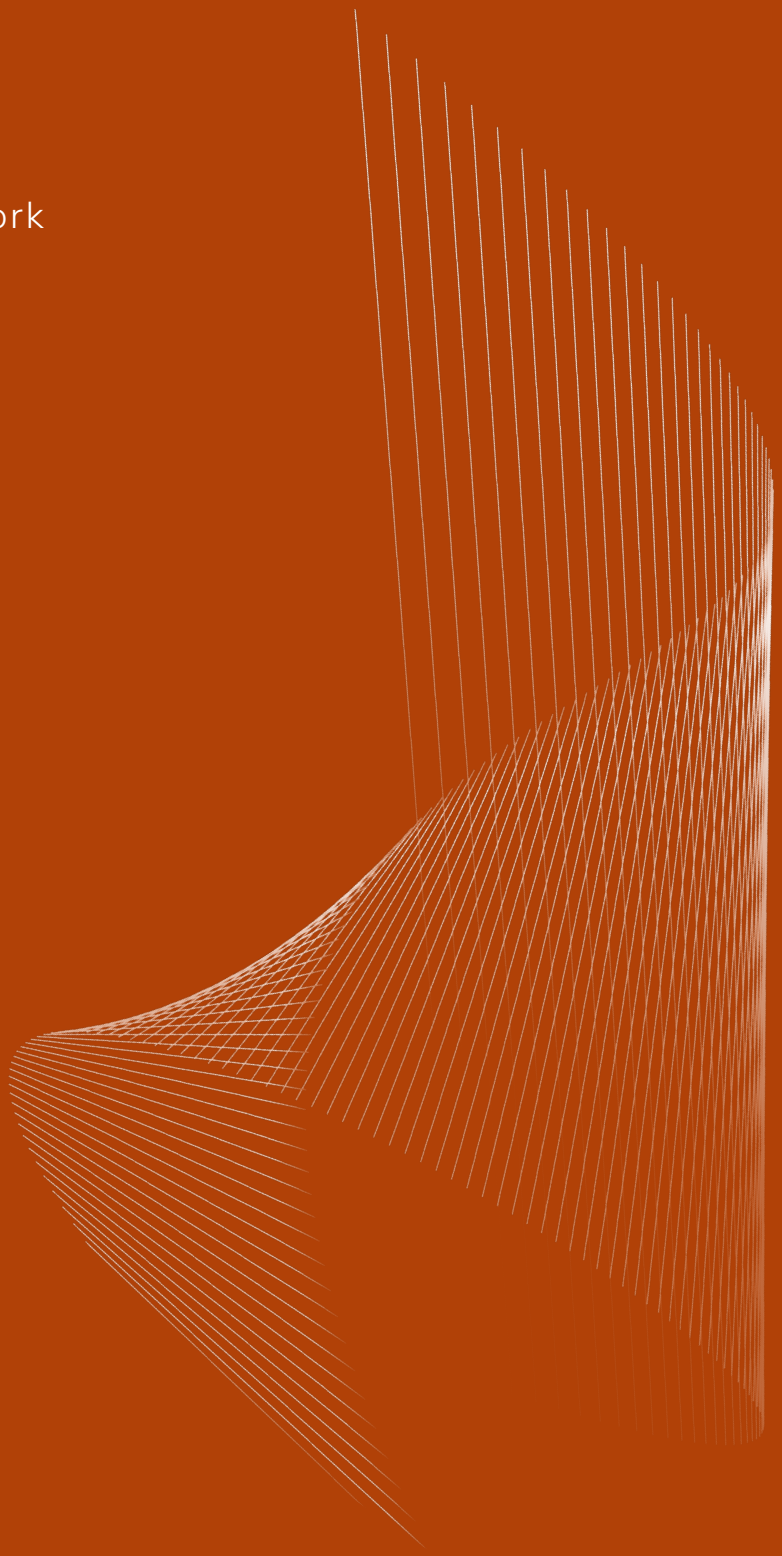
DSA, DMA, AIA
AND WESTERN BALKANS

Normative Foundation
Enforcement Mechanisms
and Institutional Framework

STUDY



SHARE FOUNDATION

IMPRESSUM

Executive Editors: Danilo Krivokapić & Andrej Petrovski

Editor: Snežana Bajčeta

Authors: Jelena Adamović, Mila Bajić, Snežana Bajčeta, Bojan Perkov, Tijana Stevanović

Peer review: Ella Jakubowska (EDRi), Maida Ćulahović (Zašto Ne?), Eliška Pírková (Access Now), Christoph Schmon (EFF)

Regional partners: SCiDEV (Albania), Zašto Ne? (Bosnia and Herzegovina), Youth Initiative for Human Rights Kosovo - YIHR KS (Kosovo), 35mm (Montenegro), Institute of Communication Studies (North Macedonia)

The publication is supported by the Open Society Foundation Western Balkans.

Proofreading: Milica Jovanović

Design: Olivia Solis Villaverde

Publisher: SHARE Foundation

2024

CONTENTS

EXECUTIVE SUMMARY

This multidisciplinary, multi-stage study is a comprehensive analysis of key systemic Acts that radically change the regulatory approach of the European Union regarding its digital ecosystem – Digital Services Act (DSA), Digital Markets Act (DMA), and Artificial Intelligence Act (AIA). The shift towards systemic regulation concerning digital services, digital markets, and artificial intelligence represents a significant milestone in establishing the normative, enforcement, and institutional foundation for the European Digital Single Market. For the Western Balkan countries aspiring to European Union membership, this regulatory change is particularly significant, as their digital challenges are even more complex and their existing legislations are significantly outdated, inconsistent, and inadequate for the systemic regulation of digital ecosystems.

The aim of this analysis was first to "unpack" the normative and value structure as well as to map out the key rules and institutions envisaged by these Acts, in order to comparatively assess the situation in the Western Balkan countries. Specifically, national legislations were examined in terms of the presence of the same or similar rules within a wide array of diverse documents that directly or indirectly relate to these areas. It was found that the alignment of previous generations of regulations allowed for the existence of individual regulations to a certain extent within a broadly diversified regulatory base. However, their legal strength in achieving a fair, secure, responsible, and transparent digital environment is very limited. Nevertheless, significant specificities and differences were also identified.

Based on the exploratory research which included mapping of key concepts, basic rules prescribed by DSA, DMA, and AIA, and key institutions participating in their implementation, we have mapped the normative foundation embedded in the specific value structure of these three Acts. According to our findings, accountability is the central value of the DSA, supported by reliability, transparency, safety, horizontality, and accessibility. The key value of the DMA is market democratisation, operationalised through transparency, accountability, interoperability, mobility, and demonopolisation/

deconcentration. Preventing and addressing adverse effects of AI has been identified as the central value pillar of the AIA, while the value structure of this Act is built on transparency, harm prevention and reduction, and oversight.

Furthermore, a total of 72 rules have been identified as profoundly changing the regulation of digital services, digital markets, and artificial intelligence in the EU towards a systemic approach (DSA – 30, DMA – 23, AIA – 19). These rules are categorised and explained according to the key contribution of the rule to the individual value of these three Acts.

Finally, the institutional framework analysis mapped groups of institutions involved in enforcing new regulations, as well as their respective roles.

DSA implementation includes a multilevel institutional design comprising: EU institutions (European Commission, European Board for Digital Services, Court of Justice of the European Union); Member States institutions (Digital Services Coordinator, Certified out-of-court dispute settlement bodies); an institutional corpus of intermediary services providers (Points of Contacts, Legal Representatives, Compliance Officers); a group of experts and auditors (Trusted flaggers, Independent auditors); institutional roles designated to recipients of services, consumers, and traders.

The institutional framework of DMA is similarly structured: EU institutions (European Commission, European Data Protection Supervisor, European Data Protection Board, European Competition Network), member states institutions (National courts, National competent authorities); experts (Digital Markets Advisory Committee, High-level group for the Digital Markets Act) and a group of business and end users (gatekeepers, business users, end users).

According to the mapping of the AIA relevant institutions, the multistakeholder approach is also applied in this institutional framework: EU institutions (European Artificial Intelligence Office (AI Office, European AI Board, Advisory forum, Scientific panel of independent experts, European Data Protection Supervisor); Member States institutions (National competent authorities - market surveillance authorities, National competent authorities - notifying authorities, Conformity assessment bodies - notified bodies,

National authorities protecting fundamental rights, National data protection supervisory authorities); AI industry institutional corpus (Providers of high-risk AI systems, Deployers of high-risk AI systems, Providers of GPAI models, Providers and deployers of certain AI systems, Importers of high-risk AI systems, Distributors of high-risk AI systems); institutional roles designated to individuals.

The assessment of current regulations in Western Balkan countries from a comparative perspective showed that there are some corresponding rules regarding digital services and digital markets within national legislations, while AI-related legislation is absent in most countries. However, they lag behind new EU regulations for several reasons. Firstly, the identified rules are mostly from previous generations, which do not provide adequate responses to current challenges and are limited in scope. Even though certain rules are identified as those that comprehensively or precisely cover the regulated matter, their drawback compared to the EU regulations is that they are diversified across various pieces and types of legislation, preventing a systemic regulatory approach. The following is a brief overview of the situation by country.

ALBANIA

Legal rules regarding digital services are spread across seven different documents. Compared to the values and rules outlined in the DSA, the majority of Albanian regulations need improvement, particularly in terms of increasing the transparency of digital service providers. While reliability, safety, horizontality, and accessibility are supported by a broader range of rules, many of these are either partial or outdated.

Regarding digital markets in Albania, there is a set of generic rules found primarily in e-commerce and e-communications laws, in addition to various general or sector-specific laws (a total of nine pieces of legislation). However, these rules are quite limited in terms of creating an accountable, transparent, deconcentrated, interoperable digital market, compared to the norms set by the DMA.

Currently, there are no specific regulations addressing the use of AI systems in Albania.

BOSNIA AND HERZEGOVINA

There are two main references for DSA-related rules in Bosnia and Herzegovina. The first comes from the transposition of the E-Commerce Directive, which applies to information society services in general. The second set of rules addresses specific types of intermediary service providers, under the framework for electronic communications. Most of these rules contribute to the reliability, horizontality, and accessibility of digital services. However, transparency mechanisms are still underdeveloped.

Existing digital market rules in Bosnia and Herzegovina are covered by sector-specific legislation focused on consumer protection and personal data protection. Additionally, Competition Law provides a more general framework for this area. Rules from seven distinct documents contribute to the democratisation of the digital market. However, gaps remain regarding transparency and interoperability.

There are no specific regulations addressing the use of AI systems in Bosnia and Herzegovina. Some AI-related values are regulated only from the perspective of personal data protection.

KOSOVO

A range of seven regulation pieces mostly indirectly or partially are related to issues covered by the DSA. Their differentiation across diverse laws calls for a more coherent and systemic approach regarding all values.

More attention is needed for digital markets. There are no legal rules regulating matters covered by the DMA. From this perspective, it is worth mentioning that there is a draft law on consumer protection that might be a relevant starting point in this field.

Apart from participating in the European Union's Digital Europe Programme, which provides strategic grants including in the area of artificial intelligence (AI), there is no regulation regarding AI in Kosovo.

MONTENEGRO

A set of rules related to digital services was identified in eight regulatory pieces. Most of these norms are outdated, as they do not provide relevant legal responses to contemporary challenges, especially in terms of the transparency of digital service providers.

Currently, there is no explicit law addressing digital market matters in Montenegro. Competition in general is covered by the Competition Protection Law. Nevertheless, an upcoming law announced in the field of digital assets may potentially incorporate certain aspects of DMA regulations.

Regarding AI, there are currently no laws or regulations that deal with AI systems use in Montenegro.

NORTH MACEDONIA

Within a patchwork of twelve different documents, including laws, bylaws, and other legal acts, digital services are recognised to some extent in North Macedonia. While specific rules do contribute to transparency and reliability, North Macedonia highlights the need for a more coherent and focused approach to digital services regulation.

Regarding digital markets, North Macedonia's legal framework only partially addresses this matter and has a limited capacity to establish a transparent, accountable, interoperable, and mobile digital market.

Some personal data protection regulations in North Macedonia might be relevant to certain aspects of AI use. But, there are currently no specific laws or other type of regulations addressing the use of AI systems.

SERBIA

The starting point for DSA-related regulations in Serbia is the Law on Electronic Commerce, which prescribes the conditions, rules, and obligations for information society services. Additionally, the Law on Electronic Media includes a small set of rules concerning video-sharing platform services. According to the analysis of these rules, transparency is a key norm that must be incorporated into future regulations.

There are no specific laws regulating DMA issues in Serbia. A few general and sectoral laws cover some of these issues from various angles, including the Law on Electronic Commerce, the Trade Law, the Law on Protection of Competition, the Personal Data Protection Law, and the Consumer Protection Law. But, this diversified structure makes it difficult to fully align with EU values in this area.

Compared to neighbouring countries, Serbia has made the most progress in regulating AI systems. There are mechanisms in place that contribute to oversight, transparency, and harm prevention in AI. AI Strategy, followed by Action Plan, Ethical Guidelines, and a working group established with the mandate to prepare a draft law on AI systems, indicate certain regulatory efforts in Serbia.

CONTEXTUAL BACKGROUND

As part of their integration process, the Western Balkans societies (Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, Serbia - WB6) have developed close connections with the European Union, not only in terms of economic relations, but also by incorporating key EU legal standards in their national legislative frameworks. The digital environment of the Western Balkans has seen the alignment of numerous laws with the EU acquis over the years, with the most recent example being the General Data Protection Regulation (GDPR) which influenced changes to personal data protection laws throughout the region.[1]

Despite these changes impacting the national legislative frameworks for information society and digital services, the weak rule of law and fragile democratic institutions hinder the establishment of the necessary standards and impede significant progress toward EU accession. Political instability, as seen in Serbia and Bosnia and Herzegovina, hampers the advancement of digital services and markets both in legislative and practical terms. This instability is caused by frequent elections, social turmoil, and systemic challenges regarding human rights and the rule of law.

A broader geopolitical picture, especially since February 2022 and the full-scale invasion of Ukraine by Russian forces, shows that balancing between interests of major regional and global powers has added another layer of complexity to EU-Western Balkans relations. Some countries, such as North Macedonia, Montenegro, or Albania, opted for a closer political alignment with key EU Member States like Germany or France in foreign and security policy. On the other hand, Serbia's refusal to impose sanctions on the Russian Federation and align its foreign policy with that of the Union, as well as numerous challenges in the normalisation process with Kosovo facilitated by the EU, make it very difficult to build long-term plans for stable economic development and further integration with the Union.

1 See: N. Ružić, "Nationalising the General Data Protection Regulation in Western Balkan", Regional Law Review, 2021, DOI: https://doi.org/10.18485/iup_rlrc.2021.2.ch19

Numerous risks arise out of political, social, and economic instability, bringing the digital environment at a very sensitive crossroads. Benefits that may arise for a safer and more prosperous digital ecosystem are uncertain and easily overshadowed by authoritarian-like uses of advanced technologies, leading to a dangerous path where interests of actors such as Russia and China may exploit the unstable situation in the region. Influence operations and the spread of propaganda exacerbated by digital tools such as social media platforms add to the weaponization of the information sphere, particularly in countries with a low level of digital literacy and divisive media scene.

On the other hand, the overwhelming power wielded by the biggest technology companies has only risen in the past years. With the popularisation and growing reliance on the internet, consumers and users have been subject to certain decisions they might not agree with or fully understand. Either way, these decisions are often made far away from them and without consultation with the general public and stakeholders, including digital rights organisations, who hold adequate expertise. Mis- and disinformation, synthetic content, non-transparent advertising models that profit from the abuse of people's personal data, and questionable data retention and distribution practices have changed the way people socialise, shop, and how they access, receive, and consume information in the modern age. Additionally, Big Tech companies currently hold the most power in the AI industry. Their position needs to be challenged given that there are rules and mechanisms that should be applied in order to curb their influence and reach. While the US still seems hesitant about regulating tech, the EU has decidedly set itself on a path to change the ways in which people and tech interact in the digital space. Given the undeniable role of the internet in today's world, the creation and implementation of the EU legislative framework demonstrates a way to reimagine the power of technology companies in terms of user protection and rights.

This study will cover three major legislative instruments introduced by the EU - Digital Services Act (DSA), the Digital Markets Act (DMA) and the Artificial Intelligence Act (AIA) - which exemplify the need for a new approach to regulating digital markets, services, and products. The logic behind these legislative texts, as explored in this study, demonstrates that previous legal rules were not adequately suited to address new societal risks and human

rights violations arising from recent developments in the global digital market and in the area of artificial intelligence. Western Balkan countries are currently exposed to these risks but lack legislative tools to address them. Additionally, with many structural issues still unresolved, these societies have often neglected the digital environment and failed to recognise its potential partly due to the lack of political will. However, a political window of opportunity is now opening, as evidenced by Bosnia and Herzegovina's accession negotiations.[2] This opportunity may be limited, depending on the willingness to reform digital governance in the Western Balkans and the overall stability across Europe, particularly in the EU's Eastern neighbourhood. DSA, DMA, and AIA provide a potential framework for shaping national legislations in Western Balkan countries. These frameworks need to be closely considered and analysed to prepare for the Digital Single Market,[3] thus facilitating smoother integration into the broader European digital ecosystem.

2 M.G. Jones, "European Union leaders approve opening accession talks with Bosnia and Herzegovina", Euronews, 21 March 2024, https://www.euronews.com/my-europe/2024/03/21/european-union-leaders-approve-opening-accession-talks-with-bosnia-and-herzegovina

3 European Commission, "A Digital Single Market Strategy for Europe", COM(2015) 192 final, 6 May 2015

METHODOLOGY

This analysis focuses on legislative acts that regulate key aspects of the European Digital Single Market: digital services - Digital Services Act; digital markets - Digital Markets Act; and artificial intelligence - Artificial Intelligence Act. The aim is to explain the normative/value basis, enforcement mechanisms, and institutional frameworks of these three Acts.

Additionally, this analysis seeks to offer a comparative perspective from the Western Balkans perspective. Therefore, the second aim is to map the existing basic rules related to digital services, digital markets, and artificial intelligence in Serbia, Bosnia and Herzegovina, Montenegro, North Macedonia, Albania, and Kosovo. The mapping aims to identify regulatory gaps in comparison to new EU regulations, according to the central values that constitute foundational pillars of the three EU Acts. Also, it assesses how the regulatory frameworks in the Western Balkans countries address the challenges in the digital ecosystem that DSA, DMA, and AIA aim to regulate comprehensively and systemically in the EU.

Therefore, the exploratory phase of the research was focused on mapping:

1. Basic *terms* and *concepts* introduced by DSA-DMA-AIA into the EU regulatory framework.

2. Basic *rules* prescribed by DSA-DMA-AIA.

3. ***Institutions*** participating in the implementation of the DSA-DMA-AIA regulatory mechanisms.

Based on exploratory findings, the normative analysis examines the value structure of the three Acts, seeking to delineate the key normative pillars underlying the new regulation. Methodologically, the value structure is derived by inductively assigning each rule one or more values to which the rule should contribute through its application in the digital ecosystem.

Subsequently, a comparative method is employed to analyse the presence of DSA-DMA-AIA-related rules within the legislation of Western Balkan countries, using both quantitative and qualitative approaches. This segment of analysis encompasses a wide range of laws and soft law instruments (laws, bylaws, draft laws, rules, strategies, decisions, guidelines, etc.) that address digital services, digital markets, and artificial intelligence in the WB6. The objective is to assess the current state - scope, level, and type of regulation concerning these issues across Western Balkan countries. In this regard, we examined whether rules mapped in the DSA, DMA, and AIA exist within the Western Balkans legislations, and moreover, whether they comprehensively/precisely or partially/incidentally correspond to the rules prescribed by these three Acts. We aim to identify not only gaps but also aspects of the regulation that could be further developed and improved in line with EU standards. Additionally, the study assesses the scope and diversity of existing rules across various pieces of regulations and their capacity to address contemporary digital challenges. Also, the study examines comparatively the extent to which existing rules in the Western Balkan countries contribute to achieving one or several values that were considered as pillars of these three Acts, highlighting areas where further rule development and mechanisms are most crucial.

The analysis thoroughly dissects the overall institutional framework of DSA-DMA-AIA, elucidating the institutional roles of all actors involved in their implementation, from users to the European Commission.

Finally, for the purpose of this study we consider the levels of rights protections under the DSA, DMA, and AIA to be of a higher standard compared to the fragmented legislative framework in the Western Balkans. However, particularly for the AIA, this does not imply that these laws are without serious issues of their own. Nevertheless, a thorough critical examination of the DSA, DMA, and AIA is beyond the scope of this study.

DSA-DMA-AIA: NORMATIVE FOUNDATION

The DSA, DMA, and AIA represent central legislative acts that normatively redefine the digital ecosystem in the EU. By introducing new rules, these Acts aim to guide the digital landscape towards achieving key values envisioned in their principles. This chapter explains the core values embedded within the DSA, DMA, and AIA, which we regard as the key normative pillars of this regulatory framework. These values address the central challenges of the digital ecosystem, with some being identified across multiple Acts, while others are specific to particular regulatory domains.

DIGITAL SERVICES ACT

Contemporary digital challenges demand a comprehensive normative response that transcends mere individual accountability, sectoral regulation, or isolated responses to digital rights infringement. Normatively, the Digital Services Act is grounded in accountability, encompassing a diverse range of public values and forms of accountability across a spectrum of stakeholders. It addresses human rights violations and societal risks that affect society as a whole, instead of individual pieces of digital content, goods, or services. It focuses on the structural factors that erode digital rights and democratic values in the EU, which simultaneously constitute the foundation of major digital players' business operations. The institutional shift from content-centric to structural solutions focusing on systems and processes deployed by private actors is based on a systemic approach, introducing due diligence obligations and formalisation of digital content moderation while aligning with existing legal frameworks within the EU and its Member States.

VALUE PILLARS OF DSA

ACCOUNTABILITY


RELIABILITY


TRANSPARENCY


SAFETY


HORIZONTALITY


ACCESSIBILITY

FORMALISATION OF DIGITAL CONTENT MODERATION

AND

DUE DILIGENCE OBLIGATIONS

RELIABILITY

Online ecosystem is facing numerous challenges, which are increasingly difficult to address on a case by case basis. Issues such as hate speech, disinformation, deceptive design, and blurred boundaries between information and advertising, among others, require a comprehensive approach that could eventually lead to a healthier ecosystem, one that would also be significantly more reliable. This is particularly important considering that an increasing number of people are engaging in trade, informing or educating themselves, and participating in cultural and social activities within the digital environment. Hence, reliability stands out as a significant meta-value embedded across several articles of the DSA.

The DSA intends to enable reliability on three levels:

- Content - Free from illegal content, with promotional kind accurately distinguished from informational.
- Structure - Non-suggestive technological infrastructure and accurate, comprehensive content of contracts.
- Ecosystem - Compliance with the law.

A multidimensional approach to reliability empowers recipients on one hand, while on the other introduces punitive measures for providers and users who violate the rules operationalised from this concept.

TRANSPARENCY

One of the fundamental sources of power for intermediary service providers lies in their opaque business practices. The average user is typically uninformed about the platform's content moderation policies or how its recommender system operates, while researchers often face rejection when seeking access to data. Additionally, public authorities are often unaware of the social, political, or systemic impacts caused by these players, and they may lack the necessary legal tools to safeguard the public interest within a profit-driven platform ecosystem. To address these challenges, the EU is incorporating legally mandated transparency as one of the normative pillars of the DSA, ensuring intermediary service providers being transparent towards:

- Recipients
- Authorities
- Independent stakeholders (researchers, academia, civil society sector, etc.).

The DSA provides transparency of:

- Terms and conditions
- Recommending systems
- Content moderation decisions
- Structure of the content moderation policies and practices
- Auditing and compliance.

