State Assets, shortly after ending his membership in the ruling political party. Introducing a cooling-off period as a formal eligibility criterion for the head of the institution would acknowledge AZOP's growing importance in protecting individuals and their rights, from the harms of digital technologies.

AZOP already enforces the GDPR, has recently been authorised to issue removal and information orders under the DSA, and is expected to act as the market surveillance authority for several categories of high-risk AI systems.

HAKOM's relative independence and risks in sensitive cases

The Croatian Regulatory Authority for Network Industries (HAKOM) is expected to exercise an adequate degree of political independence in its role as Digital Services Coordinator (DSC). However, the risk of undue political influence increases significantly in the sensitive context of illegal content removal on social media platforms, particularly in cases involving political speech critical of the government or political actors. Such pressures

are unlikely to be directed at the DSC itself, which primarily coordinates national DSA enforcement, but rather at the public bodies authorised to issue removal orders. For instance, when the Ministry of the Interior orders the removal of allegedly illegal political speech, the process entails substantial reputational risks for undue political influence. Moreover, past practice by the police indicates limited institutional capacity to respond in a proportionate manner in such sensitive cases.[30]

AZTN's passivity and lack of proactivity

As the national competition authority, AZTN has long attracted particular attention from political and business elites, a dynamic that has contributed to its limited proactivity in regulatory enforcement. This assessment was echoed by an investigative journalist interviewed for this study, who observed:

> *"The Agency remained passive while Agrokor expanded, increased its market share, and became a company with systemic impact on the Croatian economy – too big to fail. Today, it similarly turns a blind eye to obvious cartel practices in the retail sector, directly contributing to inflationary pressure; according to a Croatian National Bank report, increased profit margins account for 60% of recent price hikes. The Agency won't act proactively on any significant issue unless it is explicitly pushed to do so. If you do nothing, you can't make mistakes."*
> *– Investigative journalist, Croatia*

Given this pattern, AZTN is highly unlikely to engage proactively in DMA-related enforcement, as such actions require an assertive institutional posture and would involve powerful gatekeepers with significant geopolitical influence. While the agency is expected to formally assume

30 Tris. "Verbalni delikt: Znanstvenik koji je završio u Remetincu zbog dobacivanja ministrici Divljak može na slobodu". ["Verbal Delict: The Scientist Who Ended Up in Remetinec for Shouting at Minister Divjak Can Be Released"]. 29 August 2019. Accessed 24 June 2025. https://tris.com.hr/2019/08/verbalni-delikt-znanstvenik-koji-je-zavrsio-u-remetincu-zbog-dobacivanja-ministrici-divjak-moze-na-slobodu; Indeks.hr. "Oslobođen mladić koji je vikao 'HDZ lopovi, lopine!'". ["Young Man Acquitted for Shouting 'HDZ Thieves, Crooks!'"]. 21 April 2018. Accessed 24 June 2025. https://www.index.hr/vijesti/clanak/oslobodjen-mladic-koji-je-vikao-hdz-lopovi-lopine/1040180.aspx

its responsibilities under the DMA, it will likely refrain from initiating enforcement proceedings against designated gatekeepers. This passive stance is also expected to remain unchallenged by holders of executive power and by private actors presumed to exert influence over the agency's operations.

While Croatia remains a strong candidate for classification as a captured state, it is nevertheless expected that regulatory agencies will act with a sufficient degree of political independence and remain largely free from undue private influence in their roles as competent national authorities for the DSA, DMA, and AIA. However, politically sensitive cases, such as content-removal decisions or lobbying by major technology companies, could still trigger episodes of undue influence.

TECHNICAL CAPACITIES

Mixed capacities across agencies

AZTN and HAKOM possess adequate technical capacities to fulfil their new responsibilities under the DMA and DSA. By contrast, while AZOP has demonstrated the technical expertise needed for general GDPR enforcement, its limited resources prevent it from adequately monitoring AI systems, whether under the GDPR or the AI Act. These limitations are closely linked to constraints in human resources, which are examined in the following section.

Reliance on tools over expertise

According to an AZOP employee, the agency effectively fulfills its mandate under the GDPR, despite persistent human-resource challenges arising from salaries that are uncompetitive compared with equivalent positions in the private sector.

> *"AZOP uses technical tools to improve the efficiency of its GDPR supervisory procedures, such as the cookie-analysis tools developed by the EDPB and the EDPS, as well as through educational activities, including webinars.*
>
> *The Agency has a limited number of legal experts, while the shortage of IT specialists is particularly pronounced. Recruiting individuals with the necessary technical knowledge*

and experience is essential to ensure the capacity needed to effectively perform the Agency's current tasks, and especially to assume new responsibilities arising from the European Union's expanding digital regulatory framework, with a particular focus on the Agency's new mandate under the Artificial Intelligence Act."
– AZOP employee

HUMAN CAPACITIES

Acknowledged expertise gap

Annual activity reports, public statements, and interview responses consistently indicate that all examined national authorities recognise a gap in knowledge and expertise arising from their newly assigned roles in enforcing complex EU digital regulations. All three agencies have recognised the need to establish multidisciplinary teams and have emphasised that their expertise must be continuously developed and updated to meet regulatory demands.

EU-level participation: Learning and capacity-building

Additional training and participation in EU-level working groups and cooperation mechanisms are regarded as key to advancing institutional expertise and strengthening overall capacity.

"Existing staff continuously upgrade their knowledge through training programmes, external professional development opportunities, participation in the working groups of the European Data Protection Board, and attendance at international conferences."
– AZOP employee

HAKOM likewise recognises the importance of continuously developing its human capacities and considers active participation in EU-level enforcement mechanisms a crucial component of this effort. To support this objective, the Agency has secured adequate funding for training and capacity-building activities.

"Keeping pace requires continuous learning. We take full advantage of education programmes offered by the European

Commission, and we also organise our own training activities. Participation in EU enforcement networks significantly strengthens our capacities. HAKOM is actively involved in all eight working groups of the European Board for Digital Services (EBDS), regularly attends monthly meetings, and supports the Commission in its enforcement actions under the DSA. The DSC data-sharing platform (AGORA) is another valuable tool, allowing us to exchange advice with colleagues from other Member States. A substantial part of my working time is dedicated to these EU-level activities."
– HAKOM Employee #2

In its most recent annual report AZTN also recognises that exchanging experiences through participation in EU-level coordination and advisory activities "will further strengthen the Agency's capacity to operate effectively in this challenging and complex field."[31]

In an effort to strengthen its capacities in the area of digital markets, the Croatian Competition Agency (AZTN) established a Section for Digital Issues, Forensics, and Informatics in 2024. New data experts were hired and joined the section, enhancing the Agency's ability to "monitor market behaviour and structure in the digital environment". According to AZTN's 2024 Annual Report, the newly established section is expected to enable the Agency to "more efficiently monitor and understand the business models of large digital platforms and to contribute to consumer protection in the digital age".[32] The report explicitly highlights AZTN's reliance on multidisciplinary teams, noting that each case is handled by a team composed of at least one lawyer and one economist, and often supported by an IT expert. AZTN is also highly active in working groups, initiatives, and advisory or coordination bodies at the EU level. The Deputy President of the AZTN Council represents Croatia in the Digital Markets Advisory Committee.

31 Hrvatski sabor. "Godišnje izvješće o radu Agencije za zaštitu tržišnog natjecanja za 2024. godinu" ["Annual Report on the Work of the Croatian Competition Agency for 2024"]. Published 12 June 2025. Accessed 24 June 2025. https://sabor.hr/sites/default/files/uploads/sabor/2025-06-12/152802/IZVJ_AZTN_2024.pdf

32 Ibid. 29.

Increased workload

The growing workload of AZOP, stemming from its role as the national data protection authority (DPA) under the GDPR, has not been matched by a corresponding investment in human resources. Salaries at AZOP remain significantly lower than those offered in the private sector for professionals in data protection and law, leading to brain drain, difficulties in attracting qualified candidates, and a number of unfilled positions. Although a recently adopted bylaw increased the number of positions at the agency from 69 to 82, only 32 posts are currently occupied. Unlike most other regulatory bodies, AZOP staff are classified as civil servants under the Act on the Implementation of the GDPR. This classification subjects the agency to rigid salary schemes and limits its ability to align its human resources policies with operational needs and identified risks. Even if AZOP is not designated as the sole market surveillance authority under the AI Act, it will remain responsible for overseeing several categories of high-risk AI systems. The agency's limited human capacity therefore poses a serious risk to the effective enforcement of the AI Act.

Need for highly qualified experts in digital technologies

> *"There is a strong need to recruit highly qualified professionals with expertise in artificial intelligence and modern digital technologies... The Agency currently lacks both the human and technical capacities required to effectively assume the supervisory tasks foreseen under the AI Act. In accordance with Article 10(2) of the Act on the Implementation of the General Data Protection Regulation (Official Gazette 42/2018), the rights and obligations of AZOP staff are governed by the regulations applicable to civil servants, while the Agency's internal organisation follows the rules applicable to state administrative bodies.*
>
> *This regulatory framework prevents the Agency from offering competitive working conditions, particularly when recruiting highly educated professionals in the fields of information and communication technologies and artificial intelligence. As a result, the Agency is losing experienced staff to the private sector and faces significant difficulties in attracting new experts,*

especially those with IT backgrounds."
– AZOP employee

AZOP has recognised the need to restore the Agency's formal status as an authority with public competences, which would also entail reclassifying its employees from state clerks to public servants, ensuring higher salaries.

> *"To mitigate these risks and strengthen institutional capacities, AZOP continuously undertakes awareness-raising and outreach activities directed at relevant stakeholders and decision-makers regarding the need to reorganise the Agency. A key element of the proposed reorganisation is the reclassification of staff from the category of state clerks to public servants. This would allow for the adoption of an internal bylaw establishing appropriate salary coefficients for experts in the fields of IT and artificial intelligence, thereby creating the conditions necessary to recruit qualified IT professionals, with particular emphasis on artificial intelligence and cybersecurity. We believe that such a reorganisation would represent a crucial step toward ensuring stable, sustainable, and high-quality human resources, essential for the effective performance of supervisory tasks in the field of artificial intelligence." – AZOP employee*

During parliamentary discussions on the recently adopted bylaw, a representative of the Ministry acknowledged that discussions with AZOP on this issue are ongoing but refrained from making any commitment regarding either the timeline or the political will to initiate a formal legislative process. The representative further noted that "amending the law alone is not enough to attract new personnel", signaling considerable uncertainty about the prospects for such reforms.

The newly adopted bylaw governing AZOP's operations establishes a Department for Artificial Intelligence within the Sector for EU Affairs, International Cooperation, and Legal Matters.[33] This structural change reflects AZOP's designation as one of the authorities responsible for the

33 Hrvatski sabor. "Pravilnik o radu Agencije za zaštitu osobnih podataka" ["Rulebook on the Work of the Personal Data Protection Agency"]. Accessed 24 June 2025. https://sabor.hr/hr/sjednice-sabora/pravilnik-o-radu-agencije-za-zastitu-osobnih-podataka-predlagateljica-agencija-za?t=154410&tid=213589

protection of fundamental rights under Article 77 of the AI Act. However, the Agency will have to undertake additional organisational restructuring once it is also designated as the market surveillance authority for high-risk AI systems.