Transparency provisions are essential to ensure that recipients are fully informed about the rules and infrastructure governing the European digital ecosystem. These provisions not only facilitate awareness but also enable robust monitoring, assessment, and mitigation of systemic risks by authorities and relevant stakeholders.

SAFETY

The contemporary digital landscape is marked by a multitude of challenges that can endanger individuals, their rights, dignity, and even their lives. There have been countless examples of online harassment, data breaches, and content manipulation on social media platforms, with minors being particularly vulnerable. On the other hand, the overall digital environment is structurally prone to various risks, which manifest in the systematic erosion of rights and freedoms, democracy, and European public values.

Establishing a safe online environment stands out as one of the key goals of the DSA, which aims to provide safety for:

- Individuals, particularly minors
- Digital ecosystem.

HORIZONTALITY

The DSA integrates the principle of horizontality into its regulatory framework, affecting both the regulatory mechanism itself and consequently the appearance and structure of the broader digital ecosystem. While the digital space had been initially conceived as inclusive, open, and equal for all participants, power imbalances quickly emerged. Recipients found themselves increasingly excluded from decision-making mechanisms, while simultaneously serving as a key resource for the growth, expansion, and profit of major players. This Act establishes a framework that protects individuals and empowers them to engage in the regulatory mechanisms of digital services and the broader digital ecosystem.

ACCESSIBILITY

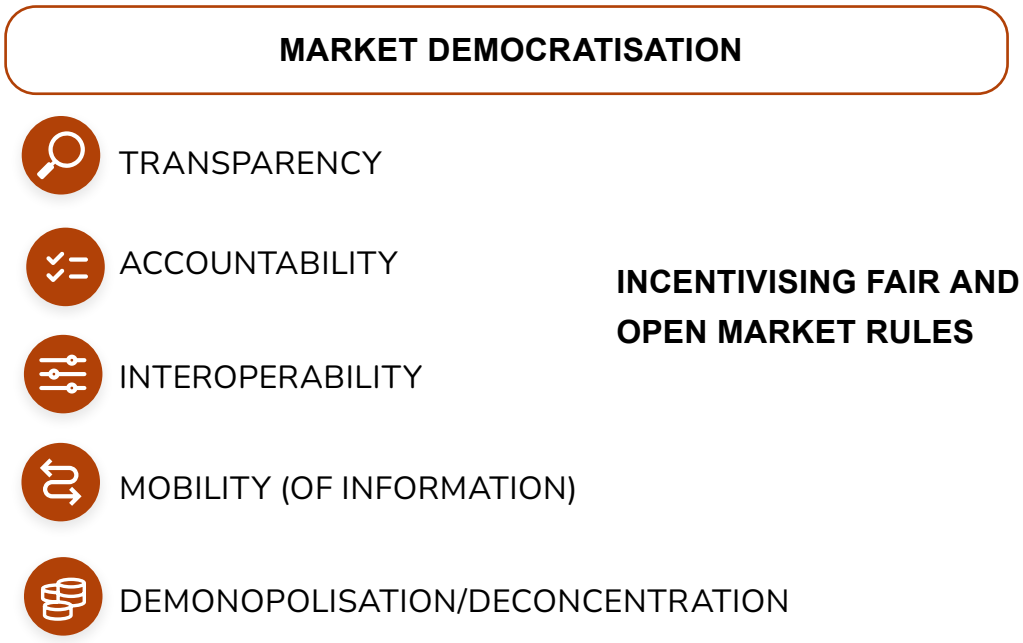
The closure and inaccessibility of Big Tech pose a significant barrier to their responsiveness to recipients, stakeholders, or authorities. Their policies and business models often remain opaque to the public and regulators. Moreover, they constitute a disruptive factor in the consistent, thorough, and appropriate monitoring and evaluation of their work, roles, and societal impact. The DSA

establishes a framework for institutionalised accessibility for all stakeholders by setting up key contact points for both institutions and citizens. In particular, very large online platforms and very large search engines (VLOPSEs), responsible for assessing compliance and systemic risks, are specifically available for external monitoring and research activities.

DIGITAL MARKETS ACT

In order to adequately regulate the digital market, it is paramount to establish responsible and fair market practices. While the DSA is more closely concerned with systemic platform accountability that directly benefits end users, the DMA aims to address the business-side of operations more closely. The majority of provisions in the Act are oriented towards incentivising fair and open market rules with the broader aim of market democratisation. Gatekeepers, the biggest tech companies that in one way or the other have a monopoly on a certain aspect of the digital market, are in a privileged position of power when compared with other smaller companies that might also be competing to offer their services to end users. Because of this, the DMA sets out to scrutinise the many advantages that gatekeepers might enjoy that have been brought on by often opaque practices.

VALUE PILLARS OF DMA



TRANSPARENCY

One of the main issues in businesses operating in the digital economy is the lack of transparency in user data handling and overall business decision-making. Particularly when it comes to big tech companies or gatekeepers (as defined by the DMA), they often leverage this information in order to prioritise their own products and services and thus contribute to the monopolisation of the overall digital market. In an effort to tackle such opaque practices, the European Union's Digital Markets Act aims to address the issue of transparency in a number of key ways:

- Auditing and compliance by gatekeepers.
- Fair and unrestricted access to third-party content on gatekeepers' services.
- Verification and audits of advertising practices by gatekeepers.

Gatekeepers rely on non-transparent techniques especially in their advertising practices, which allow them an abundance of user data through which they are able to precisely target potential audiences for their products and services. Coupled with their track record of self-preferencing, this allows companies to drive traffic and users to their own offers without explicitly removing or deplatforming their competitors.

Implementing such systems of accountability will put pressure on gatekeepers to reevaluate their practices in order to comply with the DMA. In instances of non-compliance, member states will have clearer avenues through which they will be able to take action against the companies.

ACCOUNTABILITY

The insistence on gatekeepers' accountability in regards to end users is another crucial part of the push for the democratisation of the digital market. Accountability for these companies is rooted in two main points:

- Responsibility to end users regarding the handling of their data.
- Responsibility to competitors regarding the offering of services and products.

Gatekeepers have specific responsibilities towards users and competitors. They are obligated to clearly obtain the users' consent for collecting, processing, and distributing their data. This includes the right for users to withdraw consent at any time and to transfer their data to another company's services. For competitors, gatekeepers must avoid self-preferencing and ensure that all service providers have equitable access to promote their products and services on their platforms.

The accountability principle is crucial for maintaining free and open market practices and ensuring a level playing field for all actors involved. In cases of non-compliance with accountability standards, the Commission can fine the gatekeepers to enforce future compliance, particularly when end users' rights are violated by unfair competition and data handling practices.

INTEROPERABILITY

Since the DMA is primarily concerned with regulating the market, interoperability is a crucial aspect of gatekeepers' compliance. Interoperability allows end users to choose which services they wish to use rather than being coerced into using a gatekeepers' service by default. Offering centralised services is becoming an increasingly common practice of large digital platforms and allows them to cultivate an unfair competition. Therefore, the DMA aims to incentivise smaller platforms and end users to curate their use of services through imposing strict mechanisms to avoid gatekeepers' attempts at cornering the market. This would mean that all services, including instant messaging, online retail product preferencing, and operating systems will have to be available to all under the same rules. Ultimately, the key benefit of interoperability under the DMA is to facilitate the partial or complete departure of end users from a service. This means that interoperability aims to allow users to switch away from dominant service providers rather than being bound by the convenience of gatekeepers. Failure to comply will be seen as interference with open market practices and will result in harsh financial sanctions.

MOBILITY (OF INFORMATION)

The free flow of information is necessary in order to cultivate a democratic digital market and economy and therefore presents another key pillar of the DMA. Gatekeepers will be obligated to allow end users more agency over how their information is being utilised as well as the right to revoke their consent for processing of their personal data. This is particularly important for end users in instances where they wish to change the services they use.

This principle also enhances conditions for smaller businesses as it allows them to have continuous and real-time access to their user data in order to assess their products and services that are being hosted on gatekeepers' core platform services. Usage data allows businesses to make improvements to their services and to enhance their user experience.

DEMONOPOLISATION/DECONCENTRATION

As previously defined, demonopolising digital market relies on transparent and continuous access to data and communication between gatekeepers, smaller businesses, and end users. Decentralising data and clarifying opaque business practices enhance the ability of businesses to offer their products and services to end users without engaging in price fixing to compete with gatekeepers.

Market deconcentration also makes it easier for end users to choose between various service providers without additional barriers that discourage pluralism. This ensures that gatekeepers cannot prioritise the use of their own services through convoluted and complicated conditions that would otherwise deter users from selecting alternative providers.

ARTIFICIAL INTELLIGENCE ACT

Recognising challenges posed by various implementations of artificial intelligence on socio-political processes, the EU considered introducing overarching legislation. This regulatory instrument would address the

practical use, development, and potential effects of AI on citizens in the European Union. The text of the Artificial Intelligence Act (AIA) was agreed upon by Member States and the European Parliament in late 2023, and in March 2024 the MEPs finally confirmed the passage of this long-awaited regulation. In May 2024, the Council of the European Union gave the final green light[4] for the AI Act, which at the time of writing is yet to be published in the Official Journal of the EU and enter into force.

As Recital 1 of the AIA[5] states (italic emphasis added), its purpose is to:

- Improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems) in the Union, in accordance with Union values.
- Promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of fundamental rights of the European Union (the 'Charter'), including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union.
- Support innovation.

The main intention of the AI Act is to prevent and address adverse effects of the use of AI, using the cross-cutting approach of ex-ante management of risks for society and human rights stemming from AI development and implementation.

4 Council of the European Union, "Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI", 21 May 2024, https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/

5 AI Act, Recital 1, adopted text available at: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf. As part of the preparation for the publication of the AI Act in the Official Journal of the EU, please note that a corrigendum version of the text was published on 19 April 2024: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf

It is important to note that the overarching goal of the legislation can be broken down into three areas, which are transparency, harm prevention and reduction, and oversight.

VALUE PILLARS OF AIA

PREVENTING AND ADDRESSING ADVERSE EFFECTS OF AI

- TRANSPARENCY
- HARM PREVENTION AND REDUCTION
- OVERSIGHT

EX-ANTE MANAGEMENT OF RISKS STEMMING FROM AI

TRANSPARENCY

AI systems are often referred to as "black boxes"[6] in the sense that they generate content based on user input (e.g. "create an image of a blue flower in a grass field") or express an outcome (e.g. "there is a high chance that person X will commit a crime") in a way for which there is no clear basis or explanation. While perfect transparency of AI's inner workings is unattainable due to the complexity of processes like machine learning, the AI Act aims to shed a light not only on how AI models and systems are developed, but also on their use in a more practical sense. This is particularly important when it comes to general-purpose AI models, often referred to as "foundation" models, since

6 S. Bagchi, "What is a black box? A computer scientist explains what it means when the inner workings of AIs are hidden", The Conversation, 22 May 2023, https://theconversation.com/what-is-a-black-box-a-computer-scientist-explains-what-it-means-when-the-inner-workings-of-ais-are-hidden-203888

they can be used in many different areas and for a variety of AI-powered tasks, which makes them a very versatile and powerful tool.[7]

On the other hand, the development of AI is pushed by commercial and political interests, where transparency isn't quite on the agenda. Powerful companies from outside Europe, predominantly US and Chinese tech giants, are investing enormous resources to gain a foothold in this very lucrative area. Similarly, there are numerous new actors developing advanced models, such as OpenAI and their widely used GPT large language model, and emerging as key players in the market, often backed by Big Tech money, as is the case with OpenAI and Anthropic.

Both private and government actors are increasingly using various AI systems, ranging from law enforcement and employment to financial services, but without transparency as to what these systems are and how they are used there can be no accountability. For highly invasive uses in the context of human rights, such as real-time remote biometric identification in public spaces, the principles of AI Act emphasise the importance of maintaining a track record to assess the necessity and proportionality of deploying such a system and to identify abuses. However, considering the technological and political context surrounding remote biometric identification, it is unlikely that any safeguard can fully prevent human rights abuses by such intrusive systems. Also, the transparency requirements for remote biometric identification systems are set at quite a low level by the AI Act, bringing the actual transparency for this use case into serious doubt.

Achieving transparency of AI models and systems, as well as their applications, can be further broken down into several sub-values:

» Openness and proactiveness: Reporting of serious incidents, technical documentation for high-risk AI systems, transparency obligations for generative AI, registering high-risk AI systems in a special EU database (unfortunately only parts of this database will be public and law

7 E. Jones, "Explainer: What is a foundation model?", Ada Lovelace Institute, 17 July 2023, https://www.adalovelaceinstitute.org/resource/foundation-models-explainer/

enforcement and migration uses are exempted), providing information on training data, etc.

- Traceability and explainability: Making humans aware that they are interacting with an AI system, informing deployers of the capabilities and limitations of the AI system and affected persons about their rights.
- Inclusiveness and multi-stakeholder approach: Using institutions to engage with the expert community, civil society, academia, industry.
- Track-record: Regular statistics (i.e. annual report) on the use of systems, e.g. for remote biometric identification systems.

HARM PREVENTION AND REDUCTION

Even though promises of AI are usually rife with optimism, it is like any other technology and has a darker, more negative side. We are already seeing the impact of these tools on human rights, most notably in implementing facial recognition video-surveillance in public spaces, infrastructure to support the "smart cities", and other similar tools such as predictive policing algorithms. Minoritised and historically excluded communities, like ethnic minorities, people of colour, and people on the move, are constantly being surveilled and controlled, often without legal recourse or any opportunity to evade very intrusive technologies enabled by AI.[8] In addition, once these infrastructures and technologies are installed in our public spaces, it is very difficult to reverse the decision and go back to the old ways without radical moves. Contrary to the popular narrative that AI will allow humanity to reap enormous benefits, the risks and negative consequences of the use of AI systems are already affecting numerous people worldwide. These impacts are particularly pronounced concerning the right of privacy, freedom of assembly and association, freedom of movement, the right to equality, and related human rights.

Although one of the aims of the AIA was to reduce harms caused by the use of AI, it generally follows an approach that does not grasp the complexity

8 R. Ingram, "Hikvision still sells Uyghur-tracking surveillance cameras, and they use NVIDIA chips", The China Project, 17 August 2023, https://thechinaproject.com/2023/08/17/hikvision-still-sells-uyghur-tracking-surveillance-cameras-and-they-use-nvidia-chips/

of human rights abuses facilitated by AI systems. The AIA introduces a risk-based assessment model for potential effects a certain AI system can produce.

The risk-based approach in the AI Act is problematic for providing comprehensive human rights protection, unlike a "rights-based" approach that empowers individuals and offers them robust protections across the board - a good example is the EU's General Data Protection Regulation (GDPR). Limiting obligations and protection measures to predefined high-risk AI applications, and focusing on processes, documentation, and assessments to prevent abstract harm, falls short of granting individuals specific rights and protections concerning how AI systems affect them. This approach does not seem to live up to the promise initially imagined.[9]

The provisions of the AIA prescribe that systems which are deemed as most problematic to individuals and society are explicitly forbidden, while most of the obligations, including those pertaining to risk management are prescribed for high-risk AI systems. However, it is important to note that these systems were designated by the lawmakers, who mostly ignored the advice of human rights experts in the process. In addition, providers of general-purpose AI models deemed to have systemic risks given their high impact capabilities will also face increased scrutiny, which will be explained further in the section on regulatory mechanisms.

When it comes to the application of AI, it's not only outcomes stemming from risks that are of concern, but also their design and development. In that sense, there are numerous risks pertaining to abuse of systems by external malicious actors. This leads us to the situation that AI systems need to be built with cybersecurity in mind in order to be resilient to various external influences that can greatly impact the system's security and outputs.

Harm prevention and reduction is meant to be an important component the AI Act, presenting significant challenges during implementation:

9 See: D. Leufer, F. Hidvegi, "The Pitfalls of the European Union's Risk-Based Approach to Digital Rulemaking", 71 UCLA L. Rev. Disc. 156 (2024), p. 160, https://www.uclalawreview.org/the-pitfalls-of-the-european-unions-risk-based-approach-to-digital-rulemaking/

- Efficient risk analysis and management: As a risk-based legislation, AI Act sets up management of risks associated with the AI systems as one of the key obligations.
- Responsibility along the value chain: various levels of obligations for developers, deployers, distributors, and importers as key actors in placing AI systems on the EU market or putting them into service, with particular emphasis on the developers of general-purpose AI models.
- Robust design: AI systems need to be designed in line with cybersecurity and data protection standards and resilient against attempts to alter their use, outputs, or performance.
- Continuous compliance: High-risk AI systems must fulfil all requirements throughout their lifecycle, i.e. from the moment they are first used until they are decommissioned, have post-market monitoring systems and plans, etc.

However, it should be considered whether the AI Act will actually succeed in reducing and preventing harm under its current framework, given that it is practically a product safety legislation, which effectively replicates rules for safety of physical products in the EU (the corresponding Directives and Regulations are listed in Annex I) which are not primarily suited for concepts such as AI. The focus on a product safety framework, coupled with the already problematic risk-based regulatory approach, does not fully encompass all challenges of the use of AI having an adverse effect on individuals, in particular for law enforcement purposes. Finally, enabling the use of AI and innovation in this field are also one of the key intentions of the AI Act, which is a more industry-favoured direction rather than one focused on reducing harm.

OVERSIGHT

In an "automated society"[10] an increasing number of social processes and outcomes affecting people, especially those in vulnerable and disadvantaged social positions, are turned over to technological solutions. In fact, there can never be a completely viable technological solution to deeper social

10 F. Chiusi, "Automating Society Report 2020", AlgorithmWatch, https://automating-society.algorithmwatch.org/

problems, such as inequality or abuse of power, and automated-decision making has often been presented as an ideal, unbiased and unmistakable solution to numerous issues our societies face. Without adequate human control mechanisms and oversight of how these advanced systems are used in practice, those who employ AI systems cannot be held accountable for the consequences stemming from the use of these systems, which are growing more powerful.

AI systems will always produce a small degree of errors, no matter how high their accuracy rates are during validation and testing, because they are trained on imperfect data and inputs and applied in real-world scenarios where there are numerous circumstances which can affect their outputs. However small these errors may be in terms of the amount of information processed and number of requests, they can produce serious legal consequences for people, like wrongful arrests or denials of welfare benefits. Taking into account the power imbalances created not only by technology but also structural societal issues, the use of advanced AI systems without proper oversight mechanisms and legal boundaries will only deepen the current divides (digital, social, economic, etc.) instead of contributing to a fairer society, with more equity between various social groups.

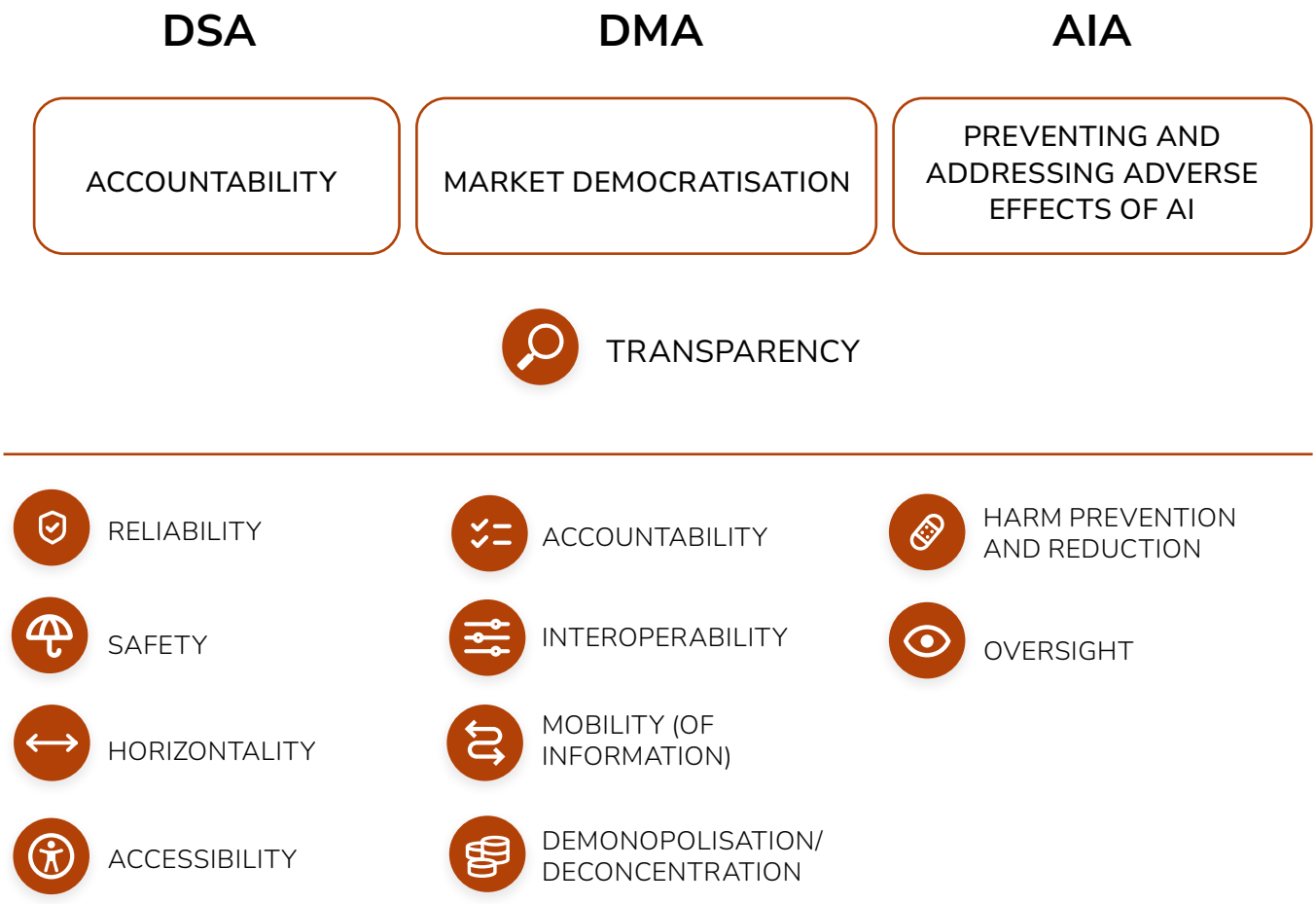
Finally, oversight includes varying levels of human and institutional scrutiny and interventions when it comes to development and use of AI systems:

- Judicial/administrative oversight: An oversight component when it comes to the use of remote biometric identification systems, but since it also enables administrative bodies (which can for example be police administrative units) to decide on such invasive measures, even retrospectively, it raises the doubt in terms of effectiveness of such oversight.
- Quality assurance: Providers of high-risk AI systems are obliged to put a quality management system in place, including techniques, procedures, and systematic actions to be used for the development, quality control, and quality assurance of the system.

» Human oversight: High-risk AI systems should be designed and developed in a way that they can effectively be overseen by natural persons.

» Redress: Natural persons have a right to explanation of individual decision-making if they believe that they have been negatively affected by a high-risk AI system, and both natural and legal persons can submit complaints regarding infringements of the AI Act.

Normative foundation of DSA-DMA-AIA regulation



DSA-DMA-AIA: ENFORCEMENT MECHANISMS

Prior to the DSA, the primary mechanism regulating digital services was the Directive 2000/31/EC (Directive on electronic commerce). The DSA adopts the Directive's definition of information society service as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services' and further clarifies that the regulation particularly applies to providers of intermediary services (intermediary services providers, ISPs), those offering 'mere conduit',[11] 'caching',[12] and 'hosting'[13] services on the digital market.

DSA addresses the entire spectrum of digital services offered to citizens across the EU, irrespective of where the company's headquarters are located or which country the company is established in. However, the obligations and responsibilities of digital service providers vary based on the scope of their users, the nature of their content moderation, structural intervention and influence they can exert in public space through their intermediation. Based on risks and obligations they bear, these are differentiated into four groups: very large online platforms and very large online search engines (VLOPSEs), online platforms (marketplaces, app stores, collaborative economy or social media platforms),[14] hosting services, cashing services, and intermediary services offering network infrastructure. On the other hand, beneficiaries of

11 Mere conduit services refer to enabling access to and transmission of information in a communication network, without any intervention regarding the initiation of the transmission process, modification of the content, or selection of potential recipients of the services (e.g., internet service providers).

12 Caching services offer automatic and temporary storage of information in a communication network, solely for the purpose of more efficient transmission of information to other service recipients upon their request (e.g., clouds).

13 Hosting services involve the storage of information obtained at the request of and by the service recipient, with no intervention in the content by the service provider (e.g., web hosting).

14 Within hosting services, online platforms are notable for their ability not only to store information upon request but also to disseminate it to the public, potentially making it accessible to everyone. Among these, very large online platforms and search engines (VLOPSEs) bear the highest level of accountability, with 45 million monthly active users, comprising 10% of the EU population (e.g., YouTube, Facebook, TikTok, Amazon Store, Google Search, etc.)

DSA rules are online content users, be it consumers or smaller platforms or start-ups, as well as recipients of the services.

One of the main goals of DMA is to address competition and fair market issues in EU digital markets. To that aim, it introduces the category of gatekeepers who are the main obligors of the law. It also introduces the notion of "core platform services" (CPS) that these gatekeepers provide and that are subject to regulation. CPS are specifically defined in DMA and include, for example, search engines, social networking, operating systems, web browsers, cloud computing, etc. The company that provides any CPS would be qualified as a gatekeeper when it reaches profit and user numbers thresholds. The main beneficiaries of the DMA to whom gatekeepers must enable certain rights are either business users or end users-natural persons who are practically consumers.

The DMA is structured in such a way that gatekeepers' obligations are regulated in three Articles, depending on their nature. The logic of the enforcement rules is that the gatekeeper must first implement the measures required for their business practices to be compliant with these three Articles and must be able to demonstrate such compliance. This is to be done via annual reports that they send to the European Commission with explanation of the measures they undertook. The non-confidential version of the report must be publicly available.

The AI Act is a piece of legislation that is different to DMA and DSA when it comes to its scope, as it should serve as an all-encompassing legal framework for artificial intelligence (at least for the foreseeable future). Its main regulatory unit is not artificial intelligence as such but AI systems and it intends to regulate those systems in a technology-neutral manner. It covers rules that are to be followed by several obligors throughout the whole lifecycle of AI systems, starting with development, going through the placement of the market as well as its continuous use in practice. The enforcement of the AI Act rules is risk based. Most harmful systems are outright forbidden and the ones that bear high risks must go through a detailed conformity assessment procedure. AI systems aimed at remote biometric identification are regulated

in greater detail, because of their potential for harmful effects that was also vocalised by civil society.

Main obligors are defined as providers and they are the ones who are developing the AI system. However, there are some obligations addressed to deployers, importers, or distributors. Large number of AI Act provisions regulate technical aspects of their obligations and conformity with required technical standards. Persons who will be subjected to AI system usage are protected directly and indirectly, for example via transparency or human rights assessment obligations.

DSA REGULATORY MECHANISM

Based on the mapping of the key DSA rules, a total of 27 basic rules are identified as foundational for the DSA enforcement. These rules are primarily procedural, designed to ensure that the EU's digital space is accountable, transparent, safe, reliable, horizontal, and accessible to all its citizens. Additionally, rules provide mechanisms for the effective implementation of both national laws of member states and corresponding EU laws, thereby contributing to the DSA's overarching goals. For example, while the DSA does not explicitly define what constitutes illegal content, it does outline procedures for reporting such content and specifies the consequences for its dissemination. Further in this chapter, rules and mechanisms are classified by value, illustrating how each rule contributes to a specific DSA objective[15].

15 Accountability, as a central and more general value within the DSA, has not been considered in detail from the perspective of corresponding rules and from a comparative perspective with the Western Balkans. However, it has been quantified since two identified rules address accountability in the digital environment in a broader sense, particularly concerning the existence of rules related to intermediary services, content moderation, and dispute settlement procedures.

RELIABILITY RULES AND MECHANISMS

Protection mechanism against misuse of digital services ecosystem

Online platform providers are required, under Article 23, to suspend services 'for a reasonable period of time' for users who consistently share illegal content, following a prior warning. Similarly, if a complainant repeatedly submits clearly baseless notifications or complaints, providers must suspend the processing of such notifications after issuing a warning. Suspension decisions should be made on a case-by-case basis, considering factors such as the volume and proportion of illegal content, the severity of abuse, and user intent. Additionally, providers must outline their abuse-detection criteria and suspension duration in their terms and conditions.

Non-manipulative interfaces rules

Under Article 25, online platform providers are prohibited from designing and operating interfaces that mislead or manipulate users, or hinder their capacity to make informed decisions freely while utilising the platform.

Clear labelling and information regarding advertisements

- Online platform providers displaying ads must ensure that recipients can identify essential details about each advertisement clearly, unambiguously, and in real-time, as stipulated in Article 26. This encompasses clarifying its nature, the represented entity and the payer, including accessible information of the targeting parameters employed for recipients, along with instructions on how to modify these parameters freely. Additionally, platforms must incorporate a functionality enabling users to flag commercial content, ensuring their effortless identification based on user declarations.
- VLOPs and VLOSEs that feature advertisements are required, as per Article 39, to establish and maintain a database accessible through their interfaces. This database should contain specified information about advertisements, available for the entire duration of an ad's display and up to one year following its last appearance, ensuring the exclusion of any personal recipient data. It must include essential details such as

the ad's content, presenting entity, payment entity (if different), display duration, and whether it was tailored for specific recipient groups, along with the parameters used for targeting or exclusion.

Reliability of contracting and trading

- Online platform providers that facilitate distance contracts for consumers are required, as outlined in Article 30, to collect essential regulated information from traders before granting them access to their platform services. Furthermore, they are mandated to verify this information. Should traders fail to furnish accurate and genuine information within the specified timeframe, the online marketplace must suspend their services until all requisite correct details are provided. In cases where the online platform provider denies a trader access to its services or suspends service provision, the trader retains the right to file a complaint.
- Online platform providers enabling consumers to enter into distance contracts are obligated, per Article 31, to design and structure their online interfaces to facilitate traders in submitting their information. To achieve this, these platforms must integrate essential functionalities into their online interfaces. Specifically, online platform providers must ensure that their online interface allows traders to provide: (i) clear and unambiguous identification of products or services offered to consumers; (ii) identification signs such as trademarks, symbols, or logos; and (iii) where applicable, information regarding labelling and marking in compliance with relevant EU laws on product safety and compliance.
- In regulated circumstances, online platform providers facilitating consumers in concluding distance contracts must, in accordance with Article 32, notify consumers who have purchased illegal products or services through their services upon becoming aware of such instances involving a trader. In cases where the online platform provider lacks contact information for affected consumers, it must ensure that details regarding the illegal product or service, along with the identity of the trader and available recourse options, are publicly accessible and easily located on its online interface.

Institutionalised compliance function

VLOPs and VLOSEs are required, under Article 41, to establish an independent compliance function comprising one or more compliance officers, including the head of the compliance function. This function must possess sufficient authority, resources, and access to the management body, enabling it to effectively oversee compliance with the DSA.

Established set of fines and penalties

Member States are mandated to establish penalties for infringements of the DSA by ISPs operating within their jurisdiction, as outlined in Article 52. Maximum fines for breaching DSA obligations are set at 6% of the ISP's annual worldwide turnover from the preceding financial year. For supplying incorrect information or failing inspection, the maximum fine is 1% of the annual income or worldwide turnover. Periodic penalty payments are limited to 5% of the average daily worldwide turnover or income of the ISP per day, calculated from the specified decision date. Furthermore, the EU Commission holds the authority to impose fines on providers of VLOPs and VLOSEs, not exceeding 6% of their total worldwide annual turnover from the previous financial year, in cases of intentional or negligent: (i) violation of DSA; (ii) non-compliance with a decision ordering interim measures issued by the Commission; (iii) failure to comply with a commitment made binding by a decision during the supervision, investigation, enforcement, and monitoring of VLOPs and VLOSEs by the Commission.

TRANSPARENCY RULES AND MECHANISMS

Transparent rules about user-provided content, with additional focus on minors

According to the DSA, ISPs are required to ensure that their 'Terms and Conditions' contain comprehensive information concerning restrictions related to user-provided content, as outlined in Article 14. This includes details regarding content moderation procedures, algorithms, human reviews, and internal complaint systems. These 'Terms and Conditions' must be easily understandable, user-friendly, and publicly accessible. Any modifications

to these terms must be promptly announced and communicated to users. Additionally, services directed to minors must present their conditions in a clear and easily comprehensible manner. Lastly, VLOPSEs are required to provide users with a summary of their terms and conditions, published in the official languages of the Member States where they operate.

Example: https://help.instagram.com/581066165581870/?helpref=uf_share

Transparency of content moderation decisions

In the event of content moderation necessitated by legal violations or non-compliance with platform policies, hosting service providers are obligated to provide a comprehensive, reasoned, and timely explanation for their intervention. This explanation, known as the Statement of Reasons (SOR), must be furnished to the recipient and includes details such as the type, reasons, and methodology behind a specific content moderation decision, as mandated by Article 17 of the DSA. The SOR comprises the following components: (i) information on the decision's nature, including actions taken (removal, access restriction, etc.); (ii) explanation of facts and circumstances leading to the decision; (iii) if applicable, details regarding the use of automated means in the decision-making process, including whether the content was detected using automated tools; (iv) reference to the legal basis for deeming the information illegal; (v) if the decision is based on the incompatibility with hosting service provider terms, reference to contractual grounds and explanations for considering the information incompatible; (vi) information on available redress options.

Three levels of transparency of content moderation policies and practices

» ISPs are mandated by Article 15 to publish an annual report detailing their content moderation practices. This report offers publicly accessible insight into a single provider's moderation efforts, encompassing: (i) The quantity of administrative or court orders received and respective actions taken. (ii) Elaborations of content moderation undertaken at the provider's initiative. (iii) The number of complaints received via

internal complaint-handling systems, with online platform providers additionally disclosing the basis for these complaints, decisions made, the median time required for decision-making, and instances where decisions were overturned. (iv) Any utilisation of automated means for content moderation, including accuracy indicators, potential error rates, and applied safeguards. These reports, required to be available in a readable format, provide interested parties with information regarding an ISP's content moderation practices. However, as the content of these reports is not precisely defined, initial reports lack comprehensiveness and detail.

» Online platforms are mandated to enhance their transparency measures, as outlined in Article 24. A centralised and easily accessible database, managed by the EU Commission, provides detailed insight into the structure of content moderation on these platforms. This database includes information regarding the initiators and types of moderation, with a specific focus on the use of automated tools. Furthermore, online platforms are required to disclose the following information in their reports: (i) Details of disputes submitted to out-of-court dispute resolution bodies. (ii) Statistics on suspensions, categorised by suspensions for manifestly illegal content, manifestly unfounded notices, and manifestly unfounded complaints. Additionally, every six months, online platform providers must update the average number of monthly active users in each member state. The Digital Services Coordinator of establishment has the authority to request updated user numbers at any time and must inform the EC in case the online platform provider transitions to a VLOP or VLOSE status. Moreover, online platform providers must furnish the EU Commission with decisions and statements of reasons for inclusion in a database managed by the EU Commission, ensuring that the submitted information does not contain personal data.

» VLOPSEs are mandated to uphold the highest level of transparency, as stated in Article 42. Their reports must encompass the following details: (i) The average number of monthly active users in each Member State. (ii) The human resources allocated by VLOP for content moderation within the EU, including details on personnel qualifications, training programs, and support mechanisms. (iii) Accuracy indicators and

relevant information concerning automated content moderation tools. Moreover, VLOPs must provide reports about their risk assessment and related risk mitigating measures, as well as their audit reports and audit implementation reports.

Example: https://transparency.fb.com/sr/dsa-transparency-report-oct2023-instagram/

Recommender system transparency

Online platform providers employing recommender systems are required to transparently outline the primary parameters utilised in these systems within their terms and conditions, according to Article 27. These main parameters must elucidate why specific information is recommended to the recipient. They should find it easy to comprehend these parameters and have the capability to adjust or modify them accordingly. In cases where multiple options influence the relative order of presented information, platforms must offer a user-friendly feature enabling recipients to modify their preferred option. Furthermore, VLOPSEs utilising recommender systems must offer at least one option for each system that is not based on profiling, as defined in the GDPR.

Annual independent auditing

VLOPSEs are required to undergo independent audits, conducted at their own cost and at least annually, in accordance with Article 37. These audits assess their compliance with specific obligations outlined in DSA, including: (i) due diligence obligations to ensure a transparent and safe online environment; (ii) commitments made under codes of conduct and crisis protocols. In case of a non-positive audit report, providers must review operational recommendations and take necessary actions within one month. They are also obligated to produce an audit implementation report detailing implemented measures or justifications for not implementing operational recommendations, along with any alternative measures taken to address non-compliance.

SAFETY RULES AND MECHANISMS

Notification of suspicions of threats to life or safety

If a hosting service provider becomes aware of information suggesting a criminal offence that threatens life or safety, it is obligated to promptly notify the law enforcement or judicial authorities of a Member State and provide them with all relevant available information, as stipulated in Article 18.

Protection of minors' rights and prevention from targeted advertising

The DSA seeks to protect the privacy, safety, and security of minors and protects against targeted advertising based on profiling, as outlined in Article 28. It is crucial that adherence to these obligations does not necessitate the processing of additional personal data to verify the user's age.

Systemic risk assessment

VLOPs and VLOSEs are required, under Article 34, to identify, analyse, and assess any systemic risks annually and in any event prior to deploying functionalities that are likely to have a critical impact on the risks within the EU, arising from the design or operation of their services and related systems, including algorithmic systems, or from the utilisation of their services. These risk assessments should demonstrate how companies have addressed various "systemic risks", encompassing: their negative effect on fundamental rights; the dissemination of illegal content through their services; any actual or foreseeable negative effects on civic discourse, electoral processes, and public security; any actual or foreseeable negative effects in relation to gender-based violence, potential negative effects on public health, protection of minors and serious negative consequences to the person's physical and mental well-being. When conducting risk assessments, VLOPs and VLOSEs must consider the influence of the following factors on systemic risks: (i) the design of their recommender systems and any other relevant algorithmic system; (ii) their content moderation systems; (iii) the applicable terms and conditions and their enforcement; (iv) systems for selecting and presenting advertisements; (v) data related practices of the provider.

Mitigation measures against systemic risks

VLOPs and VLOSEs are required, according to Article 35, to implement reasonable and proportionate mitigation measures to address specific systemic risks, such as: (i) adapting the design, features, or functioning of their services, including online interfaces; (ii) adapting their terms and conditions and enforcing them effectively; (iii) testing and adjusting their algorithmic systems, including recommender systems; (iv) adjusting advertising systems and implementing measures to restrict advertisements. Furthermore, the Board and the Commission will annually publish detailed reports on the most prominent and recurrent systemic risks reported by VLOPs and VLOSEs and best practices to mitigate these risks.

Crisis response mechanism

In times of a crisis, upon the Board's recommendation, the Commission may issue a decision requiring VLOPs and VLOSEs to undertake one of the following actions: (a) evaluate whether their services contribute to a serious threat, and if so, to what extent and how; (b) implement specific, effective, and proportionate measures to prevent, eliminate, or mitigate the identified serious threat; (c) report to the Commission within specified timelines on their assessments, the content and impact of measures taken, and any other relevant issues as outlined in the decision. The Commission plays a major role in monitoring the process and ensuring compliance with the provisions of the decision. Article 36 prescribes the detailed procedure for making the decision and its content.

HORIZONTALITY RULES AND MECHANISMS

Mechanisms enabling illegal content reporting

Hosting service providers and online platform providers are required to establish notice and action mechanisms, enabling any individual or entity to report illegal content. According to Article 16, the notice must contain as minimum: (i) a sufficiently substantiated explanation of the alleged illegal content; (ii) a clear indication of the exact electronic location (e.g., URL) and additional information for identification, as necessary; (iii) submitter's name

and email; (iv) a statement confirming the bona fide belief in the accuracy and completeness of the information. These mechanisms must be easily accessible, user-friendly, and exclusively allow the submission of notices through electronic means. If the notice includes the submitter's contacts, the hosting service provider must promptly send a confirmation of receipt. The provider must also notify the submitter of its decision, specifying whether automated means were used in the processing or decision-making.

User-friendly complaints handling system for recipients

Online platform providers are required to establish an internal complaints handling system accessible to recipients of the service, enabling them to appeal decisions made by the platform provider on submitted notices, as stated in Article 20. Online platform providers must ensure that decisions are overseen by qualified personnel and not solely reliant on automated processes. The internal complaint systems should be user-friendly, facilitating precise and substantiated complaints. Additionally, complainants must be promptly informed of the reasoned decision and provided with options for out-of-court dispute resolution and other available avenues for redress.

Recipients' right to lodge a complaint

Recipients of the service have the right to file a complaint against an ISP if they suspect a violation of the DSA to the Digital Services Coordinator, as per Article 53. The Digital Services Coordinator is responsible for assessing the complaint and, when necessary, forwarding it to the Digital Services Coordinator of establishment or another competent authority. Throughout this procedure, both parties will have the right to be heard and receive appropriate information about the status of the complaint, in accordance with national law.

Recipients' right to compensation

Recipients of the service have the right to seek compensation, consistent with EU and national laws, from ISPs for any damage or loss arising from the ISPs' failure to fulfil their obligations under the DSA, as outlined in Article 54. Furthermore, according to Article 21, recipients of the service who are

addressed by the decisions of the online platform providers may resolve such disputes in front of an out-of-court dispute settlement body certified by the Digital Services Coordinator.

ACCESSIBILITY RULES AND MECHANISMS

Established accessible points of contacts

The DSA introduces two 'points of contact' that all IPSs must designate to ensure accessibility:

» Points of Contact for Competent Authorities (Article 11). These facilitate direct, formal, certain, efficient, and formalised communication between ISPs and authorities (Member States' authorities, the Commission and the Board). It mitigates challenges arising from disparate contacts, outdated information, inaccessible channels, or ISP communication avoidance. Details of this point of contact must be publicly disclosed, easily accessible, and include information about the languages used for communication.

Example: https://www.facebook.com/help/678741677600131/?helpref=uf_share

» Points of Contact for Recipients of Services (Article 12). These enable user-friendly, not entirely automated, direct, and rapid communication between recipients and the ISPs, allowing recipients to choose their preferred method of communication (automated or human). Details of the point of contact are publicly disclosed, easily accessible, and regularly updated. This mechanism is designed to support recipients' engagement and communication with service providers.

Example: https://www.facebook.com/help/274852255072531/?helpref=uf_share

Available and accessible legal representatives of ISPs within the EU

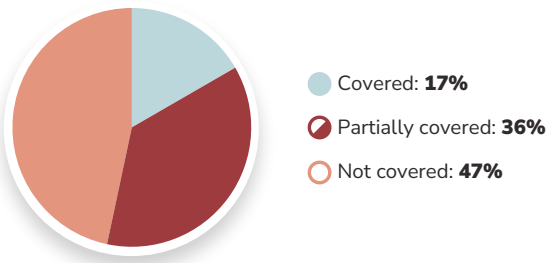
To address the challenge of extraterritoriality for ISPs operating within the EU, the DSA mandates the appointment of a legal representative in one of the Member States, as stated in Article 13. This legal representative, whether a natural or legal person, plays a pivotal role in facilitating communication between the ISP and relevant authorities. They are tasked with cooperating with authorities, adhering to their decisions, and ensuring the ISP's compliance with DSA regulations. Additionally, legal representatives are empowered to enforce decisions issued under the DSA. It's important to note that legal representatives can be liable for non-compliance with the DSA unrelated to the liability of the ISP itself. Details about the legal representative must be publicly available and easily accessible.

Example: https://www.digitalturbine.com/dsa/

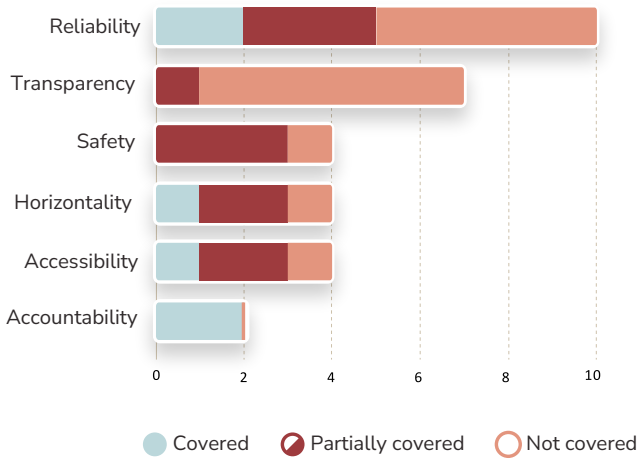
Accessibility for compliance and systemic risks monitoring

VLOPs and VLOSEs are required, as per Article 40, to grant the Digital Services Coordinator of establishment or the EU Commission access to data that are necessary to monitor and assess their compliance with the DSA. Furthermore, they must also provide access to "vetted researchers" for the exclusive purpose of conducting research that aids in identifying and understanding systemic risks in the EU, as well as assessing the effectiveness, efficiency, and impacts of risk mitigation measures.

ALBANIA



Coverage of DSA-related rules in Albanian regulation



Coverage of DSA-related values in Albanian regulation, by rules

DSA-related Regulation References in Albania:

» Law on Electronic Commerce (Official Gazette of the Republic of Albania, No. 10128/2009)

- Law on Electronic Communications in the Republic of Albania (Official Gazette of the Republic of Albania, No. 9918/2008)
- Instruction on protection of personal data in direct trade and security measures (No. 16/2011)
- Instructions on defining of rules to protect the security of personal data processed by small processing entities (No. 22/2012)
- Instruction on defining rules to protect the security of personal data processed by large processing entities (No. 47/2018)
- Law on Consumer Protection (Official Gazette of the Republic of Albania, No. 9902/2008)
- Law on Personal Data Protection

The primary legislation governing information society services in Albania includes the Law on E-Commerce and the Law on E-Communications. According to the Law on E-Commerce, an intermediary service is any natural person or legal entity that enables the transmission of messages or documents from the information society service provider to third parties, or delivers messages or information from the recipient of the services and products to the relevant information society service provider. Relevant to digital services is also a definition of an electronic communication service provider in Albanian regulation (including the provision of information society services that involve, in whole or in part, the transmission of signals over electronic communications networks) which is an operator who, inter alia, provides or is authorised to provide an electronic communications network or associated facilities.

Reliability

Referring to reliability as defined in the DSA, Albanian legislation does contain certain rules that safeguard this value. However, the majority of mapped rules are outdated and do not provide adequate normative response to contemporary challenges. Furthermore, these rules are identified within different pieces of legislation (Law on E-Commerce, Law on E-Communications, Law on Consumer Protection, Law on Personal Data Protection), resulting in a differentiated and inconsistent legislative foundation for reliable intermediary services in Albania.

On one hand, the Law on E-Commerce implies the obligation of the IPSs to interrupt services if the information transmitted through their communication networks constitutes illegal activity. Additionally, according to the Law on E-Communications, service providers may interrupt services if a contractual breach by the service recipient (i.e., subscriber) poses a serious threat to public order and safety, health, or the environment.

However, there are no specific rules regulating how intermediary service providers should design their interfaces. Nevertheless, the Law on Consumer Protection addresses unfair trade practices, which may indirectly influence interface design.

Similarly, Albanian legislation does not provide requirements for ISPs to provide users with basic information about the advertisements they display. Nevertheless, the Law on Consumer Protection includes general regulations regarding advertisements, stipulating that they should not be unfair, discriminatory, comparative, or misleading, and outlines the liability of advertisers.