HAKOM's Sector for Digital Services

Both HAKOM and the Agency for Electronic Media were initially considered potential candidates for the role of Digital Services Coordinator (DSC). However, HAKOM's stronger institutional capacities and its early proactive engagement led to a consensual decision that it was the more suitable choice. This designation represents a significant expansion of HAKOM's traditional mandate and is reflected in the establishment of new administrative structures within the agency, namely the Sector for Digital Services.

> *"The role of the DSC is fundamentally different from our traditional responsibilities. We are engaging with an entirely new set of institutional and non-institutional stakeholders. In anticipation of this shift, we proactively established early contacts and developed relationships with other national authorities designated under the DSA, as well as with relevant CSOs.*
>
> *The newly established Sector for Digital Services is expected to become fully operational by September [2025]. It will include a Sector Director and three staff positions: two to be filled by current employees and one by a new recruit. Although a final decision is still pending, it is highly likely that the new employee will be required to have a strong understanding of ecosystems of social networks and online platforms. While HAKOM already employs engineers, economists, and legal experts, the level of IT expertise in the Agency needs to be increased."*
> *– HAKOM employee #1*

Coordination and cooperation challenges

> *"One of the biggest challenges we face as the Digital Services Coordinator arises from close cooperation and coordination with other national authorities. Providing support often*

requires delving into highly specific and unfamiliar legal and regulatory contexts."
– HAKOM employee #1

It appears that the complexity of the new regulatory frameworks, combined with the novelty of the delegated tasks, has fostered a shared understanding across institutions that strengthening human capacitates is essential for effective enforcement. All examined agencies have established new administrative units and are actively working towards the formation of multidisciplinary teams.

However, AZOP stands out due to its unique legal status, which has been widely recognised as a serious impediment to both human-resource development and institutional strengthening. This structural constraint poses significant risks to the Agency's ability to effectively enforce its expanding set of responsibilities under the EU digital regulatory framework, particularly in relation to the AI Act.

OPERATIONAL CAPACITIES

Incremental development of procedures

The operational capacities of the examined institutions appear to be developing incrementally, in line with the gradual delegation of broader enforcement responsibilities under new and complex regulatory frameworks. In addition to this, development of clearly defined internal procedures and protocols remains a consistent and well-established practice across the regulatory agencies.

New work processes

"So far, HAKOM has identified nine new work processes related to DSA enforcement, six of which have already been fully defined. Additional processes are expected to emerge as enforcement activities progress."
– HAKOM employee #1

While AZOP has not yet been designated as the market surveillance authority under the AI Act, it already has experience in establishing internal procedures for the enforcement of EU legislation.

"AZOP has developed procedures for inspection and investigative processes, as well as for cross-sectoral and inter-institutional communication, and continues to work on improving them."
– AZOP employee

FINANCIAL CAPACITIES

Stable funding framework

In Croatian legislative practice, when an institution's mandate is expanded through new legislation, draft laws typically include a standard provision stating that the necessary funds for implementation will be secured through reallocation within the institution's existing budget. The Government's accompanying commentary usually notes that the required resources will be provided through the annual budgetary process, which determines the institution's financial plan. This approach was applied in the law on the implementation of the DSA and is expected to be repeated in the forthcoming law implementing the AI Act. While the budgetary process remains largely opaque, there are currently no indications that AZOP, AZTN, or HAKOM lack sufficient financial resources to perform their designated roles under these regulatory frameworks.

"It is extremely rare for the Government to propose changes to the financial and work plans that are submitted for approval each year."
–HAKOM employee #1

Adequate resources but salary constraints

"The Agency's operational funding is provided through the state budget, ensuring stable financing that is independent of both political influence and the private sector. AZOP has sufficient financial resources to cover the costs of operational infrastructure, supervisory procedures, staff training, cross-border investigations and cooperation, as well as the recruitment of new employees."
– AZOP employee

However, AZOP's legal status as a civil service body restricts its ability to offer competitive salaries, thereby limiting its capacity to attract and retain skilled professionals despite having adequate financial resources.

INSTITUTIONAL CAPACITIES FOR DIGITAL GOVERNANCE IN SERBIA

Serbia's institutional capacities are examined through the lens of a candidate country for EU membership. The analysis focuses both on the structural socio-political preconditions for developing an appropriate model of digital governance – encompassing the technical, human, operational, and financial capacities – and on the existing institutional landscape and its challenges, particularly those bodies whose roles may evolve into participation within future digital regulatory mechanisms.

INSTITUTIONAL CAPACITIES FOR DIGITAL SERVICES GOVERNANCE IN SERBIA

It remains under consideration what the optimal model of the Digital Services Coordinator (DSC) in Serbia should be – whether it should operate as a single authority, a collective body, or an entirely new institution established for this purpose.

Among existing institutions, the Regulatory Authority for Electronic Media (REM), as the national audiovisual regulator, is most often seen as the likely candidate for the role of DSC. The agency's expertise in media and audiovisual services is relevant for platforms with a strong media component; however, its capacity to assume the DSA's much broader mandate remains contested. The challenge of this "new phase of convergence" lies not only in adapting sector-specific bodies but also in addressing the structural legacies of delayed convergence, weak inter-institutional cooperation, and the wider political context characterised by executive dominance and fragile regulatory independence. The Regulatory Authority for Electronic Communications and Postal Services (RATEL) is also regarded as a potentially relevant actor in the field of digital services regulation. Finally, the analysis of institutional capacities in Serbia extends to broader institutional frameworks and professional communities relevant to digital governance.

For years, REM has been widely regarded as one of the most prominent examples of institutional political capture in Serbia – an authority that has failed to achieve genuine independence within an environment where democratic procedures exist largely in form, while their outcomes are shaped by political influence, particularly from the ruling structures.

The ongoing process of appointing members to the REM Council, intended to ensure inclusive and participatory representation, has in practice evolved into a politically orchestrated exercise. As a result, the body increasingly serves the interests of pro-government media rather than functioning as a genuine mechanism for safeguarding media pluralism, freedom of expression, and quality public information.

Delayed institutional convergence in media regulation

Serbia has experienced delayed institutional convergence compared with other European states. For instance, when REM was established in 2003 and restructured in 2014, the United Kingdom had already consolidated five regulatory bodies into Ofcom, anticipating the digital transition. By contrast, Serbia's regulators remained sectoral and conventional in design.

> *"Our REM is the peer of the British Ofcom... but you can see how differently they have grown. They do not look like peers."*
> *– Snježana Milivojević, media scholar*

While some European countries opted for a powerful convergent regulator – telecommunication, broadcasting and postal services – recognising that regulatory systems were moving toward a unified framework, others cautioned that in contexts with limited democratic capacity, such a concentration of power could prove highly problematic. There were no guarantees that such a body would possess the necessary competences or that effective checks and balances would be in place to ensure proper oversight.

> *"At that time, this wasn't yet a step toward platform regulation or digital services as a whole, but rather toward more conventional sectors like telecommunications. In 2022, when the media portfolio was transferred to the Ministry of Telecommunications, I believe that was the beginning of this trajectory, indicating that convergence is now taking place in that area. From this point onward, the media are no longer*

considered as a distinct cultural institution focused on content, but rather as a component of a public industry."
– Snježana Milivojević, media scholar

TECHNICAL CAPACITIES

REM: Administrative infrastructure between strong power and passivity

REM's technical profile reflects the effects of delayed institutional convergence. Its infrastructure is primarily administrative, with only one department responsible for monitoring audiovisual content. These limitations leave it unprepared for DSA-related functions such as systemic risk assessment, algorithmic transparency audits, or the accreditation of trusted flaggers.

"REM... has strong powers and at the same time is completely powerless and passive. It does not do regulatory work."
– Snježana Milivojević, media scholar

Sector-limited technical capacities of telecommunications regulator

Other domestic actors in Serbia possess stronger technical competences than the audiovisual regulator. The Regulatory Authority for Electronic Communications and Postal Services (RATEL), for instance, is widely recognised for its professional expertise in network and spectrum management.

"RATEL... operates with strong technical knowledge, at least based on the people from RATEL I've encountered."
– Snježana Milivojević, media scholar

Yet, despite this expertise, RATEL's mandate remains narrowly confined to telecommunications and postal services, limiting its ability to address the broader governance needs of digital platforms under the DSA.

This limitation is compounded by structural conditions within the telecom sector. The dominance of the state-owned operator, Telekom Srbija, has fostered what has been described as "a near-monopoly in telecommunications – also not the goal of regulation." Such market concentration illustrates

that technical expertise, while valuable, does not automatically translate into effective or independent regulatory outcomes.

IT community with technological capacities, but globally and profit driven

Unlike institutional regulators, Serbia's IT sector demonstrates a distinct type of technical competence – marked by agility, global connectivity, and advanced technological expertise that could, in principle, contribute to implementing DSA requirements, particularly in areas such as data access and algorithmic auditing.

> *"However, this community has developed outside any awareness or concern for regulatory frameworks... it evolved without regulatory scruples."*
> *– Snježana Milivojević, media scholar*

This suggests that while Serbia possesses significant pools of expertise, they remain dispersed across sectors and insufficiently integrated into formal institutional structures. The central challenge, therefore, lies not in technical development alone, but in creating mechanisms to channel these resources into a coherent and accountable framework for DSA implementation.

HUMAN CAPACITIES

"State administrative" instead of "regulatory" bodies

The human-capacity dimension represents another area of weakness. REM's staffing structure mirrors that of a conventional state administration, comprising legal and general service units alongside a monitoring department. This configuration leaves the authority without specialists in data science, algorithm auditing, or systemic risk analysis, skills central to the DSA's new oversight model.

> *"They have the infrastructure of a conventional state body... an administrative apparatus that only services the monitoring unit, which itself just monitors content. If you look at the structure of REM, it has absolutely no capacity to deal with digital services... it cannot even properly cover the media aspects*

of digital platforms."
– Snježana Milivojević, media scholar

No links with knowledge community

REM has failed to establish links with the knowledge community or to develop structured dialogue with other stakeholders. The absence of systematic cooperation with universities, research institutions, and civil society reduces the regulator's ability to respond to the complex knowledge demands of digital platform governance.

> *"We have never seen REM hold a consultation with academia or seek research assistance. Even tasks such as monitoring were defined without methodological consultation. There is no culture of coordination here, especially at the cognitive level."*
> *– Snježana Milivojević, media scholar*

Poor articulation of knowledge into institutional mechanisms and decision-making

When REM's structure was established nearly two decades ago, one of the key arguments for introducing a system of authorised nominators and a broad circle of stakeholders was to integrate diverse sources of knowledge. However, the resulting mismatch between the formal rationale and actual practice has produced a regulatory environment in which knowledge is poorly translated into institutional mechanisms and decisions. This, in turn, has undermined the possibility of developing a robust and forward-looking governance framework for digital services.