According to Albanian legislation, online platforms are not obligated to verify their traders. However, a general provision in the Law on E-Communication requires electronic communications service providers to store and maintain subscriber data files for two years for criminal prosecution purposes. Additionally, there are no regulations mandating the design of online store interfaces. Yet, this might be implied from provisions in the Law on Consumer Protection related to unfair trade practices, such as misleading or aggressive trade practices. Moreover, it is not required of online stores to inform consumers or make publicly available information about the sale of illegal products or services on their platforms.

In Albania, establishment of an independent compliance function is not mandated by any rule. Also, there is no mandate for administrative penalties. However, various sanctions can be imposed by relevant supervisory authorities on intermediary service providers, depending on the nature of the breach or violation. These penalties are outlined in the Law on E-Commerce, the Law

on E-Communications, the Law on Consumer Protection, and the Law on Personal Data Protection.

Transparency

The analysis shows a significant gap in the relevant regulations needed to ensure the transparent operation of ISPs in Albania. There are no rules that require ISPs to report on their content moderation practices, prepare any reports, or undergo mandatory independent audits as outlined in the DSA. Also, transparency of online advertising practices as well as the regulation of recommender systems are unregulated.

However, the Law on E-Commerce obliges service providers to inform recipients about contractual terms and conditions. Moreover, the Law on E-Communication requires service providers to inform recipients about terms that restrict access to and the use of communication services.

Safety

Most of the rules in the DSA aimed at protecting this value are recognised in some form within the legal framework of Albania. They are found in the Law on E-Commerce, the Law on Consumer Protection, and the Instructions of the IDP Commissioner. Even though the corpus of safety-related rules exist in Albanian regulation, its improvement and alignment with European standards must be the priority.

In Albania, service providers are obliged to immediately notify the competent authorities, if they have reasonable doubts that the users of the services: a) are performing illegal activity; b) have provided illegal information.

However, the information society service providers are not obliged to monitor the information that they transmit or store, nor to seek facts or circumstances indicating illegal activities. Also, there are no rules regulating the obligations of any provider of information society services regarding advertisements targeting minors. However, there is a general provision in the Law on Consumer Protection - directly targeting children to buy goods or services, or persuading their parents or other adults to buy those goods or services, is

considered an aggressive (and thus unfair) trade practice and, therefore, it is prohibited.

Also, in the Albanian legal framework, there are no rules requiring ISPs to conduct mandatory risk assessments or to implement specific measures to address identified and regulated risks. However, Instructions no. 22 and 47 of the Albanian Information and Data Protection Commissioner (IDP Commissioner) contain the obligation of data controllers to carry out the data protection impact assessment related to their data processing activities (i.e., prior commencement thereof).

Horizontality

Horizontality as a value is partially embedded in the Albanian legal framework - these rules must be improved to provide a horizontal and inclusive regulatory mechanism, ensuring a comprehensive approach that involves different actors in ISP regulation.

The Law on E-Communication sets out rules and terms for the handling of the complaints submitted by the service recipients (i.e., subscribers) to electronic communications service providers. However, there are no rules regarding the existence of any mechanism allowing individuals or entities to report illegal content, as provided under the DSA. Consequently, there are also no rules that require any ISPs to establish an internal complaint-handling system enabling recipients of the services to appeal decisions made by the platform provider on submitted notices.

Regarding rules that allow service recipients to file a complaint against an ISP with a competent authority, as outlined in the Law on E-Communications, if the service provider fails to respond to a recipient's complaint, the recipient can request the supervisory authority (Electronic and Postal Communications Authority, EPCA) to resolve the relevant issue with the service provider.

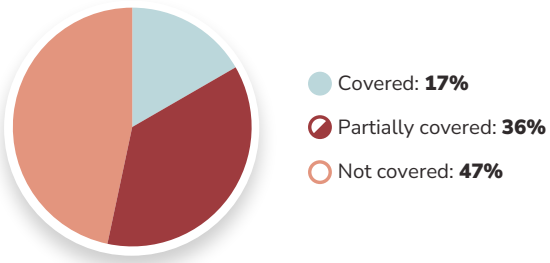
Accessibility

The Albanian legal framework provides several rules regarding accessibility of ISPs. Specifically, according to the Law on E-Communications, the service

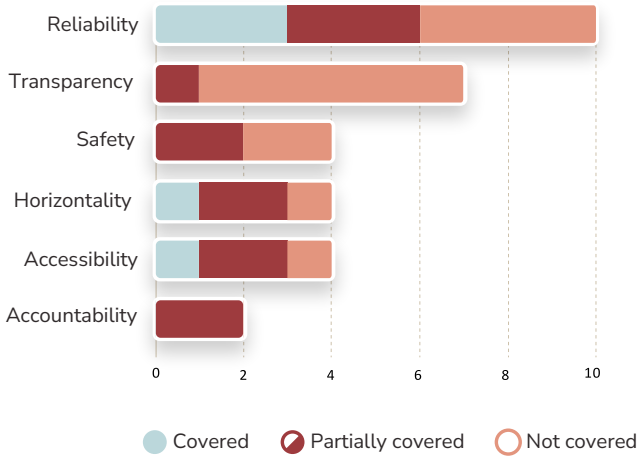
providers are obliged to notify the EPCA, inter alia, the contact persons for the communication with the authority.

In addition, according to Instructions of the Albanian IDP Commissioner which are sublegal acts issued based on the provisions of the Law on Personal Data Protection, either service provider (i.e., data controller) is obliged to appoint a data protection officer (DPO) who, inter alia, acts as a contact person vis-a-vis the IDP Commissioner.

However, there are no rules on monitoring compliance with mandatory rules of the ISPs.



Coverage of DSA-related rules in BiH regulation



Coverage of DSA-related values in BiH regulation, by rules

DSA-related Regulation References in BiH:

- Law on Electronic Legal and Business Transactions (Official Gazette of BiH, No. 88/07)
- Rule 60/2012 on the Conduct of the Activity of Internet Service Providers (Official Gazette of BiH, No. 36/12)
- Rule 96/2023 on Video-sharing Platform Services (Official Gazette of BiH, No. 41/23)

- Law on Consumer Protection in Bosnia and Herzegovina (Official Gazette of BiH, nos. 25/06 and 88/15)
- Draft Law on Internal Trade of Federation of BiH (approved by the Government of FBiH at its 353. session held on 9 March 2023)
- Law on Communications (Official Gazette of BiH, nos. 31/03, 75/06, 32/10 and 98/12)

In Bosnia and Herzegovina, several legal acts reflect the foundational principles of the regulatory framework that preceded the DSA. Notably, the EU Directive 2000/31/EC on Electronic Commerce, which is a normative ground for the DSA, was transposed into BiH legislative framework by means of the Law on Electronic Legal and Business Transactions.

Set of rules in Bosnia and Herzegovina are particularly relevant for this matter. Rule 60/2021 on the Conduct of the Activity of Internet Service Providers (hereinafter Rule on Internet Service Providers) a by-law adopted by the Communications Regulatory Agency (CRA), provides for terms and conditions for the provision of internet as a publicly available commercial service in electronic communication networks. Furthermore, Rule 96/2023 on Video-sharing Platform Services, also a CRA by-law (hereinafter Rule on VSPs), defines the criteria for the provision of video-sharing platform (VSP) services, as well as the rights and obligations of providers of these services in Bosnia and Herzegovina. This Rule is fully aligned with the Audiovisual Media Services Directive as amended in 2018.

Reliability

In comparison to the DSA rules that contribute to reliability, Bosnia and Herzegovina has introduced several principles across various regulatory pieces that address current regulatory needs. However, to ensure a reliable digital ecosystem, these rules must be further improved to provide a coherent, comprehensive, and systemic regulatory framework.

These rules are outlined in various laws and documents, including the Law on Electronic Legal and Business Transactions, the Law on Communications, the Law on Consumer Protection of Republika Srpska, and the Draft Law on

Internal Trade of the Federation of BiH, as well as by-law documents such as the Rule on VSPs and the Rule on Internet Service Providers.

The Rule on Internet Service Providers obliges service providers to allow unimpeded access to all publicly available content and services offered on the internet, with the exception of those which would cause explicit illegality or criminal offence. It requires internet service providers to "use appropriate technical measures to deny access to internet addresses", based on specific regulations or decisions of the competent institutions in Bosnia and Herzegovina that find such content to be harmful and illegal, especially if it "disseminates child pornography and other harmful content, allows for illegal online gambling, spreading computer viruses or dangerous software, illegal acquiring of personal information, threatens general security, public order, enables unlawful use of computer programs and applications, as well as other threats to safe use of the internet."

The Law on Electronic Legal and Business Transactions contains provisions on commercial communications that are part of, or constitute, an information society service. These provisions require service providers to ensure that a) such commercial communications are clearly identifiable as such; b) the natural or legal person on whose behalf the commercial communication is made is clearly identifiable; c) promotional offers, such as discounts, premiums and gifts, are clearly identifiable as such, including the conditions which must be met to qualify for them; (d) promotional competitions or games are clearly identifiable as such, including the conditions for participation.

Furthermore, the service provider who sends unsolicited commercial communications by electronic mail, without prior consent of the recipient, is required to ensure that such commercial communication is clearly and unambiguously identifiable upon receipt.

According to the Rule on VSPs, providers of these services are required to ensure that users are clearly informed where programmes and user-generated videos contain audiovisual commercial communications, provided that such communications are declared by the users who upload user-generated videos, or the provider has knowledge of that fact.

However, at the moment there are no rules obliging the online platforms to verify their trades, but such rules are expected to be adopted soon in one BiH entity, the Federation of BiH.

The Draft Law on Internal Trade of Federation of BiH stipulates in its Article 51 that the trader who manages the electronic platform must in a clear and comprehensible manner inform the consumer on whether the person offering goods or services is a trader or not, based on the statement of that person.

However, there are several regulatory gaps in the current framework. Specifically, there are no provisions governing the creation of interfaces for ISPs, nor are there any mandatory design standards for online store interfaces. Additionally, there is no requirement for online stores to inform consumers or make public the sale of illegal products or services on their platforms. The establishment of an independent compliance function is also not mandated.

The Law on Electronic Legal and Business Transactions prescribes fines for violations of provisions regulating various obligations, including the duty to inform users about implemented codes of conduct, ensuring transparency of commercial communications, and providing users with access to contractual provisions and general terms and conditions.

Regarding Internet Service Providers and VSPs, the Law on Communications gives the Communications Regulatory Agency power to apply enforcement measures on regulated subjects, ranging from oral and written warnings; inspection of licensed facilities; concrete demands for action or cessation to be complied with within a specified time limit; financial penalties; orders to interrupt the provision of services for a period not exceeding three months; and finally revocation of a licence.

Transparency

Bosnia and Herzegovina's legal framework lacks DSA-aligned rules for a transparent digital services environment. Analysis shows a significant gap regarding this value. However, there are several rules which are embedded in the principle of transparency. The Law on Electronic Legal and Business Transactions mandates that service providers grant users access to contractual

provisions and general terms and conditions. It also requires service providers to inform users about any voluntary codes of conduct they follow and provide details on how these codes can be consulted electronically.

Finally, in accordance with the Rule on VSPs, providers are required to include and apply restrictions and measures in their terms and conditions to protect their users.

Safety

Half of safety related rules, which were identified in the analysis, is contained in the Law on Electronic Legal and Business Transactions, while the other half is found in the by-law document, the Rule on VSPs. It's important to note that this regulation addresses digital services only partially compared to referential DSA rules.

There are currently no rules mandating ISPs to notify competent authorities if they suspect criminal offences. However, as per the Law on Electronic Legal and Business Transactions, service providers are obligated, based on a relevant judicial act, to provide the court with all pertinent information concerning the investigation of their service users to prevent, investigate, or prosecute court-sanctioned crimes. Additionally, in compliance with relevant administrative authority act, service providers must grant access to user names and addresses if such disclosure is deemed a significant prerequisite for fulfilling the duties of said administrative body.

When it comes to rules akin to those in the DSA regulating the obligation of online platforms or any other ISPs concerning advertisements targeting minors, Bosnia and Herzegovina has a similar regulation for VSP providers. Apart from the general obligation to implement measures aimed at protecting minors from programs, user-generated videos, and audiovisual commercial communications that could harm their physical, mental, or moral development, the Rule on VSPs specifies that "personal data of minors collected or otherwise generated by video-sharing platform providers shall not be processed for commercial purposes, such as direct marketing, profiling, and behaviourally targeted advertising."

There are no mandatory rules for ISPs to conduct risk assessments or implement measures to address identified and regulated risks.

Horizontality

Horizontal approach to digital services regulation has already been applied in several by-laws documents. However, these rules have limited legal strength and regulatory scope, and are scattered across multiple documents, which does not allow for precise and consistent regulatory prerequisites for horizontalisation.

For instance, the Rule on VSP mandates that VSP providers establish mechanisms enabling users to report illegal content on their platform. It specifically requires VSP providers to create and maintain transparent and user-friendly mechanisms for users to report or flag specific content. However, this obligation does not apply to other ISPs.

This Rule also requires VSP providers to establish and maintain transparent, easy-to use, and effective procedures for handling and resolving user complaints related to the implementation of certain measures they are obligated to enforce to protect their users.

Moreover, the Rule on Internet Service providers establishes the obligation of these providers to independently resolve user complaints, including an obligation to inform the user in the event of rejection of a complaint by means of a written decision with detailed explanation within 15 days of the receipt of the complaint.

The Law on Communications specifies that users or interested parties can address complaints, especially those concerning service quality that haven't been resolved satisfactorily with the telecommunications operator, to the Communications Regulatory Agency.

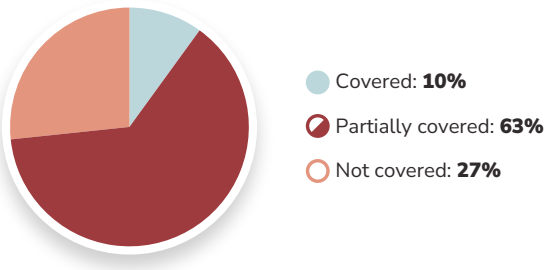
However, there are no rules allowing the recipient of the service to pursue compensation from ISPs for any damage or loss in Bosnia and Herzegovina.

Accessibility

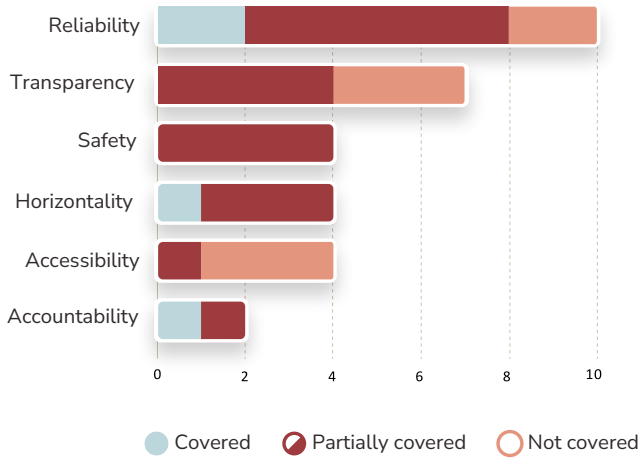
Accessibility is also a value pillar in Bosnia and Herzegovina's legal framework. However, compared to DSA rules, there are certain gaps in its regulation. The majority of accessibility-related rules are detailed in the Law on Electronic Legal and Business Transactions, with some addressed in the by-law document, specifically the Rule on Internet Service Providers.

According to the Law on Electronic Legal and Business Transactions, there is a general obligation of service providers to make easily, directly and permanently accessible to the recipients of the service, at least the following information: (a) its name or the company's name; (b) place and address of its registered office; (c) the details which allow the users to contact him rapidly and directly, including his electronic mail address; (d) where the service provider is registered in a court, trade, or a similar public register, the trade register in which the service provider is enlisted and his registration number, or equivalent means of identification in that register; (e) where the activity is subject to administrative oversight, the information of the relevant authority; (f) where the service provider is subject to rules on regulated professions, the information on professional association or similar institution with which the service provider is registered, the professional title and the state where it has been granted, a reference to the applicable professional rules and the means to access them; (g) if applicable, the tax identification number.

The Rule on VSP requires from VSP providers to enable easy, direct and permanent access to information to the public. This includes disclosing their name, address of establishment, internet address (URL) of the service, and comprehensive contact details such as email address or website, facilitating direct communication.



Coverage of DSA-related rules in Kosovo regulation



Coverage of DSA-related values in Kosovo regulation, by rules

DSA-related Regulation References in Kosovo:

- Law on the Information Society Services (Official Gazette of Republic of Kosovo, No. 04/L-094/2012)
- Law on General Administrative procedure (Official Gazette of Republic of Kosovo, No. 20 / 21)
- Law on Electronic identification and Trust Services in Electronic Transactions (Official Gazette of Republic of Kosovo, No. 11 / 23)

- Law on Information Society Government Bodies Official Gazette of Republic of Kosovo, No. 15 / 15)
- Law on Electronic Communications (Official Gazette of Republic of Kosovo, No. 04/L-109/2012)
- Law on Consumer Protection (Official Gazette of Republic of Kosovo, No. 06/L-034/2018)
- Law on Child Protection (Official Gazette of Republic of Kosovo, No. 06/L-084/2019)
- Administrative Instruction (GRK) No. 04/2022 on Measures for the Protection of Children against Websites with Pornographic Content and those that Harm the Health and Life of the Child

Within Kosovo's regulation a provision of intermediary services is regulated by the Law on the Information Society Services, while the Electronic Communications Act contains several provisions that mirror some of the rules found in the DSA.

Reliability

Kosovo's legal framework encompasses a number of rules on digital services aimed at safeguarding reliability. These rules are embedded within the Law on Information Society Services, the Law on Electronic Communication, and the Law on Consumer Protection. However, if they want to ensure reliability in accordance with the DSA, Kosovo would need to improve the existing regulations towards newer legal solutions.

No rules obliging ISP to suspend services under certain conditions are mapped in Kosovo's regulation. However, according to the Law on Electronic Communications, service providers are permitted to refuse, unilaterally suspend, or discontinue access to services, but only under specific circumstances. Such actions must be based on objective criteria, which may include technical non-feasibility or the necessity to ensure network integrity.

In the Kosovo legal framework, rules regarding the transparency of online advertising practices are being developed, with some already in place. The draft Law on Consumer Protection proposes an amendment aimed at

enhancing transparency in marketing. This includes prohibiting the use of editorial content in media for product promotion without disclosing any payment from traders. Such disclosures must be clearly identifiable to consumers through images or voice within the content. Moreover, the draft law prohibits search results from concealing advertisements or payments aimed at boosting product rankings. These measures aim to inform consumers about paid promotions across traditional media and online platforms.

Additionally, the Law on Electronic Communications underscores the transparency of electronic communications services. These obligations extend to significant market power (SMP) entrepreneurs in the sector, requiring the publication of specific information related to interconnection, technical specifications, and tariffs, among others.

Even though online platforms are not obliged to verify their traders, the Law on Consumer Protection includes a general provision outlining the information that must be provided to consumers before concluding a distance contract, particularly in the context of financial services.

Regarding rules that oblige online stores to inform consumers (or make such information publicly available) about the sale of illegal products or services on their platform, the Law on Consumer Protection addresses this in the section on Redress Mechanisms. It stipulates that consumers should be informed about the existence of an out-of-court complaint and redress mechanism related to the distance contract. Additionally, the provision on the Right to Information mandates that online platforms inform consumers about illegal products or services offered by traders through their services. This includes informing consumers about the illegality of the product or service, the identity of the trader, and any relevant means of redress.

The connection between these provisions lies in the obligation of both financial service providers (as outlined in the Redress Mechanisms) and online platforms (as outlined in the Right to Information provision) to inform consumers about redress mechanisms. This ensures that consumers are aware of their rights and avenues for seeking remedies in case of issues or disputes arising from distance contracts or illegal products/services.

Transparency

Compared to the transparency regulations covered by the DSA, Kosovo's legal framework includes several rules that protect this value. However, the regulations outlined in the Law on Electronic Communication are not as comprehensive as the new EU regulations.

The Law on Electronic Communication prescribes that entrepreneurs providing electronic communications networks and/or services shall submit to the Authority, in accordance with the procedure and conditions set forth by the Authority, data and reports on their activity.

Moreover, any entrepreneur providing public electronic communications networks or publicly available electronic communications services, except for small and medium-sized enterprises, shall ensure that their annual financial reports are audited and published.

However, there are no rules that require ISPs to be transparent about restrictions they impose to the content that is created by their users. Also, no rules regarding regulation recommender systems, or independent audits were mapped in Kosovo's regulation.

Safety

Within Kosovo's legal framework, provisions similar to DSA's rules that safeguard safety are to some extent identified in the Law on Electronic Communication and the Law on Child Protection.

The Law on Electronic Communications mandates that entrepreneurs providing electronic communications networks and/or services must cooperate with operational investigation services, pre-trial investigation institutions, prosecutors, courts, or judges by providing necessary information to prevent, investigate, and detect criminal acts.

On the one hand, there are no obligations of online platforms or any other ISPs when it comes to advertisements targeting minors. However, there is an Administrative Instruction on measures for the protection of children

against websites with pornographic content and those that harm the health and life of the child which is implemented by all relevant institutions, child protection professionals, public and private companies that provide and distribute internet and television services, video games, as well as NGOs, the community and parents, in accordance with the mandate, obligations and responsibilities that are provided in the Law on Child Protection as well as other relevant applicable legislation.

According to Law on Electronic Communications, "entrepreneurs providing public communications networks or publicly available electronic communications services shall take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services", providing a certain level of risk assessment and measures regulations.

Horizontality

DSA rules concerning horizontality are acknowledged to some extent within Kosovo's laws. These regulations are prescribed in the Law on Information Society Services and the Law on Electronic Communication.

The Law on Electronic Communications sets the obligation for the Authority to establish the rules for the settlement of disputes based on complaints submitted by end users, while compensation for damages is regulated by general rules only.

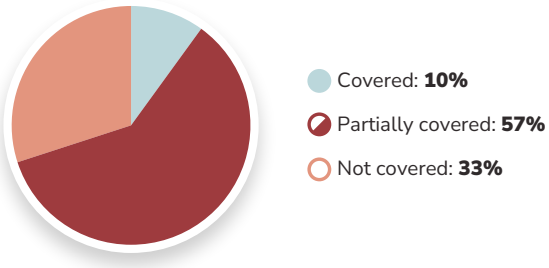
There are no rules that require any ISP to establish mechanisms enabling users to report the existence of specific information (e.g. illegal content) on their platform.

Accessibility

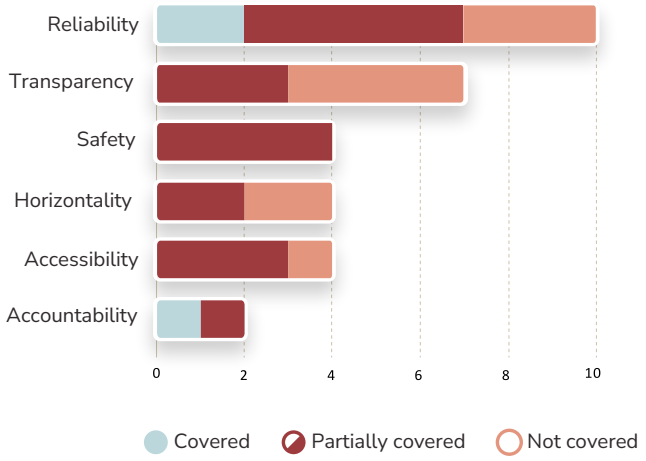
Accessibility needs a comprehensive approach and application into Kosovo's regulation. Existing rules are dispersed across the Law on General Administrative procedure, the Law on Electronic Identification, the Law on Government Bodies for Information Society, and the Law on Electronic Communications.