> *"The argument was precisely to bring together different types of knowledge within the body – from various fields or, as they saw it, from various interests. Yet it was not really about knowledge. It was about interests. This produced an amorphous and fragmented media system, led by an arguably incompetent but politically influential audiovisual regulator."*
> *– Snježana Milivojević, media scholar*

Complementary but fragmented expertise of other actors

RATEL's engineers bring strong technical expertise, particularly in networks and spectrum management, even though their mandate remains sector-limited. Civil society organisations contribute rights-based perspectives, while academia offers public-interest criteria and methodological frameworks. Yet these resources remain dispersed. Without stronger links to these knowledge reservoirs, Serbia's institutional capacities will continue to be fragmented and performative rather than substantive.

> *"The IT sector is a powerful community... providing a wide range of digital services and introducing another kind of efficiency and a repertoire of knowledge that has developed globally. Still there is little willingness to learn... only two consultations on the DSA and DMA so far."*
> *– Snježana Milivojević, media scholar*

OPERATIONAL CAPACITIES

Coordination challenges

Operationally, Serbia faces significant coordination difficulties. The DSA requires continuous horizontal cooperation between national regulators and vertical alignment with the European Commission and the European Board for Digital Services. However, current practices in Serbia fall well short of these expectations, raising doubts about REM's capacity to lead structured dialogues and cross-border cooperation as envisaged by the DSA.

> *"The experience of coordinating between different regulators in Serbia has been scandalous."*
> *– Snježana Milivojević, media scholar*

Internal procedural and functional limitations

REM's operational model remains rooted in its traditional audiovisual remit. Its monitoring work continues to focus narrowly on observing broadcast content, with little adaptation to the complexity of online platforms. The authority lacks mechanisms for accrediting trusted flaggers, overseeing systemic risk mitigation, or fulfilling EU-level reporting obligations.This reveals a significant gap between the DSA's systemic oversight model and the agency's existing practices.

"REM does not even have the methodology to monitor what happens online, it is stuck in the logic of television, counting seconds and minutes of airtime."
– Snježana Milivojević, media scholar

Autonomy and independence contested: authoritarian tendencies as structural challenges for functional regulation

An additional contextual and political concern is Serbia's increasing authoritarian drift, which undermines the principles of independence and public accountability that underpin the EU's model of digital governance. At the same time, the EU itself is redefining the concept of regulatory independence in favour of greater efficiency, often at the expense of flexibility and sensitivity to local contexts and to the specificities of certain services.

"While the EU is shifting toward centralised coordination through the European Commission, reducing regulators' ties with national legislatures and raising its own questions about democratic legitimacy and checks and balances, Serbia has yet to undergo even the previous regulatory generation, in which the regulator operates independently from the executive branch. If there are no checks and balances, independence begins to work against society."
– Snježana Milivojević, media scholar

Institutional model for DSA implementation contested

The question of institutional design remains unresolved. Serbia has not yet decided whether to designate REM, establish a new body, or develop a joint model with other regulators, such as RATEL or the Commission for the Protection of Competition.

"It may be easier to rely on an existing body than to build a completely new one... but in any case, if it is to be REM, it will have to be significantly strengthened. The starting point should be a systematic diagnostic exercise: first, to identify what our regulators actually have, what they can do, and where the missing areas are. Without such groundwork, the

implementation of the DSA risks becoming purely formal, replicating past patterns of fragmented and ineffective regulation."
– Snježana Milivojević, media scholar

FINANCIAL CAPACITIES

Traditional budgetary limits

REM's budget remains calibrated to its traditional broadcasting functions, covering primarily administrative overhead and the operation of its monitoring unit. The new responsibilities arising under the DSA will require substantially greater resources. However, Serbia has not yet established any dedicated budget lines for future DSA implementation.

Efficiency rhetoric and political risks

The political context raises concerns about sustainability, as budgetary weakness can undermine formal mandates. There is a serious risk that appeals to efficiency may once again serve as a justification for chronic underfunding, leaving the future DSC unable to perform its core tasks.

"Under the principle of efficiency, institutional capacity may be reduced – or never developed at all. We already have a regulator with strong powers but without real resources, and it has become passive."
– Snježana Milivojević, media scholar

Increasing pressure from overlapping mandates

The anticipated parallel implementation of the European Media Freedom Act (EMFA) alongside new digital legislation is expected to further strain institutional resources. The EMFA's requirements on media pluralism and transparency overlap with REM's existing mandate, creating additional administrative and substantive obligations.

"There will be significant pressure on the audiovisual regulator, raising questions about how REM could manage overlapping obligations in the absence of a substantial

expansion of its budget and staff."
– Snježana Milivojević, media scholar

Need for predictable and independent resources

For Serbia to establish a credible Digital Services Coordinator, a comprehensive financial strategy will be required – one that ensures predictable, transparent, and politically independent funding for staffing, training, technological infrastructure, stakeholder engagement, and international cooperation. Without such provisions, the institutional framework risks remaining largely symbolic and incapable of meeting the systemic oversight standards demanded by the DSA.

INSTITUTIONAL CAPACITIES FOR DIGITAL MARKET GOVERNANCE IN SERBIA

Serbia's efforts to align with EU digital market regulations represent a complex balancing act, reflecting its dual position as an EU candidate country and a developing economy facing distinct structural challenges. Its aspiration for EU membership drives the alignment of national laws with EU standards, as evidenced by the up-to-date transposition of competition law rules. However, the institutional framework remains a work in progress.

Serbia has no dedicated digital markets legislation and instead relies on existing laws, such as the Law on Protection of Competition or the Law on E-Commerce, to address issues related to the Digital Markets Act (DMA). This reliance on a general legal framework differs from the EU's targeted approach under the DMA, which is specifically designed to regulate gatekeepers and address systemic market imbalances. In the DMA's centralised enforcement model, where the European Commission holds primary authority, national authorities in Member States play a subsidiary and supportive role. This arrangement does not resolve the challenge faced by non-member states such as Serbia, which must first build the foundational institutional capacity to exercise even that supportive function.

The Serbian Commission for Protection of Competition (CPC) is the main national authority that could assume a DMA-like role domestically, as its mandate covers competition law enforcement across all sectors. However, the CPC's current mandate, resources, and enforcement practice remain

oriented towards traditional competition law and have not been adapted to the distinct nature of platform economics and data-driven gatekeeping. The CPC has conducted sectoral analyses – such as its 2020–2021 assessment of food-delivery platforms – and maintains formal cooperation links with other regulators, but it has not initiated DMA-style gatekeeper investigations.

These factors result in several overarching challenges for the CPC's ability to enforce DMA-like rules. The authority has neither an explicit DMA-related mandate, nor the specialised procedural instruments that the DMA presumes – such as continuous market monitoring, audited reporting by gatekeepers, or compliance dialogues. Moreover, as Serbia lies outside the EU's DMA enforcement chain, it cannot benefit from the European Commission's investigative powers or the opportunities for institutional learning. These structural conditions risk creating an enforcement deficit that allows gatekeeper conduct to affect Serbian users and businesses. A review of Serbia's, and specifically CPC's, capacities for the enforcement of DMA-like rules is provided below.

TECHNICAL CAPACITIES

Technical capacities available but outside institutional structures

There appear to be no major obstacles regarding the technical capacities required for DMA implementation by the CPC. In a broader sense, Serbia's tech sector represents a powerful and globally connected community with a high level of expertise.

> *"It has, however, developed largely outside of any regulatory framework and lacks a culture of engagement with institutional governance. Still, it provides a good starting position for developing the technical capacities and expertise that could be 'borrowed' from the private sector."*
> *– Bogdan Gecić, lawyer*

HUMAN CAPACITIES

The CPC's staff profile is dominated by competition lawyers and economists, with limited experience in data science, machine learning, or software-driven

market analysis. The recruitment of digital-market experts is constrained by public-sector pay scales and the pull of the private technology sector.

Outdated legal education system and lack of digital law expertise in general legal community

The most critical challenge for Serbia, reflected also in the CPC's expertise, is a severe deficit in human capital, stemming primarily from the country's outdated legal education system. Law faculties have not modernised their curricula to address the complexities of digital law. The focus remains on traditional civil law subjects, while the need to prepare students for the regulatory frameworks of the digital age is systematically neglected.

The situation is further aggravated by the disregard for students' ability to access and understand educational materials in English, as well as by the tacit practice of discouraging both students and professors from pursuing advanced studies abroad. This paints a discouraging picture in which there is no solid foundation for developing domestic expertise capable of addressing modern regulatory challenges. As a result, there is a severe shortage of legal and technical professionals with the skills necessary to undertake complex analysis – mostly visibly in the public sector.

> *"To expect that, in such a context, Serbia could adopt advanced legislation like the DMA and enable the CPC to take on Google, for example, seems beneficial only for lawyers or CSOs. Such legislation would be effectively unenforceable in our reality. I believe that smaller jurisdictions in the region stand a much better chance by entering a single market arrangement with the EU – such as EFTA or the EEA – or by pursuing full EU membership. This would put them in a position where the European Commission can take its intended primary role, while our local authorities continue to develop their capacities."*
> *– Bogdan Gecić, lawyer*

Individual enthusiasm not institutionally supported

The CPC has motivated staff who actively participate in training programmes organised by the EU Directorate-General for Competition.

"Such individual efforts are insufficient to create the 'critical mass' of experts required for systemic change. Personal initiative is not yet matched by an enabling institutional framework."
– Bogdan Gecić, lawyer

To bridge this gap, Serbia should first undertake a comprehensive reform of its law faculties to build a fundamental understanding of digital legislation. Once a solid foundation is in place, targeted training could be offered to new government agencies' employees, with EU funds used to support further professional development.

OPERATIONAL CAPACITIES

Lack of procedures for market monitoring and cross-border cooperation

Serbia lacks established procedures for continuous market monitoring and cross-border cooperation comparable to those enabled by the DMA's institutional structures. While the CPC has some experience in cooperating with sectoral regulators, there is no routine practice of conducting joint investigations that combine competition, data-protection, or consumer-enforcement approaches. The result is an institutional environment that favours case-by-case litigation over the systemic monitoring and preventive measures that the DMA's objectives imply.

Delayed implementation of traditional competition rules and "inquisitorial bias"

The CPC is still addressing the fundamentals of competition law, introduced in Serbia in the mid-2000s, nearly fifty years after the EU first established its competition framework. This delay makes it unrealistic to expect a small jurisdiction like Serbia, effectively a "rule taker" country (as opposed to "rule givers" such as the United Kingdom, traditionally seen as setting standards for others), to regulate global technology giants effectively. In addition, Serbia's legal system faces specific systemic challenges, reflected in the CPC's "inquisitorial bias": the Commission both investigates and adjudicates cases, which complicates its role and raises concerns about impartiality.

"While the CPC has increasing experience in interpreting classical competition law, the Serbian courts are still grappling with its basic concepts. In practice, this results in common situations in which appeals in competition cases are stalled until the statute of limitations expires."
– Bogdan Gecić, lawyer

Issue of institutional resilience and porosity to political interference

Institutional independence of enforcement bodies is among the key prerequisites for building operational capacity in DMA enforcement. While competition authorities in all jurisdictions face some degree of political pressure – as illustrated by the Siemens-Alstom merger case, where French and German leaders openly criticised the European Commission – the decisive factor is an institution's resilience.