Any rules similar to appointment of a single point of contact for direct communication with competent authorities or recipients of the service, as outlined in the DSA, were not found in Kosovo's regulation. However, the Law on General Administrative Procedure and the Law on Electronic Identification, already aligned with eIDAS, along with the Law on Government Bodies for Information Society, designate the Agency for Information Society as the central hub or single point of contact for G2G, G2C, and G2B services.

The Law on Electronic Communications grants the Authority the right to request information from entrepreneurs involved in electronic communications activities for specific purposes. This information must be proportionate and objectively justified and is primarily related to compliance verification with legal provisions.



Coverage of DSA-related rules in Montenegrin regulation



Coverage of DSA-related values in Montenegrin regulation, by rules

DSA-related Regulation References in Montenegro:

- Consumer Protection Law “Official Gazette of Montenegro”, No. 2/2014, 6/2014, 43/2015, and 70/2017
- Competition Protection Law “Official Gazette of Montenegro”, No. 44/12,13/18 and 145/21
- Law on Electronic Communications “Official Gazette of Montenegro”, No. 040/13 of 13.08.2013, 056/13 of 06.12.2013, 002/17 of 10.01.2017, 049/19 of 23.08.2019

- Law on General Product Safety “Official Gazette of Montenegro”, No. 45/2014 and 13/2018
- Law on Electronic Document “Official Gazette of Montenegro”, No. 132/2022
- Law on Electronic Identification and Electronic Signature “Official Gazette of Montenegro”, No. 31/2017 and 72/2019
- The Law on Electronic Commerce “Official Gazette of the Republic of Montenegro”, No. 80/2004, “Official Gazette of Montenegro”, No. 41/2010, 40/2011, and 56/2013
- Agency for Electronic Communication and Postal Services Website, The Decision of the Constitutional Court of Montenegro abolishing the provision of Article 145, paragraph 4 of the Law on Electronic Communications “Official Gazette of Montenegro”, No. 40/13 and 2/17

The Law on Electronic Commerce is aligned with EU directives, which represents a good precondition for the Digital Services Act (DSA) but has not been amended since 2013. Certain segments are also regulated through the Law on Electronic Communications, the Law on Information Security, the Draft of which is currently in the process of alignment with EU legal acquis, etc.

Reliability

Significant portion of the DSA rules aimed at protecting reliability comprehensively or tangentially are identified within Montenegro’s laws: the Law on E-Commerce, the Law on E-Identification, the Law on E-Document, the Law on General Product Safety, the Law on E-Communication, and the Consumer Protection Law.

The Law on Electronic Commerce states that the provider of information society services must ensure that every piece of information in a commercial message, which is part or in full an information society service, meets the following conditions: that the commercial message can be clearly identified as such at the moment the user receives it; that the entity on whose behalf the commercial message was composed can be clearly identified; that every

promotional call to action from the commercial message (including discounts and gifts) must be clearly identified as such; that the invitation to a promotional contest and games contains clearly and unambiguously presented terms and conditions.

There are no specific rules requiring online platforms to verify their traders as prescribed by the DSA. However, related legal frameworks in Montenegro include the Law on Electronic Identification and Electronic Signature and the Law on Electronic Document. Additionally, the Regulation on detailed conditions for qualified trust service providers, based on Article 34, paragraph 2 of the Law on Electronic Identification and Electronic Signature, prescribes detailed conditions that must be met by legal or natural persons providing services such as the issuance of qualified certificates for electronic signatures, seals, website authentication, electronic time stamps, and other related services.

While there are no explicit rules mandating online stores to inform consumers about the sale of illegal products or services on their platform, the Law on General Product Safety outlines general safety requirements and criteria that products supplied to the market must meet. This law also specifies the obligations of manufacturers and distributors, including the requirement to inform market surveillance authorities immediately, in writing, if they become aware that certain products pose an unacceptable risk to consumers due to non-compliance with safety requirements.

When it comes to penalties, various laws in Montenegro prescribe monetary fines: the Consumer Protection Law, the Law on Electronic Commerce, the Law on Electronic Communications, the Competition Protection Law, the Law on Electronic Document, and the Law on Electronic Identification and Electronic Signature.

There are no rules that obligate any ISP to suspend services under certain conditions. Additionally, there are no regulations concerning the creation of interfaces for any ISPs or the mandatory design of interfaces for online stores. Furthermore, there are no rules requiring the mandatory establishment of an independent compliance function.

Transparency

Approximately two thirds of the DSA-like rules aimed at protecting this value are partially recognised within Montenegro's legal framework. They are contained in the Law on Electronic Communications.

Also, there are no rules that require online platforms or any other ISP to prepare some kind of specific reports, but indirectly the Law on Electronic Communications states that the operator is obliged, upon written request, to provide the Agency for Electronic Communications with data at its disposal, including financial data, as well as data related to the development of networks or services that may affect its wholesale services, with some exceptions.

Regarding the rules in the DSA that require reporting from specific types of ISPs, Montenegro has a similar provision regulated by the Law on Electronic Communications. It states that for the performance of regulatory and market supervision tasks in the field of electronic communications, the Agency charges an annual fee from operators. Consequently, operators must send an annual report to the Agency. This report must detail the revenue generated from providing public electronic communication services and leasing electronic communication networks, infrastructure, and related equipment from the previous year. Operators involved in activities other than electronic communications must keep separate accounts for each activity, clearly disclosing the revenue from electronic communications services and leasing infrastructure.

There is a gap when it comes to regulating recommender systems using any ISPs, as well as rules on mandatory independent audits for ISPs.

Safety

Rules aimed at safeguarding safety are broadly recognized in Montenegro's laws: the Law on Electronic Communication, the Consumer Protection Law, the Law on General Product Safety, and the Law on E-Commerce. They represent partial regulation of this matter as compared to corresponding DSA rules.

The Law on E-Commerce states that the service provider must notify the competent authority in case there is a reasonable suspicion that the user is engaging in prohibited activities through the use of their service; or if there is a reasonable suspicion that the user of their service has provided unauthorised data. There are parts of addressing this within the Law on Electronic Communication and also one more article of the Law on E-Commerce which states that the competent authority for the information society (hereinafter referred to as the competent authority) may take one or more measures restricting the freedom to provide information society services to a service provider based in a member state of the European Union, whose service poses a serious threat to: the legal order, especially for the conduct of investigations, detection, and prosecution of criminal offences, protection of minors, and combating hate speech or intolerance based on race, gender, religion, or nationality and violations of human dignity; protection of public health or the life and health of individuals; protection of the security and defence of Montenegro; consumer protection, which also includes investors. The competent authority is obliged to inform the competent authority of the member states of the European Union and the European Commission of the intention to take these measures. If the competent authority of the member state of the European Union does not take appropriate measures within 30 days from the date of receipt of the notification, the competent authority may take measures restricting the freedom to provide information society services, while informing the competent authority of the member state of the European Union and the European Commission.

The Consumer Protection Law lists forms considered aggressive commercial practices, including advertising directly targeting children to make purchases or persuade their parents or other adults to purchase the advertised product.

The Law on electronic communication does not explicitly mention “mandatory risk assessment”. However, various aspects of the provision of this law imply the necessity for operators to evaluate and mitigate risks associated with data interception and retention.

Horizontality

In Montenegro's legal framework, we identified rules that contribute to horizontality in the Competition Protection Law.

However, there are no rules that require hosting services providers, online platform providers or any other ISP to establish mechanisms enabling users to report the existence of specific information (e.g. illegal content) on their platform, nor any rules that require ISPs to establish an internal complaint-handling system.

Regarding DSA rules that allow recipients of services to file complaints against ISPs with an authority, the Consumer Protection Law covers certain segments, Depending on the body addressed, and in connection with the relevant legislation mentioned, it is possible to file a complaint, objection, or initiate proceedings.

When it comes to rules allowing recipients of services to pursue compensation from ISPs for any damage or loss, in Montenegro's legal framework, this is mainly addressed through the Consumer Protection Law and the Law on E-Commerce.

Accessibility

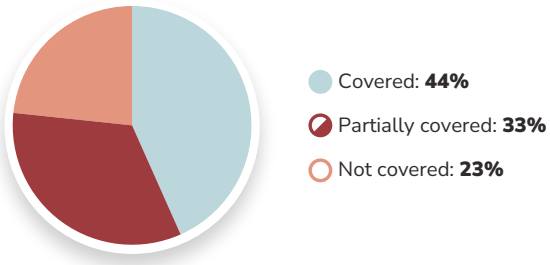
Regarding accessibility, the Law on Electronic Commerce defines the data that service providers must make available to users and competent state authorities, albeit only partially within the Consumer Protection Law.

There are no specific rules mandating ISPs to appoint a single point of contact for direct communication with competent authorities or recipients of their services. Nevertheless, the Law on Electronic Commerce delineates the data that service providers must provide to users and competent state authorities.

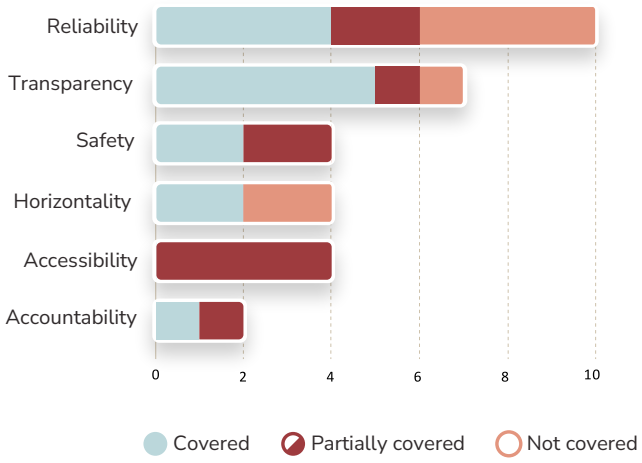
Also, any rules necessitating ISPs to designate representatives to collaborate with the competent authorities of Montenegro were not found.

There are several bodies overseeing and having different levels of authority regarding the compliance with the regulations related to ISPs: 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, as well as related ministries.



Coverage of DSA-related rules in North Macedonian regulation



Coverage of DSA-related values in North Macedonian regulation, by rules

DSA-related Regulation References in North Macedonia:

- The Constitution (as of the illegitimate amendments published in the Macedonian Official Gazette No. 6/2019)
- Law on Electronic Communications (Macedonian Official Gazette No. 39/14, 188/14, 44/15, 193/15, 11/18, 21/18)
- Law on the Provision of Remote Financial Services (Macedonian Official Gazette No. 158/10 and 153/15)

- Law on Electronic Commerce (Macedonian Official Gazette No. 133/07, 17/11, 104/15, 192/15, and 31/20)
- Criminal Code (Macedonian Official Gazette No. 80/99, 4/2002, 43/2003, 19/2004, 81/2005, 60/06, 73/06, 7/08, 139/08, 114/09, 51/11, 135/11, 185/11, 142/12, 166/12, 55/13, 82/13, 14/14, 27/14, 28/14, 115/14, and 132/14)
- Law on Violations (Macedonian Official Gazette No. 96/2019)
- Law on Commerce (Macedonian Official Gazette No. 16/04, 128/06, 63/07, 88/08, 159/08, 20/09, 48/09, 99/09, 105/09, 115/10 , 158/10, 36/11, 53/11, 148/13 , 164/13, 97/15, 129/15, 53/16, 120/18, 77/21, 215/21, 295/21, and 150/22)
- Communications Surveillance Law (Macedonian Official Gazette No. 71/2018)
- Personal Data Protection Law (Macedonian Official Gazette No. 42/2020 and 294/2021)
- Law on Mediation (Macedonian Official Gazette No. 188/13, 148/15, 192/15, and 55/16)
- Law on protection of consumers (Macedonian Official Gazette No. 236/2022)
- Law on the Security of Networks and Informational Systems (a law in preparation to be enacted as of 2024-05)
- Bylaws and related legal documents

In North Macedonia, the provision of intermediary services is (somewhat tangentially) regulated by several legal acts, including the Constitution, the Law on Electronic Communications, the Law on the Provision of Remote Financial Services, the Law on Electronic Commerce, and, by extension, the Criminal Code, the Law on Misdemeanors, the Law on Commerce, the Communications Surveillance Law, the Personal Data Protection Law, along with their bylaws and related legal acts. Content moderation is initially regulated within the Law on Electronic Communications, which includes a bylaw focused on the obligation of ISPs to inform consumers about common methods by which electronic communications can be used for illegal activities or IP infringements.

Beyond specifying particular acts and violations in the Criminal Code and the Law on Misdemeanors (such as incitement of national, religious, and ethnic hatred and discrimination, calls for genocide, or commission of a criminal offence), and aside from the general provisions in the Constitution which forbid censorship and support free expression, content moderation is only tangentially regulated in dedicated legal acts. The most concrete stipulation is found in the Law on Electronic Commerce, which outlines the responsibility of ISPs regarding illegal content. ISPs are not responsible for illegal content if they are unaware of its illegality, did not modify it while transferring it to the end user, and were not the initiator of the request. However, should a provider of an information society service somehow acquire knowledge of an illegal activity or data that they store, they are obliged to act promptly and remove or restrict access. Although providers of such services are explicitly relieved from the obligation to check data they store, transfer, or make available, they are obliged to react and inform competent authorities of any reasonable doubt regarding users that might undertake illegal or unpermitted activities. As a general stipulation, providers of services are obliged to react to requests and instructions of competent authorities (such as courts, ministries, and other institutions) when asked to stop and remove violations of applicable legal provisions.

Reliability

Majority of rules regarding reliability in the North Macedonian legal framework is contained in the Law on Electronic Communications. It prescribes that a provider of universal service can limit access, disconnect a user, or end the service provision agreement only when the user has breached the provisions of that agreement. Any action in this respect must be proportional and non-discriminatory.

When it comes to DSA rules that require online platforms to provide users with basic information about the advertisement they display, North Macedonia has a similar rule within its legal framework. The Law on Electronic Commerce regulates commercial communication, which largely equates to advertisement. It includes stipulations regarding information on advertisements and the traders that advertise. Additionally, the Law on

Audio and Audiovisual Communications contains several articles addressing advertisement, including provisions for transparency and clear identification of advertising programs and advertisers.

There are no specific provisions in North Macedonia's regulation dealing with trader verification on platforms. The general identifiability of traders is stipulated in the Law on Electronic Commerce.

There are no rules that regulate the creation of interfaces to any ISPs, nor mandatory design of interfaces for online stores. Also, no rules oblige online stores to inform consumers (or make such information publicly available) about the sale of illegal products or services on their platform. As mentioned, informing obligations are directed toward competent authorities, not consumers.

No rules mandating the establishment of an independent compliance function or addressing administrative penalties for violations related to intermediary services were identified. However, many rules governing the provision of services can be applied to intermediary ones as well, though only tangentially.

Transparency

The North Macedonian regulations offer a significant coverage of transparency. Some of these rules require ISPs to be transparent about restrictions they impose on the content that is created by their users. Additionally, ISPs are required to inform their users about the content moderation they perform since publication of their terms of service is obligatory. Also, they must specify any content moderation.

The Law on Electronic Commerce stipulates that the provider of an Information Society Service (ISS) is obligated to provide the service user with the general terms and conditions (if they are part of the agreement for service), before the agreement is finalised and signed. The Law on Consumer Protection stipulates the obligation for a trader to publish its general and specific conditions for selling or providing services in a manner accessible by a buyer or user. The same Law stipulates prohibition for discrimination when using services, which might be related to content moderation. Chapter 2 of this Law is focused on

obligations for providers of public services, and also includes obligations for providing the general terms and conditions. Some of the ISPs might at times be categorised as 'public services', particularly in regards to the provision of a universal service and communications of service or emergency nature. The Law on Electronic Communications mandates the service providers to explicitly publish and make available objective, transparent, proportional, and non-discriminatory terms and conditions. It also stipulates that the agreement between the ISP and the end-user must contain all conditions and terms applicable, including those that in some sense limit access. Finally, even though ISS operators have an obligation to retain communication metadata, they are forbidden from retaining the actual data. This makes content moderation rather difficult.

Bylaws provide rules that require ISPs to prepare specific reports. However, when it comes to rules that require reporting from any specific type of ISP, in North Macedonian legal framework there is only a general requirement.

Finally, recommender systems are not yet regulated.

Safety

According to this analysis, significant attention has been given to the safety of the digital environment in North Macedonia. This legal framework recognises to some extent all DSA rules related to safety. They are part of the Law on Electronic Communication and the Law on Electronic Commerce. Some of them are more similar to DSA rules and comprehensively cover this matter, while others are outdated or need further alignments.

The Law on Electronic Communications stipulates the obligation for Internet service providers to withhold the data they process or create for a certain period and to submit it to the competent authorities upon request. They are also obliged to inform the competent authorities should they have a reasonable doubt as to the legality of the content, services, or data that they are transferring or making available to users. At the same time, they are not obliged to actively check data nor services they transfer or make available for any illegal or forbidden activities or content.

There are no specific rules that regulate the obligation of ISPs when it comes to advertisements targeting minors, but the Law on Electronic Commerce stipulates the general protection of minors for all purposes.

Mandatory risk assessments that ISPs must perform are prescribed by the Law on Electronic Communications, as well as rules on mandatory measures to be implemented by ISPs in order to address identified and regulated risks. ISPs are obligated to undertake appropriate technical and organisational measures to appropriately manage risks upon security of networks and services i.e. in regards of integrity, (in)security, infringement of personal data security, infringement of communicational confidentiality, location data, and general data safety.

Horizontality

In the legal framework of North Macedonia there are no specific rules regarding user-initiated reporting of illegal content.

Illegal content and matters related to criminal acts are addressed through lawful surveillance of communications, and if ISPs acquire knowledge of such activities made through the provision of the service. However, this does not extend to content removal, as governmental bodies and institutions do not have the legal authority to mandate content moderation and removal. They can only initiate relevant legal procedures.

There are no rules that require an online platform or any other ISPs to establish an internal complaint-handling system.

Regarding rules that allow the recipient of the service to file a complaint against ISPs with an authority, the Law on Consumer Protection designates collective organisations for consumer protection as the authority for complaints. Additionally, the Law on Electronic Communications assigns the Agency for Electronic Communications as the authority to receive complaints against ISPs.

There are rules allowing the recipient of the service to pursue compensation from ISPs for any damage or loss, either through mediation dispute settlement or through court procedures.

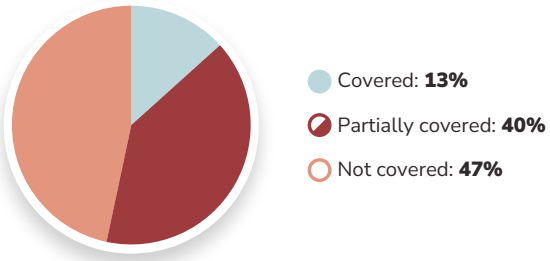
Accessibility

The laws of North Macedonia partially provide for the accessibility of intermediary services.

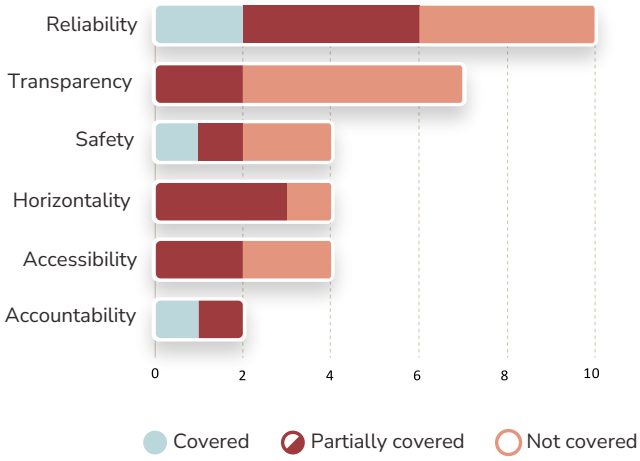
There is a general rule related to the DSA requirement for ISPs to designate a single point of contact for direct communication with service recipients. Regarding the designation of representatives to cooperate with competent authorities, each legal person must have a responsible natural person specified by law, generally obligated to cooperate with authorities.

Furthermore, the Law on Electronic Communications contains rules on monitoring compliance with mandatory ISPs rules.

While a single point of contact for direct communication with competent authorities concerning content moderation is not mandated, there are requirements for lawful surveillance of communications (for criminal investigations), dealing with security incidents and risks, and addressing technical issues.



Coverage of DSA-related rules in Serbian regulation



Coverage of DSA-related values in Serbian regulation, by rules

DSA-related Regulation References in Serbia:

- Law on Electronic Commerce (Official Gazette of RS no. 41/2009, 95/2013 and 52/2019)
- Regulations on mandatory measures for video-sharing platform service providers (Official Gazette of RS, no. 43/2024)
- Law on Mediation in Dispute Resolution (Official Gazette of RS, no. 55/2014)

In Serbia, the Law on Electronic Commerce (hereinafter: the Law on E-Commerce) is harmonised with the Directive on Electronic Commerce which is the predecessor of DSA. This Law prescribes the conditions and manner of providing services of the information society, obligations to inform users of services, commercial communications, rules regarding the conclusion of contracts in electronic form, liability of information society service providers, supervision, and offences. The Law on Electronic Media contains rules that are to certain extent related to the DSA regulations. For example, it includes a small set of rules concerning video-sharing platform services. According to this Law, video-sharing platform service is an information society service primarily aimed at making program content, user-generated videos, or both available to the public through an electronic communications network. The platform provider does not bear editorial responsibility but organises the content, particularly through displaying, tagging, and sequencing, using automated means or algorithms. Additionally, based on this Law, a bylaw — Regulations on mandatory measures for video-sharing platform service providers (hereinafter Regulation on VSP) — was enacted, which also partially reflects the DSA rules. In Serbia, the following laws govern related areas, although they currently do not include regulations related to DSA: the Consumer Protection Law, the Information Security Law, and the Electronic Communications Law.

Reliability

More than half of DSA-related rules aimed at protecting reliability is identified within Serbia's legal framework. Just a small portion of those rules is comprehensive in addressing this matter, while the majority only partially aligns with the DSA approach. They are all encompassed in the Law on E-Commerce and Regulation on VSPs.

The Law on E-Commerce regulates a measure of limitation on the provision of information society services. It allows courts to impose restrictions on these services if an applicant demonstrates either the existence of an infringement or the potential for irreparable harm.

There are no specific rules concerning the creation of interfaces for any ISPs or the mandatory design of interfaces for online stores. Also, online platforms are not obliged to verify their traders or inform consumers about the sale of illegal products or services on their platform, while the establishment of an independent compliance function for these platforms is not mandatory.

Commercial messaging is another area regulated under the Law on E-Commerce. A commercial message, whether it partially or entirely constitutes an information society service, must meet several conditions. For instance, the commercial message must be clearly identifiable as such when received by the service user; the entity responsible for composing the commercial message must be clearly identifiable; any promotional call to action, such as discounts or gifts, must be clearly identified; finally, the terms required for accepting an offer from the commercial message must be easily accessible and presented in a clear and unambiguous manner. Additionally, sending commercial messages electronically is permitted only with the recipient's consent. Service providers are required to regularly verify consent and accept withdrawals from individuals who no longer wish to receive such messages.

The Regulation on VSPs stipulates that service providers must clearly indicate when program content or user-generated video content contains audiovisual commercial communications. This requirement applies if the service providers have been informed through a declaration by the user who uploaded the content. Furthermore, the regulation emphasises that techniques affecting the user's subconscious must not be used in audiovisual commercial communications.

Penalties for violations of the Law on E-Commerce are imposed by the court after a conducted procedure. The legal framework does not prescribe administrative penalties, thus leaving the imposition of penalties solely to the judicial system.

Transparency

Significant gap is identified related to transparency as a value pillar in Serbian regulations. A small portion which only partially aligns with the DSA-

corresponding rules is found in the Law on E-Commerce and the Regulation on VSPs.