"The key is the institution's resilience and porosity to such influence. This means that the independence of an institution is directly tied to the professional expertise and knowledge of its staff. When professionals are well-educated and can substantiate their decisions, they are better equipped to resist political pressure."
– Bogdan Gecić, lawyer

FINANCIAL CAPACITIES

Income does not guarantee enforcement capacity: need for highly skilled professionals

The financial situation of Serbia's regulatory bodies is not considered the primary obstacle to DMA implementation. The CPC generates significant revenue, largely through high administrative fees – substantially higher than those applied by its EU counterparts. However, this income does not necessarily translate into effective enforcement capacity. The core challenge lies in the ability to attract and retain highly skilled professionals capable of carrying out the complex tasks required under the DMA.

INSTITUTIONAL CAPACITIES FOR AI GOVERNANCE IN SERBIA

The EU Artificial Intelligence Act establishes a risk-based enforcement architecture requiring Member States to designate market surveillance authorities, notifying authorities for conformity assessment bodies, and national institutions responsible for the protection of fundamental rights. At the EU level, the framework introduces the European AI Office and the European AI Board to coordinate cross-border enforcement of general-purpose AI and other high-risk applications. This multi-layered design presumes significant national capacities in technical assessment, market surveillance, incident reporting, and inter-institutional coordination.

Working group for the draft AI law constituted

Serbia currently has no adopted legislation on artificial intelligence. The Government has established a working group to draft a new law, but no public information is available regarding the progress of this process or the regulatory objectives the group intends to pursue. The absence of a legal framework leaves open the question of which institutions will ultimately be responsible for enforcing Serbia's future AI legislation.

Diversity of regulatory approaches: Implementation of the Personal Data Protection Law as a cautionary tale

For Serbia, the process of establishing a legal and institutional framework for artificial intelligence represents a fundamental policy choice. Depending on the substantive rules eventually adopted, several enforcement models are possible: the creation of a new, centralised enforcement authority; the assignment of centralised enforcement to an existing regulator; or a decentralised distribution of responsibilities among multiple institutions.

Serbia is not only far from reaching a decision or consensus on this issue, but there have also been no visible public debates or policy announcements. Experts interviewed for this study expressed differing views, reflecting both their experiences with Serbian institutions and their expectations for future AI regulation. However, they unanimously pointed to the country's experience with the 2019 Personal Data Protection Law – modelled on the GDPR – as a cautionary example. The Law reproduced the EU's substantive standards, yet enforcement of data-protection rules has remained weak and ineffective.

"Any discussion of institutional capacities should, in any case, be preceded by strategic decisions on the specific objectives of Serbia's AI regulation. Is the goal to regulate any AI system accessible to Serbian citizens – for instance, widely available large language models such as ChatGPT – or should the law apply only to Serbian entities, or entities operating in Serbia, that sell or use AI systems locally? The answers to these questions will determine the types of enforcement mechanisms that need to be established."
– Slobodan Marković, adviser for digital technologies

Sectoral decentralisation and shared responsibilities: pros and cons

At this stage, the most realistic scenario for Serbia would be to adopt a decentralised model of AI governance, in which enforcement and oversight responsibilities are distributed among existing sectoral regulators – each covering AI within its respective domain.

"For example, the Medicines and Medical Devices Agency of Serbia should have a role in supervising AI systems used for medical purposes, while the Road Traffic Safety Agency should address systems already falling within its regulatory domain. This approach leverages the existing domain expertise of such bodies, some of which have already engaged with questions concerning AI use."
– Slobodan Marković, adviser for digital technologies

On the other hand, this model presents significant coordination and operational challenges, particularly regarding who would be responsible for regulatory and certification matters common to all AI systems.

Extension of Commissioner's mandate instead of new institution from the scratch

The Commissioner for Information of Public Importance and Personal Data Protection is perceived by some experts as a natural candidate for an AI regulatory body, capable of playing a significant role in enforcing future AI legislation by building on its existing experience with data-protection enforcement.

"This could represent a 'natural extension' of the Commissioner's current mandate, which already includes oversight of data-intrusive technologies such as video surveillance. Establishing a new institution with enforcement powers from scratch would be a far longer and more complex path than building on the Commissioner's existing potential and regulatory experience."
– Tijana Žunić Marić, IT lawyer

TECHNICAL CAPACITIES

Tech expertise can be outsourced

Expert assessments suggest that the technical requirements for effective AI governance in Serbia are relatively modest.

"In a decentralised system, sectoral regulators will not need high-performance computing infrastructure, as they will not be processing large datasets themselves. The implementation of the AI Act does not demand deep in-house technical expertise within public authorities; rather, it requires officials with a general understanding of how AI systems function and how regulatory obligations are structured."
– Slobodan Marković, adviser for digital technologies

Sophisticated technical expertise can be obtained from externally engaged consultants, as and when needed.

Specialised software as a useful tool for automated certification

"If the Commissioner for Information of Public Importance and Personal Data Protection were to be designated as the authority responsible for general certification, companies would be required to prepare AI documentation and undergo formal approval procedures."
– Tijana Žunić Marić, IT lawyer

For this purpose, regulators may rely on specialised software to monitor defined performance indicators or benchmarks. Such tools could accelerate

and partially automate certification processes, thereby saving time and resources while enhancing compliance with the future AI regulatory framework.

HUMAN CAPACITIES

Expertise concentrated in academia and private sector, CSO not systematically included in policymaking processes

Human-resource capacity is among the most pressing challenges for AI governance in Serbia. At present, the public administration has access to only a very limited pool of AI engineers, data scientists, and certification experts. Most relevant expertise is concentrated within academia and private companies, while civil society organisations working on algorithmic harms are present but not systematically involved in policymaking. This creates a structural dependence on external experts unless the state invests in targeted recruitment, competitive remuneration schemes, and sustained training programmes.

Need for horizontal coordination of expertise

> *"Some public bodies, such as the Road Traffic Safety Agency, already employ staff with knowledge of advanced technologies like autonomous vehicles."*
> *– Slobodan Marković, adviser for digital technologies*

Such expertise could be relatively easily integrated into a future AI governance framework. In a decentralised model, this would likely result in multiple "pockets" of AI-related knowledge within sectoral regulators. However, to be effective, these dispersed competences would need to be linked through a horizontal coordinating body or network, enabling experts to exchange information, share best practices, and promote consistent approaches across sectors.

Where sectoral regulators lack in-house expertise, they should be able to engage external consultants from academia or the private sector to provide machine-learning expertise, compliance advice, and risk assessments. Institutions such as the Serbian AI Institute, although currently focused on academic research rather than regulatory tasks, could play an important advisory role by offering technical input and training for public officials.

> *"Serbia's experience with the GDPR offers an instructive benchmark: the ecosystem of CSOs, law firms, and information security experts that developed around data protection could similarly support AI governance, for example, by conducting impact assessments, peer reviews, or providing second opinions."*
> *– Slobodan Marković, adviser for digital technologies*

Institutional restructuring required if assigned AI regulatory competences

> *"Significant institutional restructuring would be required, particularly within the Commissioner's Office, if it were to assume a central role in AI regulation."*
> *– Tijana Žunić Marić, IT lawyer*

A completely new department would need to be established, staffed by a multidisciplinary team of experts in compliance, data protection, and AI, with strong knowledge of e-government systems. Low salaries in public sector remain a critical obstacle, meaning that reliance on external consultants, at least in the initial phase, would likely be unavoidable. Such consultants could assist in designing the regulatory framework, developing procedures, and training internal staff until a sustainable pool of public-sector experts is built.

Significance of practical experience and understanding of technology and its risks

> *"Recruitment must prioritise candidates with practical experience, not just formal qualifications."*
> *– Tijana Žunić Marić, IT lawyer*

Too often, regulatory staff focus on formalistic compliance checks without a substantive understanding of technological risks. What is needed are "e-government consultants" with a multidimensional skill set – combining technical knowledge, compliance expertise, and risk assessment – capable of understanding AI systems in practice. Such profiles are scarce and highly competitive on the labour market, meaning the Commissioner would need to offer significantly better employment conditions, coupled with rigorous training and evaluation mechanisms.

"New hires should undergo structured onboarding, extended training, and even certification exams before being allowed to handle cases independently. Only by ensuring such high professional standards can Serbia build the cadre of experts required for credible AI regulation."
– Tijana Žunić Marić, IT lawyer

OPERATIONAL CAPACITIES

Need for coordination among dispersed experts

"The governance of AI in Serbia will inevitably involve a broad range of sectoral regulators, each holding partial competences in relation to the application of AI within their respective domains."
– Slobodan Marković, adviser for digital technologies

This structure is likely to produce clusters of expertise across different areas of public administration, shaped by each body's prior exposure to relevant technologies. To ensure effective implementation, these dispersed experts would need to be connected, ideally through a horizontal coordinating body or an informal working group, allowing for exchange of knowledge and harmonised regulatory practices.

The ITE Office lacks AI regulatory capacity despite strong technical infrastructure

Returning to the question of potential centralisation, one of the options discussed has been the possible role of the Office for IT and eGovernment (ITE Office).

"They currently lack the depth of expertise necessary to act as an AI regulator. This is due to the fact that their primary mandate is the digitalisation of public services, and they don't have any knowledge or experience in market regulation."
– Slobodan Marković, adviser for digital technologies

While the ITE Office manages critical infrastructure – such as the Government Data Centre and the state IT network – its staff are primarily

engaged in system maintenance and organisational support rather than regulatory oversight or risk assessment. Although it possesses advanced technical infrastructure, its operational focus would first need to shift towards improved management and automation of state IT systems before it could credibly assume regulatory responsibilities.

Sectoral agencies and the AI Institute have potential for AI-related compliance and strategic roles

By contrast, certain sectoral bodies – such as the Medicines Agency and the Road Traffic Safety Agency – already employ staff familiar with risks associated with earlier generations of information technologies. These institutions could therefore transition into AI-related compliance tasks more readily than the ITE Office.

The AI Institute could also play an important role in this transition. As a newly established institution, it brings together a substantial pool of researchers and scientists. Although its mandate is primarily academic and focused on publishing scientific work and advancing research agendas, the AI Institute could, in principle, contribute to national projects of strategic importance, such as language technologies or AI applications in the public sector.

Issues of independence and institutional strengths

> *"AI regulators would not require special safeguards beyond those already applicable to public administration."*
> *– Slobodan Marković, adviser for digital technologies*

Standard ethical codes and commitments to the public interest should apply, as with any other state authority. An AI regulator would most likely function as a conventional administrative body with a market-facing mandate, where functional independence from the executive is less critical than sectoral expertise and operational effectiveness. Without proven professional competence and continuity of experience, however, institutional strength remains in question.

Furthermore, enforcement of the current Personal Data Protection Law has been weak, characterised by extremely low penalties and an almost complete absence of proceedings against companies that flagrantly violate their obligations – including, most notably, major technology companies

offering services in Serbia that are required to appoint local representatives. Instead of imposing sanctions, the Commissioner has, on occasion, publicly thanked companies for voluntary compliance.