The Law on E-Commerce mandates that providers of information society services must provide potential users with clear and understandable information and notices prior to contract conclusion. This includes detailing the general conditions of service provision if they form an integral part of the contract, as well as the codes of conduct that regulate service provider behaviour and the means by which these codes can be accessed electronically.

The Regulation on VSPs requires service providers to establish and implement a system for informing users about decisions and measures taken in response to content reporting on their platform. This system must address content that could harm the physical, mental, or moral development of minors, content that incites violence and hatred, and content constituting a criminal offence such as public incitement to commit terrorist acts, child pornography, or racial and other forms of discrimination.

Despite these requirements, significant gaps exist in the regulatory landscape. Notably, ISPs are not obliged to report on their content moderation practices, nor are there any rules necessitating online platforms or ISPs to prepare specific reports. Furthermore, the regulatory framework does not mandate reporting from any particular type of ISP under specific circumstances. There are also no regulations concerning recommender systems used by online platforms or ISPs, and no rules requiring mandatory independent audits for ISPs.

Safety

Rules relevant for the safety are encompassed in the Law on E-Commerce and the Law on Electronic Media. This value needs further operationalisation through legal framework, since there is a significant lack of safety-related rules, while those that exist are outdated or do not provide comprehensive legal response, as compared to the DSA.

The Law on E-Commerce requires providers of information society services to inform the competent authority if there is suspicion that a service user

is engaging in unauthorised activities or has shared unauthorised data. Additionally, service providers are obliged to disclose all relevant information, based on an appropriate judicial or administrative act, for the purpose of identifying or prosecuting perpetrators of criminal offences or protecting the rights of third parties.

The Law on Electronic Media stipulates that video-sharing platform service providers must take appropriate measures to protect minors from harmful program content, user-generated videos, or audiovisual commercial communications. This Law emphasises safeguarding minors from content that could harm their physical, mental, or moral development. Moreover, the Regulation on VSPs mandates that service providers ensure audiovisual commercial communications do not exploit minors' inexperience or gullibility, encourage minors to persuade parents to purchase advertised products or services, exploit the special trust minors have in responsible adults, or unjustifiably portray minors in dangerous situations.

However, there are notable gaps in the regulatory framework. Specifically, there are no rules requiring mandatory risk assessments to be conducted by ISPs, nor are there mandatory measures that ISPs must implement to address identified and regulated risks.

Horizontality

Horizontality is broadly but partially covered by relevant rules, as compared to the DSA. Rules that safeguard horizontal approach are primarily identified within the Law on E-Commerce and the Regulation on VSPs.

The Law on E-Commerce stipulates the requirements for notices of illegal activity or information. Upon receiving such notifications, service providers that store data must act promptly to remove or disable access to the illegal content. Similarly, service providers offering access to data from another provider (e.g., links) must take the same action upon learning of illegal activity. Additionally, the law allows courts to impose measures restricting the provision of information society services, order the removal of content, and ban actions that have led to the violation of rights.

The Regulation on VSPs requires video-sharing platform providers to establish and implement user-friendly and transparent mechanisms for reporting harmful content. Users can report content that may harm the physical, mental, or moral development of minors, incite violence and hatred, or constitute criminal offences such as public incitement to commit terrorist acts, child pornography, or racial and other forms of discrimination. Providers are also mandated to have a transparent, user-friendly, and efficient procedure for handling and resolving user reports and complaints.

Furthermore, the Law on E-Commerce obligates providers of information society services to remove unlawful content without delay, and no later than two days from the receipt of an order from the competent authority responsible for enforcing the law. This authority can issue the removal order either ex officio or upon the request of a party.

However, regulation in Serbia has no rules that would allow recipients of services to pursue compensation from ISPs for any damage or loss incurred.

Accessibility

In Serbia's legal framework, half of the DSA rules concerning accessibility is recognized to some extent. Such rules represent only partial regulation of this matter and are contained in the Law on E-Commerce.

The Law on E-Commerce requires providers of information society services to make certain information available to competent authorities, including: (i) the name of that provider; (ii) the registered office of the service provider; (iii) other details about the service provider through which service users can quickly and smoothly communicate with them, including an email address; (iv) registration details in the Register of Business Entities or other public register; v) details of the competent authority if the service provider's activity is subject to official supervision; vi) for specially regulated activities or professions: the professional or similar professional association where the service provider is registered; professional title and the country that issued it; instructions on professional rules in the country where the activity is carried out and their availability; (vii) tax identification number (TIN).

There are no rules that require ISPs to designate their representative to cooperate with the competent authorities.

Supervision over the implementation of the Law on E-Commerce is carried out by the ministry responsible for trade and services, or the ministry responsible for electronic communications and the information society, through inspection oversight.

DMA REGULATORY MECHANISM

In total, the DMA introduces 22 enforcement rules for gatekeepers in order to comply with the regulation. The rules are put in place in order to guarantee transparency, accountability, interoperability, mobility of information, and the demonopolisation of digital markets. The majority of the rules are reliant upon gatekeepers to disclose information in a timely and straightforward manner in order to ensure fair conditions for both businesses and end users, as well as to allow the EU Commission and other bodies proper oversight.[16]

TRANSPARENCY RULES AND MECHANISMS

Unrestricted access to third party content and other items by end users

According to Article 5, paragraph 5 of the Digital Markets Act, gatekeepers must allow free and full access to end users to third party content through its CPS. This promotes user choice and prevents gatekeepers from limiting access to certain services.

Example: https://newsroom.spotify.com/2024-03-01/a-letter-to-the-european-commission-on-apples-lack-of-dma-compliance/

Transparency and verification of advertising practices

Gatekeepers are obliged by Article 5, paragraphs 9 and 10 and Article 6, paragraph 8 to disclose the following details of their advertising policies to publishers and advertisers: (i) the granular price the advertiser paid for the advertisement and the metrics used to determine that price (the publisher can obtain this information if the advertiser consents, or average data are to be provided); (ii) the granular remuneration the publisher received and the metrics used to determine that remuneration (the advertiser can only obtain

16 Market democratisation, as a central and more general value within the DMA, has not been considered in detail from the perspective of corresponding rules and from a comparative perspective with the Western Balkans. However, it has been quantified since one identified rule addresses democratisation of the digital market in a broader sense - the existence of rules regulating provision of information society services (ISS), and those thet fall into the definition of “core platform service”.

this information if the publisher consents, or average data must be provided); (iii) performance measurement tools and data to enable verification of the advertisement's aggregated and non-aggregated data. This information should be provided upon request and free of charge to the advertiser.

Example: https://advertising.amazon.com/blog/amazon-ads-and-the-digital-markets-act

Fair access to online search engine data

Article 6, paragraph 11 of the DMA stipulates that business users will be able to access marketing data in order to improve their services and products. That means that if third-party online search engines request performance data, gatekeepers should provide clear and detailed answers to their queries. Gatekeepers are not generally allowed to make use of the same data in competition with the business user, nor are they allowed to bundle it with other personal data generated elsewhere in their ecosystem unless they receive consent from users.

Compliance and reporting obligations for gatekeepers

The gatekeepers must be able to demonstrate compliance with the obligations regulated in DMA, in accordance with Articles 8 and 11, including by preparing the reports to the Commission with explanations of the measures implemented to ensure compliance. This is an important mechanism for verification and transparency of the compliance, because non-confidential summaries of the reports must be amended at least annually and must be made publicly available.

Audited description of techniques for profiling of consumers

Under Article 15, the gatekeeper must submit to the Commission an independently audited annual description of any techniques for profiling of consumers that the gatekeeper applies to or across its CPS. The reports on consumer profiling techniques must describe, in a detailed and transparent manner, all relevant information on all techniques used for profiling of consumers applied to or across any core platform services

offered by gatekeepers. Gatekeepers are required to submit this description to an independent audit, and the reports should also contain the auditor's assessment on the completeness and accuracy of the description. In case of failure to comply, the gatekeepers shall be sanctioned in accordance with the regulation. Such oversight of profiling techniques by gatekeepers will allow competent authorities more insight and better ways to protect end users.

ACCOUNTABILITY RULES AND MECHANISMS

Consent as the only legal basis for collection and processing of personal data

By prioritising end users' consent, Article 5, paragraph 2 stipulates that the gatekeeper is not allowed to perform any of the following actions without explicit consent: (a) the processing of end users' personal data using services of third parties that make use of CPS for the purpose of providing online advertising services; (b) combining personal data from the relevant CPS with personal data from any further CPS or from any other services provided by the gatekeeper or with personal data from third-party services; (c) cross-using of personal data from the relevant CPS in other services provided separately by the gatekeeper, including other CPS, and vice versa; (d) signing in end users to other services of the gatekeeper in order to combine personal data. This rule also moves privacy enforcement from the national courts to the federal court, which means there is a much more aggressive enforcement regime likely to take place.

Example: https://www.theverge.com/2024/1/12/24036312/google-digital-markets-act-services-user-data-opt-out

Forbidden use of non-public data

Utilising user collected data through business users' services in order to improve advertising practices or for other non-transparent means will be sanctioned, in line with Article 6, paragraph 2. Gatekeepers will not be permitted to use non-publicly collected data in order to compete with business users in any capacity. This will be enforced in an effort to prevent gatekeepers'

monopolistic approach towards the digital sector, allows smaller business users' autonomy over their collected data and also strengthens rules around how business users treat end users' data.

Right of end user to make complaints

Under Article 5, paragraph 6, the gatekeeper is not allowed to prevent or restrict business users or end users from raising any issue of non-compliance with governing law by the gatekeeper with any relevant public authority, be it directly or indirectly. This does not exclude the possibility for business users and gatekeepers to agree to the terms of use of complaints-handling mechanisms that are lawful. These rules give more authority to end users to hold gatekeepers accountable in case of non-compliance.

Fair general conditions of access and termination of the CPS use

The gatekeeper must prepare general conditions that are regulated by Article 6, paragraphs 12 and 13. Under these rules, the gatekeepers would need to provide understandable information to avoid reading lengthy general terms and conditions. For the purpose of implementation of these rules, the provided information should include necessary and clearly understandable terms with their meanings and implications, to ensure that users fully understand the necessary elements to make a meaningful decision. The information should provide objectively neutral language and design elements to avoid dark patterns. The information should also be provided in a user-friendly way through pictograms or other graphical elements to ease comprehension, when possible and appropriate. These rules should enable fair and understandable conditions for business users in case they wish to terminate their cooperation with the gatekeepers CPS without price fixing, preferential treatment, or hidden costs or conditions.

Non-discriminatory and fair ranking

According to Article 6, paragraph 5, the gatekeeper is not allowed to treat more favourably its services and products in ranking and related indexing and crawling than similar third-party services or products and it will apply transparent, fair and non-discriminatory conditions to such ranking. In

regards to business users, non-discriminatory and fair ranking practices promote a transparent environment for products and services to reach users. Self-preferencing is considered to benefit major companies designated as gatekeepers and contribute to the monopolisation of the market. This rule would ensure fairness and a level playing field.

Right of the end user to data portability

Under Article 6, paragraph 9, end users will be afforded the right to transfer their data to another service in case they choose to switch from a gatekeeper's CPS. The right to data portability affords more transparency to end users in handling their own data and promotes fair market competition between service providers. As is prescribed by the GDPR, end users have the right to access and have their data transmitted where technically feasible. Therefore this rule ensures that data portability is an element of genuine choice of users to give them control over their data/self-determinism

Example: https://developers.google.com/data-portability/policy

Independent compliance function of the gatekeeper

Gatekeepers must, under Article 28, introduce a compliance function that is composed of one or more compliance officers, including the head of the compliance function, which is independent from their operational functions. Such a compliance function must have sufficient authority and resources to monitor gatekeeper's compliance. Gatekeeper's management body must ensure that compliance officers have relevant professional qualifications, knowledge and experience. Compliance officers are, inter alia in charge for: (i) overseeing the gatekeeper's compliance; (ii) advising the management and employees on compliance; (iii) cooperating with the Commission.

Penalties

Gatekeepers' violations of the DMA will be punished by imposing large financial penalties and will therefore incentivise gatekeepers to abide by the regulation, as prescribed by Articles 30 and 31. Infringements will be sanctioned by fines of up to 10% of a company's worldwide turnover. In cases

where gatekeepers repeatedly violate the DMA, the fine can increase to 20% of annual revenue.

INTEROPERABILITY RULES AND MECHANISMS

Mandatory interoperability for operating system and virtual assistance hardware and software

According to Article 6 para 7, the gatekeeper must, free of charge and without compromising the integrity of its service (i) allow providers of services and providers of hardware interoperability with the same hardware and software features of its operating system or virtual assistant, free of charge, (ii) allow business users interoperability with the same operating system, hardware or software features. These rules encourage open market circulation.

Mandatory interoperability of number-independent interpersonal communications services

According to Article 7, the gatekeepers for core platform messenger services (i.e. “number-independent interpersonal communications”) must enable interoperability, free of charge, in following three scenarios: (i) individual user sharing functionality - that enables core platform messenger service users to send end-to-end text messages, images, voice messages and videos to users of other messenger services, (ii) group chats - involve group sharing of end-to-end text messages, images, voice messages and videos, in a group that consists of users of core platform messenger services users of other messenger services, and (iii) voice and video calls – where interoperability between messenger services is enable for end-to-end voice calls and video calls, between individuals and within a groups. The gatekeeper must also: provide the same level of security, including the end-to-end encryption to all end users and publish a reference offer laying down the technical details and terms and conditions of interoperability.

Continuous and real time access to data

Article 6, paragraph 8 helps businesses assess their products and services and also allows them to have real-time insights in order to improve their offer to end users and also improve interoperability. It is also designed to impact competition – namely antitrust issues – consumer protection, and privacy in the digital sector through adequate regulation. Contrary to old data portability rules, this mechanism strives to ensure continuous interoperability, meaning that even in the event of an end user choosing to leave a service, they will still be able to interact with other users which have not chosen to do so. This way end users will get to keep the benefits of the aforementioned service while opting for another service that better meets their needs (such as privacy, transparency, integrity, etc.). If gatekeepers fail to produce continuous and real time access to business users' data and end users' data which is hosted on the gatekeepers CPS they will be subject to sanctions.

Right of end user to uninstall and change default settings of gatekeeper's software and to install 3rd party (default) software

According to Article 6, paragraphs 3 and 4, the gatekeepers must enable end users to (i) easily uninstall any non-essential software applications on the operating system of the gatekeeper, (ii) easily change default settings on the gatekeeper's operating system, virtual assistant, and web browser that direct or steer end users to gatekeeper's products or services, including by asking them to choose alternative service providers before first use, (iii) install and use third-party secure software applications or application stores using its operating systems and access to such software by third party services, and (iv) not prevent such third-party software from asking end users to be set as default. This provision allows end users more options and autonomy when choosing which services and products they wish to use. It also disincentivises market capture and the exclusion of smaller businesses from market participation.

Example: https://developer.apple.com/support/dma-and-apps-in-the-eu/

Freedom to determine prices for end users

The gatekeeper is not allowed to prevent business users from offering the same products or services to end users through third-parties' services or through their own direct online sales channel at prices or conditions that are different (better for end users) from those offered on gatekeeper's platform, as prescribed by Article 5, paragraph 3. This provision gives business users more autonomy when determining their own prices for products and services regardless of whether they are hosted on gatekeepers' platforms. It also allows end users to make more informed decisions.

Freedom to provide special offers to end users, different to what if offered via gatekeeper

With respect to business users, gatekeepers will be obliged, under Article 5, paragraph 4, to free of charge: (i) communicate and promote their offers to end users, including under different/better conditions, regardless of whether the end user is acquired by business user via gatekeeper's CPS or through other channels, and (ii) conclude contracts with those end users, for which purpose a business user can use gatekeeper's CPS or third party service.

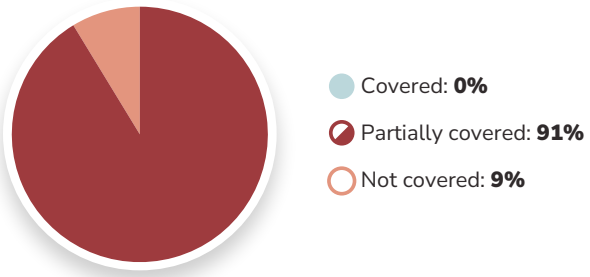
Freedom to use third party ID, browsing and payments services

Under Article 5, paragraph 7 gatekeepers cannot require business users wanting to use the gatekeeper's core platform to also use the gatekeeper's identification services. This relates to businesses such as advertisers or publishers who might be required to use the platform's own ID solution when offering their services. It is about data collection by the gatekeeper and refusal to use an alternative IS service. End users and business users will have more responsibility for choosing ID and payment services for their platforms, also gatekeepers will retain less control over business users and will not be allowed to impose internal services for additional profits.

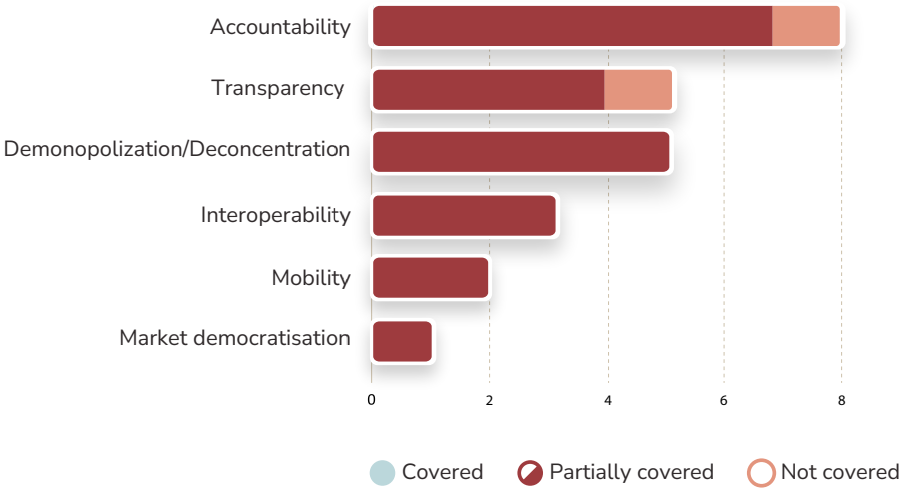
Ban on mandatory use of additional CPS as condition for use of any CPS

End users that wish to use a CPS provided by the gatekeeper, according to Article 5, paragraph 8 will not have to register or subscribe to any additional CPS in order to functionally use the service.

ALBANIA



Coverage of DMA-related rules in Albanian regulation



Coverage of DMA-related values in Albanian regulation, by rules

DMA-related Regulation References in Albania:

- Law on Electronic Commerce (Official Gazette of the Republic of Albania, No. 10128/2009)
- Law on Protection of Competition (Official Gazette of the Republic of Albania, No. 9121/2003)

- The Constitution of the Republic of Albania
- Law on Personal Data Protection (Official Gazette of the Republic of Albania, No. 9887/2008)
- Instruction on processing, protection and security of personal data in the public electronic communication sector (No. 14/2011)
- Instruction on protection of personal data in direct trade and security measures (No. 16/2011)
- Draft of the Law on Personal Data Protection
- Law on Electronic Communications in the Republic of Albania (Official Gazette of the Republic of Albania, No. 9918/2008)
- Law on the Civil Procedures Code of the Republic of Albania (Official Gazette of the Republic of Albania, No. 8116/1996)

In general, there are no specific rules in Albania on the functioning of the digital market for provision of CPS, except the generic regulation provided under the laws that regulate e-commerce and e-communications. Some rules from the DMA scope might be indirectly covered by some general or sector-specific laws, such as those regulating civil law procedures, protection of personal data or protection of competition.

The Law on E-Commerce does not regulate CPSs as such, but it does regulate information society services, some of which would fall into that category. From the definitions provided under the Law on E-Commerce, Article 3, it can be concluded that some of the ISSs that would fall under the category of CPS would be (i) online intermediation services, (ii) number-independent interpersonal communications services, (iii) operating systems; and (iv) online advertising services, advertising exchanges, and any other advertising intermediation services.

Under the Albanian laws, there is no definition for certain companies that would amount to gatekeepers. However, the Law on E-Communications that regulates undertakings operating in the electronic communications sector in several of its provisions regulates the status and the obligations of the "undertakings having a significant impact on the market". The Law on E-Communications contains the same definition of "information society

services" as provided under the Law on E-Commerce. It does not contain a positive list of ISSs that would fall under its scope.

Nevertheless, provisions of the Law on E-Communications would apply to all ISSs listed in the paragraph above (i.e. (i) online intermediation services, (ii) number-independent interpersonal communications services, (iii) operating systems; and (iv) online advertising services, advertising exchanges and any other advertising intermediation services). Accordingly, all of the ISS providers meeting the requirements set out by the Law on E-Communications in order for an undertaking to be considered as having a significant impact on the market shall undergo the relevant obligations imposed by the said law.

Albanian Law on Personal Data Protection currently in force is fully aligned with Directive 95/46/EC. There is a draft law in process of adoption which is harmonised with the GDPR and is publicly available, but it is not possible to say when it will be adopted.

Transparency

The majority of the DMA-like rules aimed at protecting transparency in the digital sector are recognized in some form or manner within Albania's legal framework. They are mainly contained in the laws that regulate e-communications and personal data protection.

The Law on E-Commerce does not have any rules regarding the transparency obligations of an ISS provider. On the other hand, the Law on E-Communications provides for certain obligations that can be considered as transparency-related duties. Under this Law, EPCA is entitled to obtain from undertakings operating in the electronic communications sector any kind of information necessary for carrying out the functional duties assigned by law. In addition, EPCA may impose on undertakings having a significant impact on the market the obligation to publish certain information regulated by the Law and further determine the level of detail and modalities of publications of the information required.

Profiling is regulated only by the Law on Personal Data Protection, so any transparency duties would be regulated from the perspective of the data controller notifying obligations.

Accountability

The vast majority of the rules focused on accountability within the DMA are in some way recognised in Albania's laws. However, all of them only indirectly or incidentally regulate these issues.

When it comes to personal data protection accountability and legal basis for data processing, there are no specific rules regulating the collection of personal data in the specific context of the provision of CPS or any other ISS. These matters are regulated only by the Law on Personal Data Protection. Albanian supervisory authority issued in 2011 some instructions that deal with the processing of personal data in the ambit of e-communication services. Additionally, the new law on personal data protection, which aims to approximate GDPR standards, is expected to regulate data portability, so it remains to be seen how it will affect the provision of ISS. By way of example, the Law on E-Communications provides for the rights of the phone number portability, rather than the data portability.

Users' right to complain about ISS providers' practices is regulated under general civil procedure laws. In addition, according to the Albanian Constitution, the right to complaint cannot in advance be prevented or restricted by means of law, bylaws, or agreement between parties.

Matters related to the non-discrimination obligation of ISS providers in the context of the provision of ISS are covered in general, on the principles level, in the Law on E-Commerce. According to this Law commercial transactions carried out through electronic means are based on the equality principle, free will, contractual freedom, free exercise of undertaking activity for the participants therein, as well as on the free movement of goods and services in Albania.

There are no direct rules regarding terms and conditions that must be provided by certain ISS providers in their B2B relations.

The Law on E-Commerce and the Law on E-Communications provide some penalties for violation of the rules related to the provision of some ISS, although they do not prescribe any fines when it comes to any CPS specifically.

Interoperability

There are no rules that would regulate ISS provider interoperability obligations. However, Albanian Law on E-Communications contains some rules aimed at interoperability for undertakings operating in the electronic communications sector.

Mobility

In both Albanian Competition Law and Law on E-Commerce, rules related to mobility value are recognised to some extent.

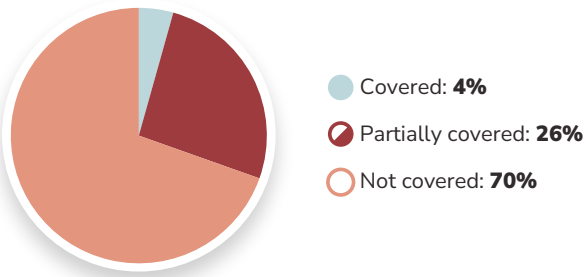
There are no rules that directly regulate the right to direct access to data in B2B transactions, or the right of end users to uninstall features of digital services or products, as are those set by DMA. However, the Law on E-Commerce has a general rule that parties to transactions in the field of electronic commerce may not impose restrictions on acquisitions or exercise of rights or obligations pertaining to natural persons of legal entities, except in the cases provided by law. In addition, any ISS provider, in the course of the exercise of its activity for the offering of services remotely, must ensure that such services ensure consumers' and investors' rights as per the provisions of the legislation in force.

Demonopolisation/Deconcentration

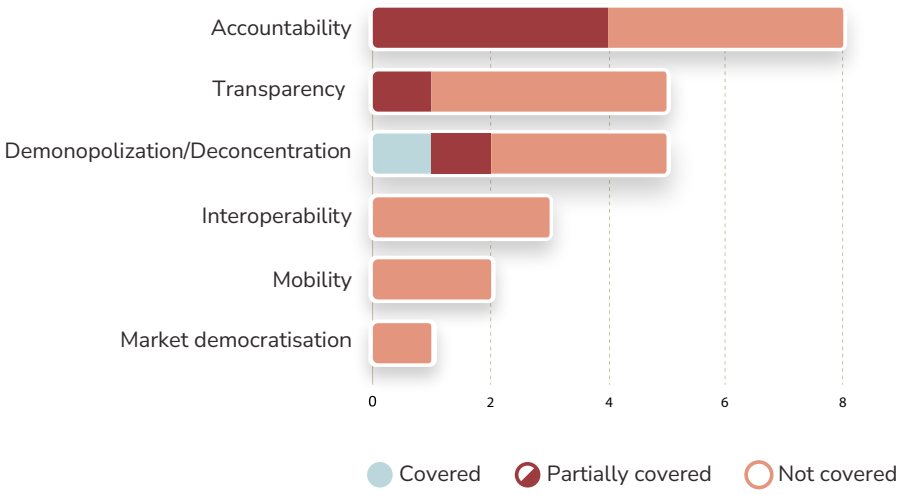
DMA rules related to demonopolisation are recognised to some extent in Albania's legal framework and are contained in the Competition Law and the Law on E-Communications.

The Competition Law regulates restrictive agreements and abuse of dominant position in a general, non-sector-specific manner. Currently, there is no competition law practice when it comes to its application in the digital services market.

The Law on E-Communications has some sector-specific competition protection rules for undertakings having a significant impact on the market in the e-communications sector. The EPCA can also impose on these undertakings the obligations of non-discrimination and interconnection.



Coverage of DMA-related rules in BiH regulation



Coverage of DMA-related values in BiH regulation, by rules

DMA-related Regulation References in BiH:

- Law on Protection of Personal Data (Official Gazette of BIH, nos. 49/06, 76/11 and 89/11)
- Decisions of the Competition Authority
- Law on Consumer Protection in Bosnia and Herzegovina (Official Gazette of BiH, nos. 25/06 and 88/15)
- Law on Consumer Protection in Republika Srpska (Official Gazette of RS, nos. 6/12, 63/14, 18/17 and 90/21)

- Law of Obligations of Federation of Bosnia and Herzegovina and Republika Srpska (Official Gazette of SFRJ nos. 29/78, 39/85, 45/89 and 57/89; Official Gazette of RBiH nos. 2/92, 13/93 and 13/94; Official Gazette of FBiH nos. 29/03 and 42/11; Official Gazette of RS nos. 17/93 and 3/96)
- Law on Competition (Official Gazette of BIH, nos. 48/05, 76/07 and 80/09)
- Law on Information Security of Republika Srpska (Official Gazette of RS, No. 70/11)

In Bosnia and Herzegovina, there are no special laws that address matters regulated by DMA. There are, however, a couple of laws that can be indirectly applied to some specific situations such as the Law on Competition, the Consumer Protection Law, the Law on Internal Trade, the Personal Data Protection Act, the Law on Obligations, etc. In addition, new laws on communications and the new Regulation on EC services, which are announced, may include some relevant rules.

Transparency

Some transparency-related rules can be found in data protection laws.

There are no rules regulating the right of the CPS or other ISS end users to access their online content, but there is a personal data protection rule that grants access to personal data to data subjects.

There are also no rules regulating reporting obligations of ISS providers directly. But under the Personal Data Protection Law, the data controllers are obliged to submit an annual report on the rejected data subjects' requests to the Agency for Protection of Personal Data. Furthermore, according to the Information Security Law of Republika Srpska, incidents regulated under this law that threaten public interest must be reported to National CERT.

Transparency in B2B transactions and obligations with respect to general terms and conditions are regulated to some extent in the law concerning obligations and torts.

Accountability

In the absence of explicit DMA-type rules, some accountability issues are addressed in general laws. Namely, if a CPS user is a natural person, the Consumer Protection Law guarantees certain complaint rights. This instrument recognises remote contracting (via the internet, for example), which is a characteristic of ISS/CPS. Furthermore, data protection may be applicable if CPS practices involve personal data.

Interoperability

There are no rules in Bosnia and Herzegovina that would regulate interoperability-related DMA values.

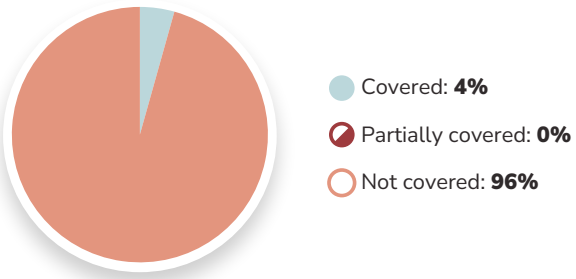
Mobility

There are no rules in Bosnia and Herzegovina that would regulate mobility-related DMA values.

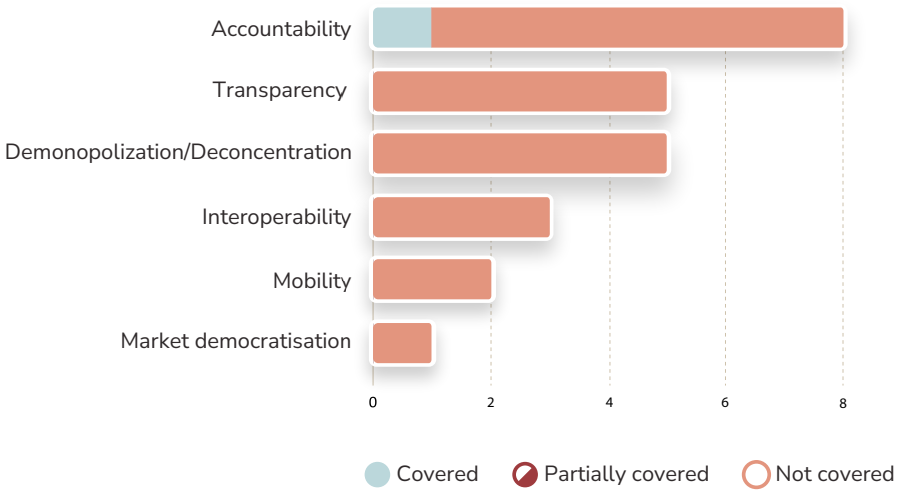
Demonopolisation/Deconcentration

Only general competition and consumer protection rules would apply to the issues of demonopolisation/deconcentration-values in the DMA sense, when it comes to fair competition and, more generally, fair business practices. Namely, there are decisions of the Bosnia and Herzegovina competition authority on price and sales condition determination in general, but none are specifically addressing the digital market.

There is also a layer of protection provided to consumers, as relevant consumer protection laws prescribe that advertisements must not contain any statement or visible representation that are directly or indirectly misleading consumers through omission, vagueness, or exaggeration. Also, the advertising of products and services must not be inappropriate, deceptive, or ambiguous and should adhere to established business practices.



Coverage of DMA-related rules in Kosovo regulation



Coverage of DMA-related values in Kosovo regulation, by rules

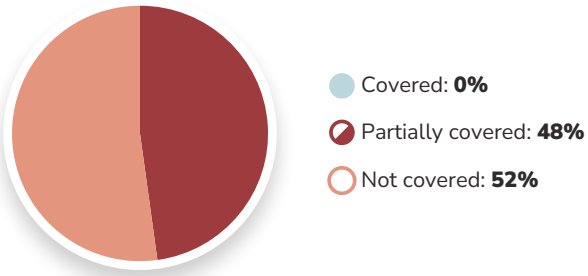
DMA-related Regulation References in Kosovo:

» Draft Law on Consumer Protection

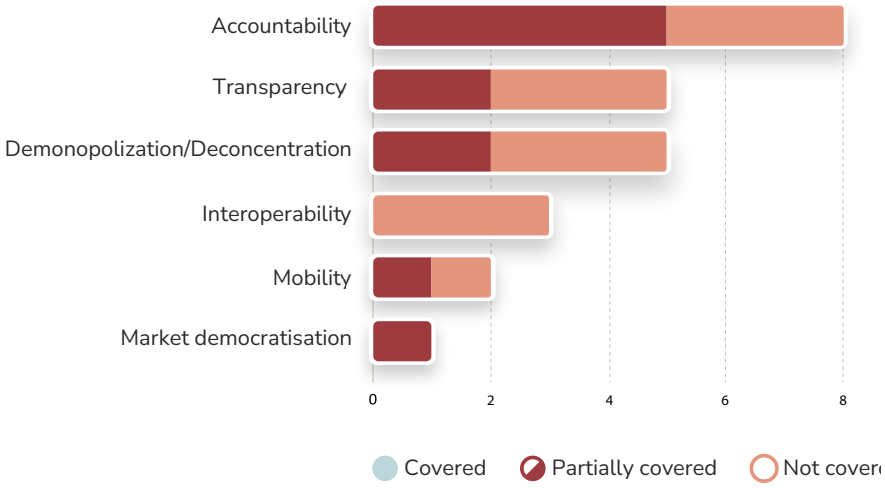
In Kosovo, there are no legal rules whatsoever that regulate matters covered by DMA, so it seems that DMA values would be difficult or impossible to protect under national legal regime.

When it comes to accountability rules and mechanisms, it might be worth mentioning that there is a draft law on consumer protection that might be

relevant to some digital content. According to this text, the conditions and measures defined under the provisions of the law apply to any distance and off-premises contracts concluded between the trader and the consumer.



Coverage of DMA-related rules in Montenegrin regulation



Coverage of DMA-related values in Montenegrin regulation, by rules

DMA-related Regulation References in Montenegro:

- Competition Protection Law "Official Gazette of Montenegro", No. 44/12,13/18 and 145/21
- Law on Personal Data Protection 079/08, 070/09, 044/12, 022/17)
- Law on Electronic Communications "Official Gazette of Montenegro", No. 040/13 of 13.08.2013, 056/13 of 06.12.2013, 002/17 of 10.01.2017, 049/19 of 23.08.2019

- The Law on Electronic Commerce “Official Gazette of the Republic of Montenegro”, No. 80/2004, “Official Gazette of Montenegro”, No. 41/2010, 40/2011, and 56/2013
- Law on Electronic Document “Official Gazette of Montenegro”, No. 132/2022
- Law on Electronic Media “Official Gazette of Montenegro”, No. 046/10 of 06.08.2010, 040/11 of 08.08.2011, 053/11 of 11.11.2011, 006/13 of 31.01.2013, 055/16 of 17.08.2016, 092/17 of 30.12.2017, 082/20 of 06.08.2020
- General Law on Obligations “Official Gazette of Montenegro”, No. 047/08, 004/11, 022/17
- Law on Consumer Protection “Official Gazette of Montenegro”, No. 002/14 006/14, 043/15, 070/17, 067/19)
- Digital Transformation Strategy
- Draft Law on Digital Assets
- Draft Law on Games of Chance and Prize Games

Currently, there is no explicit law addressing DMA matters in Montenegro. In general, competition matters are covered by the Competition Protection Law. An upcoming law in the field of digital assets may be suitable to address certain DMA regulatory aspects.

Transparency

Some transparency related rules in Montenegrin laws are found in the Law on E-Commerce according to which the provider of ISS must ensure that every piece of information in a commercial ISS message meets certain conditions. This Law also regulates the use of electronic communication for sending unsolicited commercial messages. Transparency in B2B transactions in relation to terms and conditions that are to be accepted by service users must be in line with general requirements from the law that regulates contracts and torts.

Accountability

Accountability mechanisms from the perspective of personal data protection can be found to some extent in the current Law on Personal Data Protection. This Law is harmonised with Directive 95/46/EC. A draft of the GDPR-compliant law was published in 2019, but it is hard to predict when it will be adopted.

Complaints related rules can also be found in the Law on E-Communications, as its provision outlines the rights of the users to submit complaints to service operators regarding access, quality of services, and billing issues. The Law regulates the complaints procedure and deadlines. If the complaint is rejected or the operator fails to respond, the user can bring the issue to the relevant Agency.

Interoperability

There are no rules in Montenegro on interoperability specifically addressing any CPS.

It might be worth mentioning that the Digital Transformation Strategy focuses on interoperability, but it is mostly related to data communication within the public sector.

Mobility

There are no rules in Montenegro that would regulate mobility-related DMA values.

Demonopolisation/Deconcentration

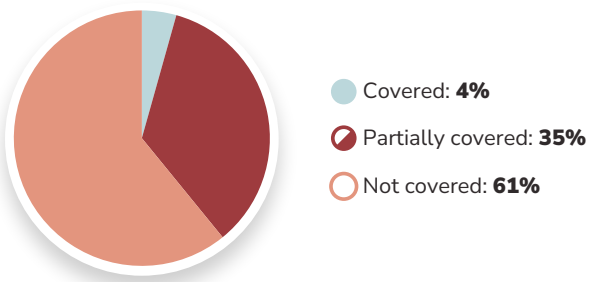
Some rules that address demonopolisation and deconcentration values can be found in the Law on E-Commerce, the Law on E-Communications, as well as in competition and consumer protection laws.

The Competition Protection Law regulates any restrictive agreements or abuse of dominant position on a general sector non-specific level. It can be used as a legal basis to support the DMA's provisions, as it enforces rules

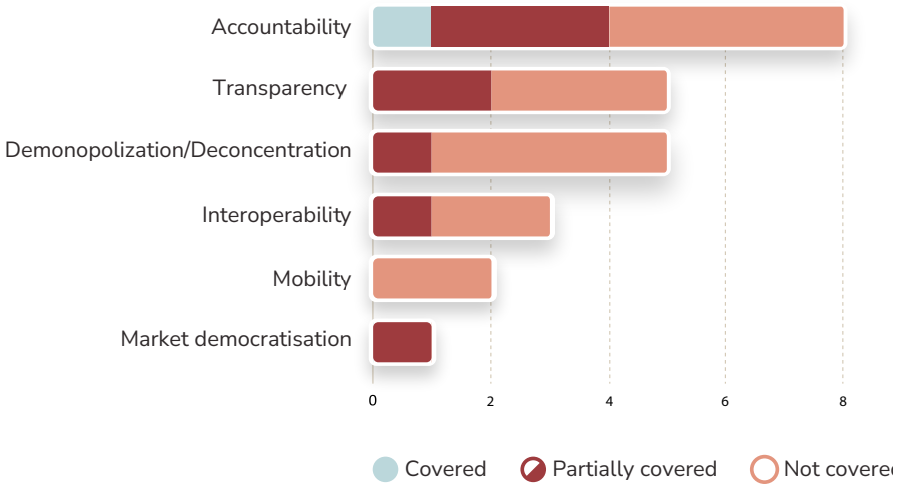
against anti-competitive practices that could hinder the freedom of ISS to set prices and conditions, ensuring a competitive and fair market environment.

The Law on E-Commerce regulates multiple matters that might be helpful for achieving demonopolisation/deconcentration goal, but only indirectly (for example the obligations of ISS providers with the aim to ensure compliance with various regulatory areas such as copyright, industrial property rights, and consumer contracts or their responsibilities and liabilities regarding data storage, transmission, and access to third-party data). These rules promote the freedom to provide services without bureaucratic hurdles, enhance market access and opportunities for service providers and protect consumers from deceptive practices and unwanted communications.

The Consumer Protection Law requires traders to adhere strictly to the displayed prices and obliges traders to advertise prices by relevant laws. It also contains rules for price reductions and clearance sales, including conditions and transparency requirements.



Coverage of DMA-related rules in North Macedonian regulation



Coverage of DMA-related values in North Macedonian regulation, by rules

DMA-related Regulation References in North Macedonia:

- Law on Electronic Commerce (Macedonian Official Gazette No. 133/07, 17/11, 104/15, 192/15, and 31/20)
- Personal Data Protection Law (Macedonian Official Gazette No. 42/2020 and 294/2021)
- Law on Electronic Communications (Macedonian Official Gazette No. 39/14, 188/14, 44/15, 193/15, 11/18, 21/18)

» Law on Protection of Consumers (Macedonian Official Gazette No. 236/2022)

In North Macedonia the Law on E-Commerce deals with ISS in general, although it does not define CPSs. Other sectoral laws may also regulate DMA-like topics to some extent.

Transparency

Some transparency-related rules are to be found in the Law on E-Commerce and the Law on Consumer Protection.

The Law on E-Commerce stipulates obligations for ISS providers to clearly provide information on commercial communication they undertake.

The Law on Consumer Protection stipulates that traders or sellers must clearly and freely provide information and data regarding themselves and their offer for trade before any agreement is reached. Consumers should never be confused about the substantial nature of the trade or the trader.

Accountability

There are several sectoral laws that regulate certain DMA-like accountability aspects.

For example, accountability rules with respect to personal data protection are to be found in the Law on the Protection of Personal Data. In case of data protection related violations, complaints mechanisms from this Law can also be used. In addition, the Consumer Protection Law recognises remote contracting (via the internet, for example), which is a characteristic of ISS/CPS. So if the ISS user is a natural person, some rights granted by this Law might be available to them.

The Law on Consumer Protection also tackles non-discrimination obligations as it obliges the traders to give access to public services under non-discriminatory conditions. As defined, public services include provision of water, electricity, heating, public telecommunication, communal cleanliness,

public transportation, public parking, etage (condominium) management, and public economic services.

The right to complaint is to some extent regulated in the Law on Consumer Protection that regulates the requests of the natural or legal person whose rights are or have been violated through the provision of the ISS. According to this Law, a consumer is allowed to submit a complaint on all and any infringement of rights stipulated by the same Law, including in regards to public services (as defined). The provider of public or other services is obliged to respond to a submitted complaint within 15 days of the receipt. This law also stipulates penalties for non-compliance in regards to ISS provision.

Interoperability

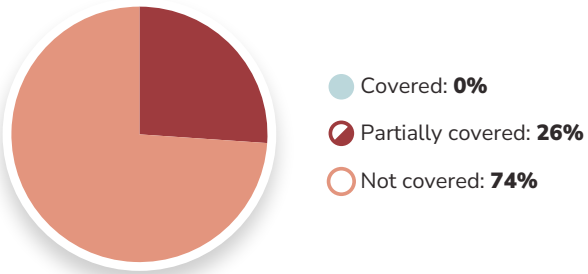
There are no rules in North Macedonia on interoperability specifically addressing any CPS.

Mobility

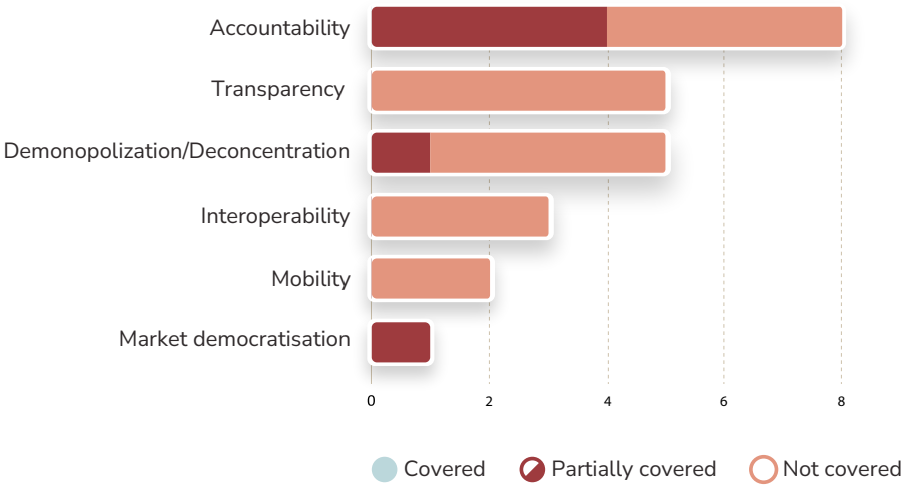
There are no rules in North Macedonia that would regulate mobility-related DMA values.

Demonopolisation/Deconcentration

There are no rules in North Macedonia that would regulate demonopolisation/ deconcentration-related DMA values. There is, of course, a general law on the protection of competition, which stipulates demonopolisation and deconcentration powers for the Commission for the protection of competition. This Law is not tailored specifically to digital markets.



Coverage of DMA-related rules in Serbian regulation



Coverage of DMA-related values in Serbian regulation, by rules

DMA-related Regulation References in Serbia:

- Law on Electronic Commerce (Official Gazette of RS no. 41/2009, 95/2013 and 52/2019)
- Trade Law (Official Gazette of RS, no. 52/2019)
- Law on Protection of the Competition (Official Gazette of RS no. 51/2009 and 95/2013)
- Personal Data Protection Law (Official Gazette of RS, no. 87/2018)
- Consumer Protection Law (Official Gazette of RS, no. br. 88/2021)

There are no laws in Serbia that would regulate DMA issues as such, but a few general or sectoral laws cover some of those issues from various angles.

Namely, Serbia has the Law on E-Commerce that regulates the provision of information society services, in the same vein with the EU Directive on E-Commerce. According to a definition from this Law, information society service is "a service that is provided at a distance, as a rule for a fee through electronic equipment for processing and storing data, at the personal request of the service user, and in particular online trading, offering data and advertising on the internet, electronic search engines, as well as enabling the search for data and services that are transmitted over an electronic network, providing access to the network or storing data of service users".

Therefore, in addition to the general ISS definition that is in line with a definition from DMA (i.e. Directive (EU) 2015/1535), definition from the Law on E-Commerce also includes some of the CPSs, like online search engines or online advertising services. Nonetheless, because of the lack of Serbian practice when it comes to interpretation of the ISS definition from the Law on E-Commerce, it would be difficult to clearly establish what the exact overlap is between this definition and the CPS definition from DMA. For example, it is not clear whether "storing data of service users" is the same service as "cloud computing services" from DMA.

Serbian Trade Law contains the definition of "electronic platform" as a means by which a person in the capacity of an information society service provider, provides a connection service to parties trading electronically. The person that manages the electronic platform can also sell their own goods/services through that platform. However, the only rules with respect to these platforms in this Law concern trade issues with the end users, in their consumer capacity.

When it comes to fair competition rules, there are no rules that regulate the digital market specifically, but Serbia has an EU-harmonised general Law on Protection of the Competition.

Some relevant issues might be covered by personal data or consumer protection laws, or general civil law procedure rules.

Transparency

There are no DMA-like transparency rules in Serbia's laws, but few sectoral rules are relevant for some of these aspects.

With respect to transparency in the context of contracts conclusion, there are several laws that regulate some aspects of the contracts concluded at distance or contracts concluded in the e-form, such as the Law on E-Commerce, the Consumer Protection Law or the Trade Law. These may regulate information that must be provided by service providers in the course of contract conclusion.