> *"Such practices undermine the seriousness of the law and send a message that, in Serbia, compliance is optional."*
> *– Tijana Žunić Marić, IT lawyer*

Effective AI governance requires credible enforcement and a professionalized institutional culture

> *"For the Commissioner to credibly take on AI regulation, both legal and practical independence must be ensured. Enforcement must apply equally to state bodies and private companies."*
> *– Tijana Žunić Marić, IT lawyer*

The perception that public authorities face no consequences for non-compliance, while private firms bear the regulatory burden, risks delegitimising the entire governance framework. A stronger sanctioning policy and a more professionalised institutional culture are therefore preconditions for expanding the Commissioner's mandate to include AI oversight.

Regulators must address both existing and novel categories of AI risk

> *"Two categories of risks will be central to any AI governance framework. The first are existing risks, such as threats to privacy, which will grow exponentially with the spread of AI. The second are novel risks, including hallucinations, algorithmic bias, and emerging cybersecurity vulnerabilities."*
> *– Tijana Žunić Marić, IT lawyer*

Regulators must be capable not only of verifying whether companies have adequately documented their AI use, but also of assessing whether genuine risk evaluations and mitigation measures have been conducted.

Corporate compliance models offer lessons for institutional design

> *"Lessons could be drawn from corporate e-compliance models, where governance boards typically include officers from compliance, legal, information security, and data protection. This approach could inform the design of future Serbian institutions tasked with AI oversight."*
> *– Tijana Žunić Marić, IT lawyer*

FINANCIAL CAPACITIES

Financial resources are the foundational bottleneck for AI governance capacity

Financial resources remain a key constraint for Serbia's preparedness to govern AI systems. Adequate financial investment is the enabling condition for all other forms of capacity: technical, human, and operational. Without stable and predictable funding streams, Serbia's AI governance framework risks remaining fragmented, ad hoc, and overly reliant on goodwill rather than on institutional resilience.

Lack of strategic prioritisation undermines financial planning, leaving sectoral regulators without dedicated resources for AI oversight

> *"Recent governments have shown little strategic focus on AI or broader digital regulation, with current developments largely driven by inertia from earlier initiatives. The state will likely need to rely on a combination of loans and direct budget allocations to finance AI-related governance."*
> *– Slobodan Marković, adviser for digital technologies*

Sectoral regulators, in particular, will require dedicated budgetary lines to cover the costs of compliance oversight. While the financial demands are not insurmountable in scale, they are essential to enabling regulators to perform their functions effectively.

> *"Effective AI supervision would require funds to cover very practical needs: hiring staff to organise compliance mechanisms, equipping them with basic infrastructure such as*

laptops and office space, and retaining external experts to carry out tasks such as AI risk mapping."
– Slobodan Marković, adviser for digital technologies

Without such baseline investments, regulatory structures would remain purely nominal.

Chronic underfunding of digital governance has limited institutional maturity

Experts emphasise the chronic lack of adequate funding for digital governance in Serbia. While relevant expertise exists – whether among private consultants, law firms, or professionals trained through GDPR implementation – such capacities cannot be mobilised without sufficient financial resources.

"Substantial resources are needed either to attract these experts into public service or to contract them externally. If domestic talent cannot immediately fill the gap, international consultants could be brought in to design the system and provide training, ensuring that local capacities are built up over time."
– Tijana Žunić Marić, IT lawyer

INSTITUTIONAL CAPACITIES FOR DIGITAL GOVERNANCE IN MONTENEGRO

Montenegro has achieved formal legislative alignment with the EU's digital acquis through the provisional closure of Chapter 10 – Information Society and Media. However, institutional and coordination challenges persist. Capacity building remains a key priority under EU scrutiny, while repeated government reorganisations have resulted in overlapping mandates and uncertainty, particularly in the areas of electronic commerce and implementation of the Digital Markets Act (DMA), where the Ministry of Economic Development still lacks sufficient expertise and resources.

By contrast, the Digital Services Act (DSA) process appears more coherent, with the Ministry of Culture coordinating implementation in parallel with the European Media Freedom Act (EMFA). Montenegro is also progressing in aligning with the NIS 2 Directive, the eIDAS 2 Regulation, and the AI Act, developing a National AI Strategy and establishing a dedicated unit within the Ministry of Public Administration. These developments signal increasing strategic attention to digital governance, although institutional maturity remains limited.

Chapter 10 provisionally closed, but practical implementation remains ongoing

Montenegro has provisionally closed Chapter 10 – Information Society and Media, following the adoption of legislation in the field of electronic communications and the alignment of its media legislation with the EU regulatory framework. These steps, completed during 2024 formally fulfilled the legislative requirements.

> *"Media legislation is not formally part of Chapter 10, but we included it within this package because the European Commission has, for some time now, considered Chapters 23 and 10 together in the context of media-related topics. We have also adopted the Law on Information Security, aligned with the NIS 2 Directive. It has not been fully transposed, and certain provisions of the Directive will be implemented through amendments to the Law on Electronic Communications, as that area falls under the competence of another institution – the Ministry of Economic Development. The European*

Commission's attention is strongly focused on capacity building, not only for this chapter but across all negotiation areas. This challenge is not unique to Montenegro but common to the entire region.
– Ružica Mišković, Head of the Working Group for Chapter 10

DMA poses a significant coordination and capacity challenge

"I must particularly emphasise that the DMA represents a major challenge, as Montenegro has undergone several government and institutional reorganisations that have resulted in shifting competences. Specifically, electronic commerce was once under the responsibility of the Ministry of Information Society and Telecommunications. At that time, there was no ambiguity regarding which institution was in charge, and it was that ministry which adopted the still-valid Law on Electronic Commerce. Following its dissolution, the Ministry of Public Administration was established. However, institutional policy subsequently evolved so that electronic commerce was no longer recognised as part of its mandate. Through a government decree, the competence was transferred to the Ministry of Economic Development."
– Ružica Mišković, Head of the Working Group for Chapter 10

Because of limited institutional capacity and the continued application of the existing Law on Electronic Commerce, there was no immediate incentive to introduce additional measures until the entry into force of the two new EU regulations – the Digital Markets Act (DMA) and the Digital Services Act (DSA). At present, the Ministry of Economic Development is not sufficiently prepared to assume coordination of DMA implementation, not only due to limited resources, but also because the regulation introduces an entirely new policy and enforcement domain for the institution.

As a result, the administration faces a coordination gap, particularly regarding the DMA and the question of which authority should lead its implementation.

DSA process is more advanced and institutionally anchored

Unlike the DMA, the implementation of the DSA has been formally recognised and institutionally anchored within the Ministry of Culture, which has taken proactive steps to coordinate alignment in parallel with the European Media Freedom Act (EMFA). This reflects a more coherent governance approach to the DSA, in contrast to the fragmented institutional landscape surrounding the DMA.

Gradual alignment with related EU digital frameworks

Beyond the DSA and DMA, Montenegro is actively pursuing harmonisation with other key EU digital acts, including the NIS 2 Directive – through the Law on Information Security – and the forthcoming eIDAS 2 Regulation, to be transposed through the planned Law on Electronic Identification and Trust Services, expected by 2026. In the field of AI regulation, work is underway on the National Strategy for Artificial Intelligence.

> *"Within the Ministry of Public Administration, we have established a new organisational unit within the relevant directorate specifically dedicated to this area, so the topic will be monitored and developed through that structure. The strategy, I believe, is also planned for adoption either by the end of 2025 or 2026."*
> *– Ružica Mišković, Head of the Working Group for Chapter 10*

INSTITUTIONAL CAPACITIES FOR DIGITAL SERVICES GOVERNANCE IN MONTENEGRO

Montenegro's digital-services governance landscape is marked by formal readiness but functional fragility. The institutional framework is in place, centred on the Agency for Audiovisual Media Services (AMU) and the Ministry of Culture and Media, yet technical, human, and financial capacities remain limited. Effective implementation of the DSA and related EU frameworks will depend on EU-supported training, inter-agency coordination, and sustainable funding, all essential to transform existing administrative structures into an operational regulatory system capable of addressing systemic risks posed by digital platforms.

TECHNICAL CAPACITIES

Audiovisual regulator as a DSC candidate

The Agency for Audiovisual Media Services (AMU) is currently the most plausible candidate to assume the role of Digital Services Coordinator (DSC).

> *"The first [institution] that wants to deal with this – and will probably be [the DSC] – is the Agency for Audiovisual Media Services. The Agency possesses a baseline of expertise and an initial understanding of the DSA framework. At this moment, it has human potential... They have knowledge about the DSA and what needs to be done."*
> *– Goran Đurović, Director of the Media Center*

However, this expertise remains largely conceptual rather than operational. The Agency lacks established mechanisms for monitoring, data collection, and algorithmic oversight, core functions under the DSA framework. As interviews indicate, the technical infrastructure required for compliance verification and systemic-risk assessment will need to be developed almost from scratch..

Telecommunications regulator with limited interest in digital regulations

Montenegro's other key regulatory body, the Agency for Electronic Communications and Postal Services (EKIP), possesses strong technical expertise in telecommunications and spectrum regulation but has shown little interest in expanding its remit to cover the domain of digital platforms.

> *"The Agency for Electronic Communications and Postal Services ... simply does not want to deal with this."*
> *– Goran Đurović, Director of the Media Center*

This reflects a broader structural limitation: while sectoral expertise exists in telecommunications, institutional mandates remain narrowly defined and do not yet extend to the systemic and cross-platform dimensions required under the DSA framework.

HUMAN CAPACITIES

Limited but emerging expertise

Interviews indicate that Montenegro's main candidate for the role of Digital Services Coordinator (DSC) – the Agency for Audiovisual Media Services (AMU) – has a basic understanding of the Digital Services Act but lacks the specialised staff required for its effective implementation. The novelty and complexity of the digital services field further exacerbate this capacity gap. Experts underline that without substantial investment in training and recruitment, AMU will struggle to perform core DSA functions such as algorithm auditing, systemic risk assessments, and the accreditation of trusted flaggers.

> *"The Agency at this moment has human potential... they have knowledge about the DSA and what needs to be done, but that does not mean they have a sufficient number of people, nor those who will tomorrow have to do the concrete tasks."*
> *– Goran Đurović, Director of the Media Center*

> *"These are new topics, relatively recent, so we cannot expect that the necessary expertise already exists. We have many young people who are willing to learn, but they definitely need experience and support."*
> *– Ružica Mišković, Head of the Working Group for Chapter 10*

Need for the EU engagement and knowledge transfer

Experts highlight that capacity-building efforts must be closely linked to EU cooperation and structured knowledge transfer. Strengthening institutional capacities will require sustained engagement with EU counterparts and peer institutions that have already operationalised the Digital Services Act (DSA).

> *"Without expertise from European colleagues who have already gone through this process, our progress will be limited."*
> *– Ružica Mišković, Head of the Working Group for Chapter 10*

Civil society and academia as under-utilised resources

Beyond regulators, CSOs and academia represent additional reservoirs of expertise, though their potential remains largely underused. While Montenegro's expert ecosystem is still narrow, it offers a foundation for participatory governance once the institutional framework matures.

> *"We have about five NGOs that have been active in the field of media so far... maybe two or three will take some role, but their capacities also need to be built. Through public debates and cooperation, I believe all actors will be included and interested, because it is in everyone's interest that this functions as required by the acts."*
> *– Goran Đurović, Director of the Media Center*

OPERATIONAL CAPACITIES

Necessary internal restructuring and risks

Montenegro's operational readiness remains constrained by administrative inertia and fragmented coordination. This cautious approach delays the internal restructuring and staffing processes that should precede formal legal designation, increasing the risk of institutional under-preparedness once the mandate for Digital Services Act (DSA) implementation is officially transferred.

> *"There are no talks yet... They are waiting for the law, because it would be premature for the Agency to reorganise itself before the official decision is made."*
> *– Goran Đurović, Director of the Media Center*

> *"There have been recurrent shifts of competences between ministries – for instance, the reassignment of e-commerce from one institution to another – which has repeatedly disrupted continuity and blurred accountability lines."*
> *– Ružica Mišković, Head of the Working Group for Chapter 10*

No implementation before EU integration

Substantial implementation of the Digital Services Act (DSA) framework is unlikely to take place before Montenegro's accession to the European Union. This transitional logic suggests that the coming years will primarily focus on institutional development rather than enforcement, with tangible results expected only upon membership.

> *"I don't believe that before 2028 there will be full or major application of the rules. Until then, it will mostly be about preparatory steps – education, equipment, organisational preconditions."*
> *– Goran Đurović, Director of the Media Center*

FINANCIAL CAPACITIES

New mandate requires a new funding model

The Agency for Audiovisual Media Services (AMU) is currently financed through fees collected from media and operators – a structure unsuited to the expanded mandate envisaged under the Digital Services Act (DSA). The new responsibilities will require dedicated budget lines and predictable funding to support staffing, training, and the development of IT infrastructure. *"They are financed by fees from the media and operators. But when this new function is taken on, it will probably have to be financed by the state budget."*
– Goran Đurović, Director of the Media Center

> *"Capacity building is a continuous process under EU scrutiny, requiring stable long-term investment rather than ad-hoc allocations."*
> *– Ružica Mišković, Head of the Working Group for Chapter 10*

INSTITUTIONAL CAPACITIES FOR DIGITAL MARKET GOVERNANCE IN MONTENEGRO

Montenegro's preparedness for digital market governance remains at an early stage. Effective alignment with the Digital Markets Act (DMA) will require not only the adoption of new legislation but also a complete institutional redesign, including clearly designated coordination structures,

specialised staff, interoperable monitoring systems, and sustainable funding mechanisms. The current administrative model, characterised by fragmented competences and a reactive policy approach, is not sufficient to address the systemic and cross-border challenges posed by the DMA. Closing this gap will depend on strategic EU support, inter-ministerial coordination, and sustained investment in expertise and infrastructure.

Absence of debate about institutional capacities

At present, there is no publicly available information on Montenegro's preparedness to implement the Digital Markets Act (DMA). The lack of data underscores a fundamental challenge: the country's institutional capacities for digital market governance have not yet been mapped, discussed, or transparently documented. In practice, the findings identified for Serbia appear equally relevant for Montenegro. Experts note that the regulatory and enforcement challenges posed by the DMA are likely to be similar across Western Balkan jurisdictions, reflecting the shared institutional experience of competition authorities in the region.

DMA as a significant coordination and capacity challenge

Institutional discontinuities have complicated Montenegro's capacity to address the new digital-market rules. Interviews emphasised that the DMA represents a particularly significant challenge due to recent government reorganisations and shifting competences among ministries. Electronic commerce initially fell under the Ministry for Information Society and Telecommunications, which also prepared the current Law on Electronic Commerce. Following the dissolution of that ministry, responsibility was transferred to the Ministry of Public Administration. Later, through a government decree, oversight of electronic commerce was again reassigned, this time to the Ministry of Economic Development.

The institutional reshuffling has left Montenegro insufficiently prepared to assume responsibility for DMA coordination and enforcement. While the existence of the Law on Electronic Commerce meant that no immediate institutional response was required in previous years, the entry into force of the DMA introduces an entirely new regulatory framework that cannot be managed through existing structures alone. The Ministry of Economic Development, which currently holds the mandate, lacks the specialised expertise and administrative capacity needed to coordinate DMA implementation. This has created uncertainty over institutional leadership,

particularly regarding inter-ministerial coordination and compliance monitoring.

Overall, Montenegro's situation reveals two key risks: first, that frequent institutional reorganisations erode administrative continuity and weaken capacity; and second, that new EU digital legislation requires a proactive and well-coordinated governance response which national institutions are not yet equipped to provide.

INSTITUTIONAL CAPACITIES FOR AI GOVERNANCE IN MONTENEGRO

The institutional foundations for artificial intelligence (AI) governance remain at a very early stage. The country does not yet have a dedicated AI strategy, although one is reportedly under preparation and not expected to be adopted before 2026. In the absence of such a guiding framework, it is difficult to assess existing institutional capacities. No regulatory authority has been formally designated to oversee AI, and sectoral regulators have not yet begun developing specific competences in this field.

AI governance in Montenegro remains at a conceptual stage

The absence of systematic efforts to build technical expertise, develop human resources, and establish horizontal coordination mechanisms places the country behind its regional peers. At present, Montenegro remains in the preparatory phase, with debates about institutional design still largely conceptual rather than operational. Concrete progress will depend on the adoption of an AI strategy, which is expected to provide both the policy direction and institutional mandates necessary for governance capacities to emerge.

AI governance will require the creation of a new institutional structure

The primary challenge in establishing AI governance bodies stems from the current institutional and regulatory vacuum. The Artificial Intelligence Landscape Assessment (AILA) of Montenegro (UNDP, May 2025) notes that the country's institutional preparedness for ethical AI remains at an early stage of development. Mechanisms needed to ensure that AI actors are held accountable for system outcomes are largely absent, while frameworks for public oversight and citizens' rights to challenge algorithmic decisions

are described as "either lacking or underdeveloped". The AILA further emphasises that there is "minimal formal policy or infrastructure in place" to ensure accountability in the ethical deployment of AI. This means that, unlike sectors where existing regulators can be repurposed – as considered for DSA/DMA implementation – AI governance will require not merely the expansion of an existing body but the creation of an entirely new institutional framework for oversight.

Shortage of qualified experts capable of performing AI regulatory functions

The establishment and resourcing of any future AI oversight body in Montenegro faces significant human-capital and financial constraints. Even if a political decision were made to designate an existing institution – such as the Agency for Personal Data Protection – that body would immediately encounter the challenge of attracting and retaining specialised technical expertise. As seen across the region, low public-sector salaries compared to the private IT industry represent a major obstacle. This makes it difficult to build multidisciplinary teams comprising data scientists, AI engineers, and ethics experts – all essential for performing functions such as certification and systemic risk assessments.

Risk of an under-resourced and purely nominal authority

The absence of dedicated funding and a comprehensive strategy to upskill or recruit specialised personnel exposes Montenegro to the risk that any newly mandated body may become an under-resourced and purely nominal authority, unable to credibly enforce complex AI regulations within its jurisdiction.

COMPARATIVE DISCUSSION

This comparative analysis examined institutional capacities for digital governance in Croatia, Serbia, and Montenegro under the new European digital regulatory framework. It assessed institutional, technical, human, operational, and financial dimensions across the DSA, DMA and AIA, drawing on expert interviews to explore how political contexts, administrative legacies, and resource constraints affect alignment with the EU governance model. Croatia, as an EU Member State, demonstrates a more advanced and structured system, whereas Serbia and Montenegro, both candidate countries, continue to face fragmentation, politicisation, and limited capacity. Despite differing levels of institutional maturity, all three cases reveal persistent systemic weaknesses, capture risks, and gaps in expertise that hinder effective implementation.

In Croatia, institutional capacities for digital governance reflect both structural maturity and persistent weaknesses in independence and expertise. Political and business capture continue to shape the governance environment. Despite formal autonomy, regulatory agencies remain influenced by the ruling political elite and major private actors. Political appointments, weakened ethical safeguards, and the erosion of conflict-of-interest oversight have undermined institutional credibility. Yet digital regulation appears less exposed to capture risks, largely due to the absence of very large online platforms or gatekeepers with systemic economic importance.

Within this context, the principal challenges relate to institutional performance and human resources. The Agency for Personal Data Protection (AZOP) faces constraints stemming from its legal status and limited technical capacity, which affect its ability to enforce forthcoming AI Act obligations and current data protection rules in relation to AI systems. The Croatian Regulatory Authority for Network Industries (HAKOM) benefits from operational stability and relative independence but encounters increasing coordination demands under the DSA. The Croatian Competition Agency (AZTN) remains largely passive with no proactive enforcement.

While participation in the EU cooperation network and the use of shared technical tools partly compensate for expertise gaps, recruiting and retaining skilled IT and AI professionals remains a key challenge. Agencies

acknowledge the need for multidisciplinary teams, continuous training, and active participation in EU working groups as essential mechanisms for learning and adaptation.

Financially, Croatian agencies operate within stable budgetary frameworks: funding levels are generally sufficient, but civil-service salary structures limit their ability to attract and retain qualified IT staff. Overall, Croatia's institutions are broadly aligned with EU requirements. Although they remain constrained by entrenched patterns of political influence, it is expected that such constraints will be less evident in the enforcement of the analysed digital regulation.

Serbia's institutional landscape presents a complex picture, marked by delayed convergence, entrenched politicisation, and fragmented expertise. The Regulatory Authority for Electronic Media (REM) exemplifies these challenges: formally endowed with broad powers but operationally passive and politically dependent. It lacks both the technical infrastructure and professional profiles required for DSA implementation, and its administrative model resembles that of a traditional state authority rather than a modern, analytically driven regulator.

The Regulatory Agency for Electronic Communications and Postal Services (RATEL) in Serbia possesses stronger technical capacities in telecommunications, yet its mandate is sector-limited and disconnected from the broader platform governance framework. The domestic IT community, although highly skilled and globally integrated, operates outside public governance structures and remains commercially rather than institutionally oriented.

Human capacities across Serbian regulators are limited. Public agencies rely largely on administrative staff rather than interdisciplinary experts, maintain weak cooperation with academia, and show little interest in knowledge-based decision-making. Operationally, coordination between regulators is poor, procedures are outdated, and authoritarian political tendencies further undermine institutional independence. The institutional model for DSA implementation remains contested, with no clear decision on whether to strengthen existing bodies or establish a new one.

Similar patterns extend to DMA and AIA governance in Serbia. The Commission for the Protection of Competition (CPC) holds formal authority but functions within an outdated legal and educational

environment that produces few experts in digital markets or data-driven regulation. Individual professional enthusiasm exists but is unsupported by institutional mechanisms or sustained investment. AI governance remains at a conceptual stage: a working group has been formed, but no law or institutional framework has yet been adopted. Experts differ on whether to decentralise enforcement across sectoral regulators or expand the mandate of the Commissioner for Information of Public Importance and Personal Data Protection.

Across all domains, Serbia's regulatory agencies face traditional budgetary limits, political interference presented as efficiency reform, and growing pressure from overlapping mandates. Financial resources are not the principal constraint; rather, the absence of strategic prioritisation, qualified human capital, and institutional integrity continues to hinder effective governance.

Montenegro presents a case of formal alignment coupled with functional fragility. The country has provisionally closed Chapter 10 on the Information Society and Media, achieving legislative harmonisation with EU directives on audiovisual media, electronic communications, and information security. However, practical implementation remains uneven.

The DSA process is institutionally anchored within the Ministry of Culture and Media, which coordinates with the Agency for Audiovisual Media Services (AMU), the most likely candidate for the role of Digital Services Coordinator. In Montenegro, AMU demonstrates basic awareness of the DSA's requirements but lacks the personnel, technical systems, and analytical capacity needed for enforcement. The Agency for Electronic Communications and Postal Services (EKIP) retains strong technical expertise but shows little interest in extending its mandate to platform governance.

Human capacities remain limited, though younger staff and new institutional units suggest emerging potential. Both experts and officials emphasise the need for structured EU engagement and knowledge transfer to build competence. Civil society and academia, while underutilised, could become important partners in this process.

Operationally, institutional restructuring is necessary but has been delayed pending formal legal mandates. Montenegro's integration trajectory

suggests that substantial enforcement is unlikely before EU accession, with the current phase focused on education and institutional preparation.

Financially, AMU's existing fee-based funding model is unsuitable for new digital obligations, requiring direct support from the state budget. In the areas of DMA and AI governance, institutional capacity is even more limited. The Ministry of Economic Development holds nominal responsibility for market regulation but lacks the expertise and internal coherence to coordinate DMA implementation. AI governance remains at a conceptual stage, awaiting the adoption of a national strategy and the establishment of new oversight bodies. The shortage of qualified experts and persistent underfunding create a substantial risk that any new regulatory structure will remain under-resourced and nominal in practice.

Taken together, these findings reveal a clear hierarchy of institutional maturity. Croatia's integration into EU governance structures and access to capacity-building mechanisms have produced measurable, though uneven and belated, progress toward effective digital regulation. Serbia's regulatory landscape remains characterised by political dependence, institutional inertia, and fragmented technical expertise, while Montenegro's efforts are largely preparatory and closely tied to the EU integration process.

Across all three countries, human capacity remains the decisive bottleneck: recruitment, retention, and continuous professional training are critical yet constrained by low salaries and rigid administrative rules. Operational procedures are improving incrementally, but coordination – both horizontal among national institutions and vertical with EU counterparts – remains limited. Financial resources, though sometimes formally sufficient, are often inaccessible for sustained skill-building and technological investment.

In conclusion, while formal harmonisation with EU rules continues to advance, the transition from legal alignment to functional governance depends on strengthening institutional autonomy, developing expertise, and fostering inter-institutional cooperation to ensure credible and resilient digital regulation across the region.

WESTERN BALKANS TOWARDS THE EUROPEAN DIGITAL SINGLE MARKET – INSTITUTIONAL BRIDGE TO HUMAN RIGHTS APPROACH IN DIGITAL GOVERNANCE

The study has shown that digital regulation is both horizontally and vertically anchored to the institutions of the European Union, which makes alignment with EU digital policies a significant challenge for countries operating outside the EU framework. Building on this finding, this chapter examines the broader political, legal, and institutional conditions that shape the region's prospects for closer integration with the European Digital Single Market (DSM) as an institutional bridge to European digital governance. Its aim is to clarify what is realistically achievable in the short and medium term by identifying actionable steps that can strengthen regulatory convergence, enhance governance standards, and support a more coherent digital policy environment.

The chapter therefore maps the key obstacles and opportunities that define the current landscape, from treaty asymmetries and limited institutional capacities to emerging instruments such as the Growth Plan for the Western Balkans. It outlines potential pathways through which the region could gradually align with core DSM frameworks and highlights where policy efforts would have the greatest impact. By setting out feasible entry points,

the chapter seeks to inform a practical roadmap for digital integration that reinforces both institutional credibility and long-term accession dynamics.

DIGITAL SINGLE MARKET

Serving as the digital arm of the EU's Single Market, the Digital Single Market (DSM) brings together twenty-seven Member States under a shared set of rules, regulations, and a common legal framework. Through the DSM, the European Union harnesses the collective weight of its 450-million-strong consumer base to establish enforceable standards for digital platforms, online services, and emerging technologies.

> *"The EU uses the weight of its market to compel large companies (Big Tech) ... to comply with basic rules."*
> *– Đorđe Bojović, Parliamentary Advisor*

In essence, the DSM's primary objective is to remove digital barriers within the Union, ensuring the free movement of online goods, services, and data. It aims to create a fair and competitive environment where the protection of fundamental rights, market fairness, and innovation can coexist. As such, the DSM is both an economic integration project and a normative governance model, combining competitiveness with a rights-based approach to digital regulation.

The European Union began developing digital market regulation in the 2010s, recognising the growing need for clear and consistent rules governing this part of the economy. A major milestone came with the adoption of the General Data Protection Regulation (GDPR) in 2016.

> *"This marked the beginning of a new wave of comprehensive digital legislative packages adopted at the EU level, designed to curb the dominance of Big Tech and introduce a rules-based framework for digital markets. This dynamic is commonly referred to as the Brussels Effect, the EU's ability to project its rules and regulatory demands beyond its borders, influencing not only other states but also companies and various non-state actors across the global digital economy."*
> *– Đorđe Bojović, Parliamentary Advisor*

Building on this foundation, the EU launched several major legislative initiatives, including the Digital Services Act (DSA), Digital Markets Act (DMA), and Artificial Intelligence Act (AIA). However, by 2024, the Union's digital regulatory momentum had slowed. Many significant legislative "files" that were in the pipeline for adoption were put on hold, as the EU and the United States entered a broader regulatory and market confrontation over the future of global digital governance.

DSM GOVERNANCE: BETWEEN SIMPLIFICATION AND IMPLEMENTATION

At present, the governance of the Digital Single Market is shaped by two prevailing schools of thought. The first reflects the general orientation of the new European Commission, whose mandate began only at the end of last year.

> *"The key word here is simplification. This reflects a trend towards 'unpacking' or revising existing digital legislative files, in an effort to deregulate certain aspects of EU digital law. A concrete example is the GDPR, which has now been in force for eight years and has generated a substantial body of case law and established legal practice. The EU is now considering ways to ease or reinterpret some of these rules, largely in response to transatlantic market pressures. This approach, however, leads onto a slippery slope, as it risks undermining well-established norms and legal precedents."*
> *– Đorđe Bojović, Parliamentary Advisor*

Debates around simplification are increasingly intertwined with the American discourse on digital rights, particularly in relation to freedom of expression, the limits of content moderation, and standards of acceptable online behaviour. These debates are likely to shape the future course of EU digital policy.

The second school of thought argues not for simplification, but for the stricter implementation of existing legislation. The DSA and DMA have only recently entered into force, while the GDPR remains relatively new in legal and institutional terms.

"Unsurprisingly, there are loopholes, inconsistencies, and enforcement gaps. Thus, alongside the push for simplification, there is an opposing vision that calls for stronger implementation, targeted identification of weak enforcement areas, and a tightening of the regulatory framework to ensure that market rules operate more effectively and consistently across all Member States."
– Đorđe Bojović, Parliamentary Advisor

THE EFFECT OF THE "BRUSSELS EFFECT"

The Brussels Effect describes the European Union's capacity to regulate global markets through the extraterritorial impact of its internal rules. By leveraging the scale and attractiveness of its single market, the EU effectively compels third-country actors – whether states, corporations, or other entities – to align with its regulatory standards. This influence extends from relatively straightforward domains, such as consumer protection and product safety, to highly complex areas, including the governance of digital ecosystems and the regulation of online markets and the digital economy.

On the other hand, several countries maintain differentiated contractual relationships with the EU. The closest circle comprises those that have, to varying degrees, transposed EU legislation and enjoy selected benefits of the acquis, depending on the legal basis of their relationship with the Union.

"At present, there are about ten such countries in this 'first ring', each at a different stage of the EU enlargement process – from negotiating members to candidates and potential candidates. The nature of each relationship depends on the type of agreement concluded with the Union. For instance, Serbia's Stabilisation and Association Agreement (SAA), signed in the early 2000s, was designed with a clear objective: to facilitate the integration of the Western Balkans – the post-Yugoslav states plus Albania – into the EU. As a result, the SAA is a comparatively less ambitious and less detailed instrument, essentially conveying a single message: 'You must align with the EU acquis, adopt EU standards, and once you are in, you will have full access.'"
– Đorđe Bojović, Parliamentary Advisor

By contrast, Ukraine, Moldova, and Georgia have concluded Deep and Comprehensive Free Trade Agreements (DCFTAs) with the European Union.

> *"These are far more ambitious frameworks, designed for countries that may not become full members in the near term but are nonetheless granted extensive regulatory alignment. Serbia's SAA, for instance, is roughly twenty pages long, whereas Ukraine's DCFTA exceeds over one hundred and twenty pages, detailing every area of cooperation and alignment."*
> *– Đorđe Bojović, Parliamentary Advisor*

In practice, this means that certain benefits of the Digital Single Market – such as roaming-free communication – can already be extended to Ukraine, Georgia, and Moldova, as their legal frameworks explicitly provide for such arrangements. Serbia, by contrast, lacks a legal basis for comparable measures: its SAA grants full access only upon accession. This situation highlights the asymmetry of contractual frameworks and the limitations of the EU's regulatory projection toward third countries.

There are two distinct layers of EU influence: the first is the global Brussels Effect, which shapes markets and norms worldwide; the second encompasses the "first ring" of candidate and associated countries, where the degree of access to the Single Market depends on the depth and structure of each country's contractual relationship with the Union.

Within this second layer, certain policy areas are relatively easy to implement and could serve as early integration steps – for example, roaming, electronic signatures, or data interoperability.

> *"More complex areas, such as the DSA and DMA, require much deeper legal and institutional alignment. The European Commission is currently exploring ways to replicate the Ukrainian model across all enlargement countries. The logic is simple: if a citizen in Kyiv can call someone in Berlin without roaming charges, why shouldn't a person in Belgrade be able to do the same? The main challenge lies in identifying the legal foundation that would make this possible, as current treaties*

provide none."
– Đorđe Bojović, Parliamentary Advisor

The European Union can grant varying degrees of access to the Single Market – and, by extension, to the Digital Single Market – depending on the legal framework governing its relationship with a given country. Consequently, while Serbia and Ukraine may appear politically comparable, their respective contractual arrangements generate markedly different legal outcomes and levels of market integration.

The application of EU instruments beyond its borders can be observed in recent cases from Romania, Moldova, and Georgia. In Romania, the Constitutional Court annulled the first round of presidential elections after uncovering evidence of foreign interference identified through digital forensic analysis on platforms such as TikTok and X (Twitter), which revealed algorithmic manipulation and irregular online financing. Although the EU's involvement in this case was indirect, it nonetheless demonstrated how domestic legal mechanisms, when guided by EU standards, can contribute to safeguarding electoral integrity.

In Moldova, the EU's involvement was primarily political rather than technical, following allegations of vote-buying and interference during a simultaneous referendum on EU membership and a presidential election. Here, too, digital evidence played a role; however, unlike in Romania, there were no direct legal consequences for the platforms involved, such as TikTok. This case has been described as a "lesson learned": while the EU successfully identified the problem, it lacked the legal instruments to hold digital actors accountable.

These examples illustrate both the potential and limits of the EU's influence. While the Union can project its standards and indirectly shape outcomes beyond its borders, the absence of a formal legal mandate constrains effective enforcement. Nevertheless, its digital policy instruments remain essential tools for extending democratic and regulatory norms across the broader European neighborhood.

WESTERN BALKANS INTEGRATION INTO THE DSM – WHOSE BENEFIT?

The integration of the Western Balkans into the European Digital Single Market (DSM) offers reciprocal benefits, though the motivations and expected outcomes differ on each side. From the EU's perspective, expanding the DSM represents a strategic investment in security and stability.

> *"The Western Balkans are an enclave surrounded by EU territory, a kind of digital Wild West with no EU regulation."*
> *– Đorđe Bojović, Parliamentary Advisor*

This largely unregulated digital space enables various actors to develop business and data ecosystems that may later spill over into the EU market, generating legal, cybersecurity, and reputational risks. Integrating the region into the DSM would therefore help close the regulatory gap between EU Member States and their immediate neighbourhood, thereby reducing exposure to systemic and cross-border vulnerabilities.

The economic rationale for integration is equally compelling. The Western Balkans constitute an adjacent market of over 17 million people with a rapidly expanding ICT sector. Removing regulatory barriers would facilitate cross-border digital trade, investment, and innovation, while extending the EU's normative and technological reach. Moreover, the inclusion of candidate countries within EU digital frameworks would enhance the Union's global competitiveness vis-à-vis the United States and China, reinforcing its normative "digital sovereignty."

For Western Balkan states, integration into the Digital Single Market (DSM) would generate benefits across the economic, consumer, and governance spheres. From an economic and business perspective, alignment with DSM rules would open access to a predictable regulatory environment and the world's largest digital market.

> *"Such access would help reduce barriers to trade and unlock growth for domestic IT and service sectors."*
> *– Đorđe Bojović, Parliamentary Advisor*

Equally important are the implications for citizens and consumers. Integration would extend EU-level rights and protections to people in the region.

> *"Citizens in the Western Balkans would enjoy the same protections that EU citizens have against Big Tech."*
> *– Đorđe Bojović, Parliamentary Advisor*

Under current conditions, countries such as Serbia lack the leverage to enforce obligations on global platforms. A telling example is Booking.com, which refuses to share data with Serbia's tax authority, claiming the market share is negligible. Within the DSM framework, however, platforms like Booking or Airbnb would be legally required to cooperate with national institutions under EU directives – transforming today's asymmetry of power into rule-based accountability.

Finally, in terms of institutional and political alignment, early adoption of DSM standards would strengthen the region's track record of regulatory compliance – a key criterion in the EU accession process.

> *"Earlier harmonisation means earlier proof of credibility."*
> *– Đorđe Bojović, Parliamentary Advisor*

This would not only support accession prospects but also promote higher governance standards, transparency, and institutional maturity across the digital sector.

HOW TO ACHIEVE INTEGRATION: LEGAL, INSTITUTIONAL AND POLICY PATHWAYS

While the rationale for integrating the Western Balkans into the European Digital Single Market is compelling, the pathway toward that goal remains insufficiently defined. Existing legal frameworks, institutional capacities, and political priorities do not yet provide a concrete mechanism for participation. Nevertheless, a growing body of EU instruments – ranging from association agreements to the Growth Plan for the Western Balkans – is gradually laying the groundwork for partial and phased DSM integration.

The Legal Basis: Between Association and Deep Integration

The Western Balkans currently participate in the European integration process primarily through Stabilisation and Association Agreements (SAAs), signed in the early 2000s as political and economic pre-accession instruments. These agreements establish free trade zones and require legislative harmonisation with the EU acquis, yet they do not provide a legal basis for participation in the Digital Single Market.

> *"Our agreement is far less ambitious than, for example, Ukraine's or Georgia's, because it assumes full EU membership as the end point. It says: adopt the acquis, and we'll see you in the Union."*
> *– Đorđe Bojović, Parliamentary Advisor*

By contrast, Ukraine, Moldova, and Georgia operate under Deep and Comprehensive Free Trade Agreements (DCFTAs). These frameworks explicitly extend selected DSM benefits to non-member states, including the elimination of roaming charges, recognition of electronic signatures, and regulatory convergence in areas such as e-commerce and telecommunications.

> *"Their agreements list everything, in exhaustive detail: what can be done, how it is applied, and what rights it entails."*
> *– Đorđe Bojović, Parliamentary Advisor*

This asymmetry reveals the legal gap that currently prevents the Western Balkans from formal participation in the Digital Single Market (DSM). Several approaches could help bridge this gap.

One option would be to amend existing SAAs through a dedicated digital annex, specifying which DSM provisions apply to candidate countries. This model would preserve the existing treaty framework while introducing a legal mechanism for gradual digital integration.

Another possibility involves adopting a stand-alone EU-only agreement.

> *"A legal initiative signed solely by the European Commission, not requiring ratification by all Member*

States, could enable faster and more flexible integration."
– Đorđe Bojović, Parliamentary Advisor

Such an instrument could take the form of a Commission Decision or EU-only Memorandum of Understanding, similar to arrangements used for the Energy Community Treaty or Transport Community Treaty.

A third approach would rely on sectoral pilot models, extending selected DSM chapters – such as roaming, electronic identification (eIDAS), or cybersecurity – to the region through secondary legislation or delegated acts. This modular integration method would mirror earlier steps taken in energy and transport cooperation.

These models share a common purpose, to operationalise participation in the DSM without requiring full EU membership, thereby creating an incremental bridge between association and accession.

Institutional Preconditions: Building Capacity Before Access

Legal approximation alone is not sufficient. Effective participation in the DSM institutional maturity and regulatory competence, both of which remain underdeveloped across much of the Western Balkans.

"There must be institutions capable of supervising and implementing the rules of the digital market. That's the precondition."
– Đorđe Bojović, Parliamentary Advisor

The institutional dimension of DSM alignment involves building the administrative and regulatory infrastructure necessary to implement EU digital legislation effectively. This includes designating and adequately equipping competent authorities responsible for digital services, competition, and AI oversight – such as Digital Services Coordinators, national competition bodies, and market surveillance authorities. It also requires strengthening data protection agencies, which in many Western Balkan countries function as de facto anchors of digital governance. Finally, achieving meaningful alignment depends on the establishment of inter-ministerial coordination mechanisms to manage horizontal regulatory domains such as cybersecurity, e-commerce, and platform accountability.

These tasks are consistent with the EU's Growth Plan for the Western Balkans (2023), which identifies "digital convergence with the EU Single Market" as a strategic priority and allocates dedicated funding to strengthen administrative capacities. The Growth Plan introduces conditional access to selected EU programmes and markets, contingent upon the fulfilment of legislative and institutional benchmarks. In this sense, it serves as both a financial and procedural entry point for gradual DSM integration.

> *"The Growth Plan is an excellent foundation. It comes with fresh cash to strengthen legal and institutional capacities in candidate countries."*
> *– Đorđe Bojović, Parliamentary Advisor*

In practice, the Plan could support twinning projects, technical assistance, and training programmes for regulatory bodies in areas such as systemic risk assessment, content-moderation oversight, and algorithmic transparency – all of which constitute essential prerequisites for credible DSM participation.

Policy Instruments and Roadmaps

To operationalise integration, three policy tracks can be distinguished:

To operationalise DSM integration, three complementary policy tracks can be distinguished:

1. Growth Plan-driven integration

This track would leverage Growth Plan funding to establish pilot frameworks for DSM participation – for example, shared digital identity systems (aligned with eIDAS 2.0), joint cybersecurity initiatives under NIS 2, or interoperable electronic communications standards. These pilots could serve as proof-of-concept mechanisms for broader integration.

2. Regional approach under enlargement logic

The EU could treat DSM integration as part of a combined enlargement package covering the Western Balkans, Ukraine, and Moldova. This comparative framing would create a political incentive for equal treatment, reinforcing the EU's credibility and coherence in its neighbourhood policy. It would also allow the European Commission to act under a unified enlargement rationale, avoiding the need for separate bilateral frameworks.

3. Structured roadmap for DSM accession

A pragmatic roadmap would identify short-, medium-, and long-term milestones for each country:

- Short-term: legal approximation of DSA, DMA, and AIA provisions; establishment of coordinating bodies; pilot participation in digital infrastructure initiatives (e.g., EU4Digital).
- Medium-term: implementation of interoperability frameworks; participation in EU-level digital risk assessment mechanisms; integration into cross-border e-commerce systems.
- Long-term: full regulatory participation in DSM sectors, including platform oversight and cross-border digital services governance.

Such a roadmap would formalise a gradualist approach to DSM enlargement, linking measurable progress to tangible benefits for participating states.

Political Feasibility and Regional Dynamics

The political calculus across the Western Balkans remains uneven. Montenegro and Albania, having opened or provisionally closed most EU negotiation chapters, may perceive limited added value in temporary DSM arrangements. By contrast, Serbia, North Macedonia, and Bosnia and Herzegovina, whose accession processes are advancing more slowly, could benefit from early DSM participation – both as a credibility boost and as a functional bridge toward eventual EU membership.

This asymmetry makes regional coordination essential. A joint Western Balkan initiative, potentially framed within the Common Regional Market Action Plan (2025–2028), could provide the EU with a single interlocutor and help reduce administrative fragmentation.

> *"The goal should be to advocate for the region as a whole, not individual countries, and to present a concise, evidence-based brief that clearly shows the mutual benefits and*

concrete steps."
– Đorđe Bojović, Parliamentary Advisor

Toward a New Model of "Digital Enlargement"

Ultimately, Digital Single Market integration is more than a technical process or regulatory exercise – it constitutes a new model of digital enlargement. By linking institutional convergence with rights-based governance, the European Union can project its standards and values beyond formal borders, reinforcing the "Brussels Effect" as both a normative and a functional mechanism. For the Western Balkans, early participation in the DSM would accelerate their evolution from rule-takers to rule-makers in the emerging European digital ecosystem.

Experts interviewed for the study:

Snježana Milivojević, Retired Professor of Public Opinion and Media Studies, University of Belgrade, Serbia

Bogdan Gecić, Competition lawyer, Serbia

Tijana Žunić Marić, IT lawyer, Serbia

Slobodan Marković, Digital Policy Advisor, UNDP Serbia

Ružica Mišković, Head of the Working Group for Chapter 10 – Information Society and Media, Government of Montenegro

Goran Đurović, Director of the Media Center and Member of the Working Group on media and digital legislation, Montenegro

HAKOM employee 1 (DSA implementation), Croatia

HAKOM employee 2 (DSA implementation), Croatia

AZOP employee, Croatia

Investigative journalist, Croatia

Đorđe Bojović, Parliamentary Advisor, European Parliament

SHARE
FOUNDATION

2025