With respect to ISS providers' reporting obligations, general competition laws may be relevant. Namely, in the sectoral analysis of the state of competition on the market of digital platforms for mediation in the sale and delivery of mainly restaurant food and other products in the period 2020-2021, the Serbian Commission for Protection of Competition noted that the only law in Serbia that regulate this area of digital services is the Law on E-Commerce. It also noted EU regulatory development via DMA, and in the "proposals" part of the opinion it recommended the adoption of further regulation in Serbia. As a concrete measure, the Commission proposed the establishment of a "Digital platforms registry". This proposal was not further elaborated, so there is no available information as to what would be the content of the registry, nor would there be any reporting obligations for providers of digital platform providers.

Accountability

Accountability rules that might be relevant for the provision of CPS in Serbia relate mostly to those that involve the processing of personal data. Serbia has a GDPR-harmonised personal data protection law that would apply on a general level also in the context of provision of any ISS, when it comes to complaints mechanisms, right to data portability, or collection of personal data.

When it comes to the right to complain, it should also be noted that according to Serbian laws, one cannot waive in advance their right to bring a claim to

the court on any matter (i.e. any provision in any contract where the end-user would waive the right to sue the ISS provider would be null and void).

The Law on E-Commerce regulates misdemeanour fines for violations of that law, which might also be relevant for some ISS that would fall into the CPS category.

Interoperability

There are no rules in Serbia that would regulate interoperability-related DMA values.

Mobility

There are no rules in Serbia that would regulate mobility-related DMA values.

Demonopolisation/Deconcentration

Rules concerning demonopolisation/deconcentration in Serbia are to be found only in general competition protection regulation. When it comes to ISS provision it might be worth mentioning that the Serbian Commission for Protection of Competition conducted a sectoral analysis of the state of competition on the market of digital platforms for mediation in the sale and delivery of mainly restaurant food and other products in the period 2020-2021, that was published in February 2023. Services on this market have been qualified as ISS by the Commission. During this analysis, in the contracts concluded by Glovo (one of two major digital platforms in this area, in addition to Wolt) with its partners, the Commission had insight into contractual provisions that could have the effect of excluding or hindering the expansion of other, competitive platforms. There were also provisions that could amount to discrimination against partners through the application of unequal business conditions, all of which constitute an abuse of a dominant position. For this reason, the Commission initiated the procedure ex officio to examine potential abuse of a dominant position against Glovo. The results of these investigations are still not publicly available.

When it comes to rules regarding offers addressed to end users of any CPS or other ISS, or concluding the contracts with the end users, there are rules in the Law on E-Commerce on communication with the end users and contracts concluded at distance that are in line with the Directive on E-Commerce, but no rules similar to those from DMA.

AIA REGULATORY MECHANISM

The previously identified normative values of the AI Act are closely connected, which also affects the identified rules and mechanisms. Most of the rules and mechanisms do not fall into one single value, i.e. they are intertwined, and for the sake of easier interpretation and the context of two other Acts covered in this study, we have categorised the rules according to the most dominant value out of the three: transparency, harm prevention and reduction, and oversight.[17]

TRANSPARENCY RULES AND MECHANISMS

Transparency obligations for providers and deployers

One of the intentions of the AI Act is to provide more transparency of systems and AI in general, not only between different actors that develop and use AI systems, but also towards individuals.

In that sense, there are detailed transparency obligations for providers and deployers, outlined in Articles 13, 50, and 86. Providers have the obligation to enable transparency of the AI system functioning towards deployers, including via preparation of instructions for use, in order to enable deployers to interpret the system's output and use it appropriately. However, this raises an issue of entities deploying AI systems being bound by instructions from companies that develop AI systems, and consequently potentially being legally liable if they don't abide by these instructions. Deployers and providers have the obligation to disclose that certain material is artificially generated or manipulated. Deployers of an emotion recognition system or a biometric categorisation system, outside of those that are banned, must notify natural persons exposed to the system of its operation. Deployers of a high-risk AI system must provide to affected persons subjected to a significant decision,

17 Preventing and adressing adverse effects of AI, as a central and more general value within the AIA, has not been considered in detail from the perspective of corresponding rules, and from a comparative perspective with the Western Balkans. However, it has been quantified since one identified rule adresses this value in a broader sense - the existence of regulations regarding AI.

taken by the deployer on the basis of the output from such a system, clear and meaningful explanations on the role of the AI system in the decision-making procedure and the main elements of the decision taken. But, taking into account the intrusiveness of some AI systems, such as those for biometric categorisation, the transparency measures envisaged by the AI Act does not prevent the harmful effects they can cause.

Obligation to register high-risk AI systems in the EU database

Given the potential number of high-risk AI systems that will fall under the scope of the AI Act, EU lawmakers envisioned a database which will contain information in order to better understand who is responsible for a specific AI system.

The database aims to provide transparency of high-risk systems deployed in the EU and establish the responsible persons of providers or deployers, as per Articles 49, 60, and 71. Providers and/or deployers of certain high-risk AI systems must register themselves and the system in the EU database, which is kept by the Commission and is publicly available. They must do so before placing the system on the market or putting it into service. A serious downside however is that not all the information contained in the database will be publicly available, as the AI Act provides for blanket exceptions (i.e. law enforcement or migration use).

Reporting of serious incidents

Reporting of incidents concerning AI systems is key for system security, safeguarding personal data, especially sensitive data, as well as fundamental human rights. Article 3(49) defines a “serious incident” as an incident or malfunctioning of an AI system that directly or indirectly leads to any of the following: (a) the death of a person, or serious harm to a person’s health, (b) a serious and irreversible disruption of the management or operation of critical infrastructure, (c) the infringement of obligations under EU law intended to protect fundamental rights or (d) serious harm to property or the environment.

Therefore, in accordance with Article 73, providers of high-risk AI systems must report any serious incident to the competent authorities (i.e. market

surveillance authorities of the Member States where the incident occurred) and must perform the necessary investigations.

Personal data and data governance

As per Articles 10 and 59 of the AI Act, personal data used in training datasets must be subjected to data governance and management practices, which includes transparency about the original purpose of the data collection. Special categories of data can be exceptionally used for training for the purposes of ensuring bias detection and correction in relation to the high-risk AI systems. For AI regulatory sandbox purposes, personal data lawfully collected for other purposes can be used for training under special conditions. Data sets that do not have personal data must also be used within compliance with data governance and management practices appropriate for the intended purpose of the AI system (which take into account, for example, design choices, the formulation of assumptions, examination in view of possible biases, identifying the relevant data gaps).

HARM PREVENTION AND REDUCTION RULES AND MECHANISMS

AI systems are regulated depending on the risk (risk based approach regulation)

In order to understand the subject matter of the AI Act, the initial approach is that the AI systems are regulated depending on the risk, i.e. it is a risk-based regulatory instrument, and it is covered in Article 1. There are however two approaches to risks: one concerns the specific risk of a particular system, while the other takes into account general risk regarding a certain area and use cases (e.g. law enforcement, as stated in the Annex III of the AI Act). Harm to citizens is claimed to be the reasoning behind the regulation and the main interpretative tool, but the risk-based product safety approach directed at innovation is not fully suited for effective human rights protection, as previously argued. The level of regulation of AI systems depends on the risk (potential harm) they can cause and the regulated categories and practices covered by the AI Act are unacceptable risk (prohibited AI practices), high risk

(heavily regulated AI systems) and limited or minimal risk (limited rules for some systems, e.g. concerning transparency).

It is important to note that the paragraph 3 of Article 2 exempts national security competences of Member States from the provisions of the AI Act, which is open for broad interpretation on the national level and can be seen as a workaround to use invasive AI systems. The same goes for AI systems exclusively used for military, defence, or national security purposes, which are covered by an exception as well.

Some AI systems are prohibited

Another key point to understand at the beginning is that the AI Act prohibits specific AI practices outlined in Article 5 which by default cannot be sold or used, as it is deemed they bear unacceptable risk of harm. These include AI systems used for the following practices:

- Deployment of subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques to distort the behaviour, effectively impairing the ability to make an informed decision.
- Exploitation of people's vulnerabilities, disability or a specific social or economic situation to materially distort the behaviour in a manner that could cause significant harm.
- Evaluation or classification of natural persons or groups of persons based on their social behaviour or known, inferred or predicted personal or personality characteristics, i.e. "social scoring".
- Making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics.
- Creating or expanding facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage.
- AI systems used to infer emotions of a natural person in the workplace and education institutions, with the exception of medical or safety reasons.

- Biometric categorisation systems that categorise natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation.
- Real-time remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement. However, there are exceptions for which objectives real-time biometric identification systems can be used, those being:

  (1) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, and search for missing persons,

  (2) prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack,

  (3) the localisation or identification of a person suspected of having committed a crime, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II of the AI Act (which contains a list of specific criminal offences).

The matters become more complicated when it comes to allowing the generally forbidden practice of the use of real-time remote biometric identification systems, as there are additional exceptions, such as that the use of such systems may start without them being registered in the EU database of high-risk systems or without a carried out fundamental rights impact assessment "in duly justified cases of urgency" (Article 5, paragraph 2). Another exception which leaves a lot of doubt into the practical aspects is the provision in Article 5, paragraph 3 that prior authorisation granted by a judicial authority or an independent administrative authority issued upon a reasoned request is needed for the use of real-time remote biometric identification. However, there is an exception that "in a duly justified situation of urgency", the use of such a system may be commenced without an authorisation, provided that

such authorisation is requested without undue delay, at the latest within 24 hours.

In addition, the exceptions to rules banning the use of real-time remote biometric identification systems can be prescribed on the national level (Article 5, paragraph 5), which can also lead to varying standards and broad interpretations across the Member States.

Requirements for high-risk AI systems

As mentioned, in addition to sanctioning and preventing forbidden practices, the crux of the AI Act is the risk-based regulation of systems deemed as high-risk. Classification rules for high-risk AI systems are outlined in Article 6, based on the EU harmonisation legislation for various products and safety components (in detail covered in Annex I) or used for one of the purposes listed in Annex III. The eight areas of application of high-risk AI systems listed in Annex III are as follows:

- Biometrics: Remote biometric identification systems, as well as biometric categorisation and emotion recognition systems.
- Critical infrastructure: Management and operation of critical digital infrastructure, road traffic, supply of utilities (water, gas, heating or electricity).
- Education and vocational training.
- Employment, workers' management and access to self-employment.
- Access to essential private and public services and benefits.
- Law enforcement: Assessing the risk of a person becoming the victim of criminal offences, polygraphs or similar tools, etc.
- Migration, asylum, and border control management.
- Administration of justice and democratic processes.

It should be noted however that high-risk only apply for specific uses in a particular area: one such example in education and vocational training are AI systems intended to be used for monitoring and detection of prohibited behaviour of students during tests in the context of or within educational and vocational training institutions at all levels.

The specified use cases of these very intrusive systems, as listed in detail in Annex III, present a high-risk according to the AI Act and therefore the corresponding systems must fulfil detailed standards in order to reduce the risks as much as possible. When it comes to the requirements for AI systems, they are outlined in Section 2 of the Chapter III on high-risk systems (Articles 9-15) and include a mandatory risk management system, rules on training data and data governance, detailed technical documentation as outlined in Annex IV, recording logs of events in the system, transparency and provision of system information to deployers, human oversight, and finally, requirements concerning accuracy, robustness and cybersecurity.

Requirements for general-purpose AI models

Another subject of regulation extensively covered by the AI Act (Chapter V) are the general-purpose AI (GPAI) models. General-purpose AI models (GPAI) are potentially very powerful - systems can be built upon them and used for a multitude of purposes which can produce significant risks for human rights and social processes. Well-known examples of such AI models include GPT-4,[18] Stable Diffusion[19] and Midjourney.[20]

However, one of the key aims of the AI Act is to regulate GPAI models which are deemed to have systemic risks, as prescribed in Article 51. Article 3(65) defines "systemic risk" as a risk specific to the high-impact capabilities of GPAI models which have significant impact on the Union market due to their reach, actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights or the society as a whole, that can be propagated at scale across the value chain. According to Article 51, the GPAI model can be classified to have systemic risk if it is evaluated to "high impact capabilities", or based on a Commission decision that it has equivalent capabilities or impact in accordance with the detailed criteria as outlined in

18 OpenAI, "GPT-4", 14 March 2023, https://openai.com/index/gpt-4-research/

19 Midjourney, "Version", https://docs.midjourney.com/docs/model-versions

20 Stability AI, "Stable Diffusion Public Release", https://stability.ai/news/stable-diffusion-public-release

Annex XIII. Finally, a GPAI model will also be classified to have a systemic risk if a high amount of computation[21] was used for its training.

The obligations concerning GPAI models are mostly aimed at their providers, which according to Article 53 are required to have the necessary technical documentation of the model, at minimum including information prescribed in Annex XI, and to provide the information and documentation to the providers of AI systems, so they would have good understanding of the capabilities and limitations of the model, and contain at minimum the elements of Annex XII. Providers of free and open source licensed models are exempted from these two requirements only if they don't have systemic risks. Additional requirements include EU copyright legislation compliance and making public a summary about the content used for training the model. As per Article 54, providers of GPAI models from third countries also have to appoint an authorised representative established in the EU, which is important since the two countries with the most influence on the AI market are the US and China.

On the other hand, providers of GPAI models with systemic risks have additional obligations apart from those set out in Articles 53 and 54, which as per Article 55 include:

- Performing model evaluation, including adversarial testing to identify and mitigate systemic risks.
- Assessing and mitigating possible systemic risks and their sources that may stem from the development, distribution, or the use of GPAI models.
- Tracking and reporting serious incidents and corrective measures to the AI Office and where appropriate national competent authorities.
- Ensuring adequate cybersecurity of the GPAI model and its physical infrastructure.

21 For more information on the importance of compute for AI see: J. Vipra, S. Myers West, "Computational Power and AI", AI Now Institute, 27 September 2023, https://ainowinstitute.org/publication/policy/compute-and-ai

Risks management, technical documentation, keeping of logs, accuracy and cybersecurity

Among the key requirements for high-risk systems is that they are evaluated throughout their whole lifecycle, so that new risks are identifiable. Articles 9, 11, 12, and 15 cover these obligations in detail.

There are detailed rules on how risk management must be set up for high-risk AI systems. The aim of the risk management is to implement a continuous and regularly updated process that runs throughout the entire lifecycle of a high-risk AI system, until it is placed on the market. Providers must also prepare technical documentation before placing an AI system on the market, which must be drawn up in such a way as to demonstrate that the high-risk AI system complies with the regulated requirements. In order to ensure a level of traceability of the AI system's functioning, high-risk AI systems must technically allow for the automatic recording of events ("logs") over the duration of the lifetime of the system. High-risk AI systems must be designed to achieve an appropriate level of accuracy, robustness, and cybersecurity. The accuracy metrics must be declared in the instructions of use. But as already noted, this can prove to be quite problematic - e.g. system instructions intended for use by government bodies or entities are written by corporate actors, which means that the governmental use of the system is essentially privately dictated.

Obligations of importers and distributors

An important part of the AI Act is that responsibility along the value chain (i.e. among all the actors in connection with an AI system) will ensure that the AI system will be compliant throughout its lifecycle. This particularly concerns importers and distributors of AI systems who will be placing them on the EU market.

As per Articles 23 and 24, importers and distributors of high-risk AI systems must fulfil a regulated set of obligations, aimed to verify AI system conformity with prescribed requirements, which includes the documentation keeping and management obligations, verifying that conformity assessment procedure is conducted and they must cooperate with competent authorities. If an importer

or distributor has reasons to believe that an AI system is non-compliant, they must not make that AI system available on the market until all issues are resolved.

Fundamental rights impact assessment

As the application of technology should be human-centred, fundamental rights must be respected in line with national regulations and international standards and one of the mechanisms envisioned by the AI Act is the fundamental rights impact assessment for high-risk AI systems, prescribed as an obligation for deployers in Article 27.

Deployers of high-risk AI systems that are bodies governed by public law, or private operators providing public services and operators deploying certain high-risk AI systems, such as banking or insurance entities, must carry out a fundamental rights impact assessment prior to putting it into use. Such assessment should identify the specific risks to the rights of individuals or groups who are likely to be affected, as well as identify measures to be taken in case of the materialisation of these risks. The deployer must notify the market surveillance authority of the results of the assessment. On the other hand, there are no requirements or consequences in case risks are identified in the assessment but not mitigated, or if there are unacceptable residual risks, which raises a question into the effectiveness of the assessment process.

Obligations in relation to post-remote biometric identification

When it comes to obligations of deployers concerning post-remote biometric identification systems, Article 26, paragraph 10 outlines rules for their use. New obligations and measures for deployers are aimed to reduce the likelihood of abuses of these very intrusive systems, but given that the measures (e.g. annual reports with aggregate data) are limited and dubious as to whether they can prevent abuses in practice, the doubts regarding their effectiveness remain.

Namely, in the framework of an investigation for the targeted search of a person convicted or suspected of having committed a criminal offence, the deployer of an AI system for post-remote biometric identification must request

prior authorisation by a judicial or administrative authority for the use of the system. Such AI systems shall not be used for law enforcement purposes in an untargeted way, without any link to a criminal offence or proceeding, a genuine threat of a criminal offence, or the search for a specific missing person. No decision that produces an adverse legal effect on a person may be taken by the law enforcement authorities solely based on the output of this system. Each use of these systems must be documented and made available to the relevant market surveillance authority and the national data protection authority upon request. Deployers must submit annual reports on the uses of this system.

OVERSIGHT RULES AND MECHANISMS

Obligations of providers

Not all AI systems will be able to be launched in the EU in accordance with the AI Act - providers of high-risk AI systems would have to fulfil obligations to be in position to legally offer their products. These are covered in detail in Section 3 of the chapter on high-risk systems, more specifically in Articles 16-22.

Providers of high-risk AI systems must fulfil, inter alia, the following: (a) have a quality management system in place that must be documented in a systematically via written policies, procedures and instructions, (b) keep prescribed documentation for 10 years after AI system has been placed on the market or put into service (c) keep automatically generated logs for specific time periods, (d) where and as required, take corrective actions to bring AI system into conformity, to withdraw it, to disable it, or to recall it, (e) cooperate with competent authorities, (f) appoint EU representatives, as applicable.

Obligations of deployers

Similarly to importers and distributors, deployers, i.e. entities using the systems, also have obligations in the context of the responsibility along the value chain for high-risk AI systems. However, deployers of such systems

have a bigger legal burden and responsibility, as they are in essence the users of these systems.

In line with Article 26, deployers of high-risk AI systems must fulfil, inter alia, the following: (a) ensure they use a system in accordance with the instructions of use, (b) assign appropriate human oversight, (c) ensure that input data is relevant in view of the intended purpose of the system, (d) inform the relevant stakeholder that use of the system may produce a risk or that serious incident occurred, and suspend its use, (e) keep the logs automatically for specific time periods, (f) cooperate with competent authorities.

Human oversight

Technology is not infallible, and AI-based systems are prone to error, for example when producing outputs based on visual inputs (image, video). These errors can lead to serious consequences for humans, such as wrongful arrests or criminal investigations, denial of social welfare services, and the like. Although human oversight is a control mechanism described in Article 14, the problems of automation bias will still be difficult to handle when it comes to operating the system.

High-risk AI systems must be designed in such a way to be effectively overseen by natural persons, in order to enable preventing or minimising risks to health, safety, or fundamental rights. The concrete measures will depend on the risks, level of autonomy, and context of use of the AI system. The designated person must fully understand the capacities and limitations of the AI system, monitor output for signs of anomalies, dysfunctions, and unexpected performance ("automation bias"). That person must also have the power to decide not to use the AI system in any particular situation or to otherwise disregard, override, or reverse the output, as well as to intervene by stopping the system to a halt in a safe state.

Conformity assessment procedure

The conformity assessment procedure is one of the most important elements of the AI Act, as the idea is that the harmonised standards will ensure common AI safety measures across the EU.

The conformity assessment procedure is covered by Article 43. Providers of high-risk AI systems must verify their compliance with mandatory obligations and requirements via a conformity assessment procedure, under regulated conditions. However, since the standards are developed by private entities, it will be very difficult for this process to actually be transparent and inclusive, in particular when it comes to including civil society and human rights experts. The exact rules of this procedure depend on the concrete AI system and provider in question. High-risk AI systems that have already been subject to a conformity assessment procedure must undergo a new procedure whenever they are substantially modified, regardless of whether the modified system is intended to be further distributed or continues to be used by the current deployer.

The conformity assessment procedure for high-risk systems in point 1 of Annex III (Biometrics) can be either an internal control as referred to in Annex VI, or an external assessment of the quality management system and the technical documentation with the involvement of a notified body as per Annex VII. However, for high-risk systems from points 2 to 8 of Annex III - essentially everything other than biometrics - only an internal control in accordance with Annex VI is prescribed. This is a very controversial provision as the most invasive systems, such as those intended for border control or law enforcement purposes, will be assessed by the providers themselves.

Post-market monitoring

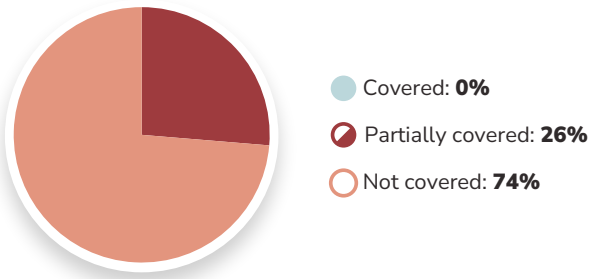
Given the pace of AI development, monitoring systems enable continuous tracking of how the systems are used in the market and whether they are still in compliance with the AI Act and other applicable regulations. In accordance with Article 72, high-risk AI systems providers must establish and document a post-market monitoring system based on post-market monitoring plan that actively and systematically collects and analyses relevant data (provided by deployers or collected through other sources) in order to allow the provider to evaluate the AI system continuous compliance.

Penalties

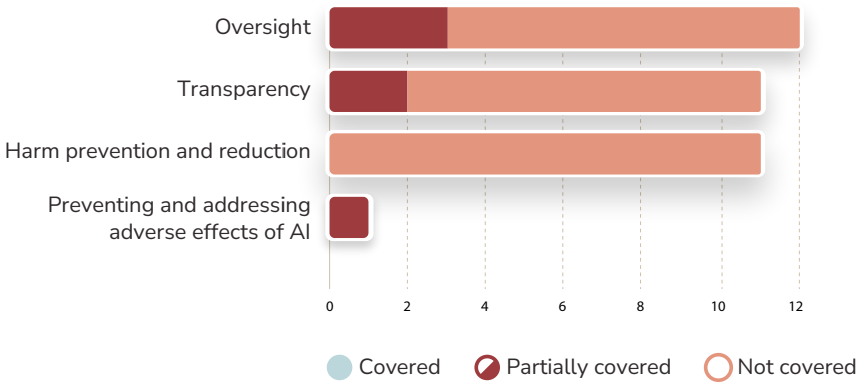
Large monetary fines should not just be “a cost of doing business” for most companies - they can also affect their reputation which can influence their stock prices, among other things, so in the long run, the tech companies sometimes strategise to invest in compliance to avoid being exposed for continuous legal breaches. Also, given the ex ante regulatory approach of the AI Act, some violations will be easier to pinpoint. Penalties under the AI Act, including general ones, those intended for EU entities and providers of GPAI models, are prescribed by Articles 99-101.

For violation of the banned AI practices rules, administrative fines can be up to 35,000,000 EUR or, if the offender is a company, up to 7% of its total worldwide annual turnover for the preceding financial year. For other substantive violations fines are up to 15,000,000 EUR or, if the offender is a company, up to 3% of turnover calculated in the same manner. Fines up to or up to 7,500,000 EUR or, if the offender is a company, up to 1 % turnover are prescribed for supply of incorrect, incomplete or misleading information to notified bodies and national competent authorities.

ALBANIA



Coverage of AIA-related rules in Albanian regulation



Coverage of AIA-related values in Albanian regulation, by rules

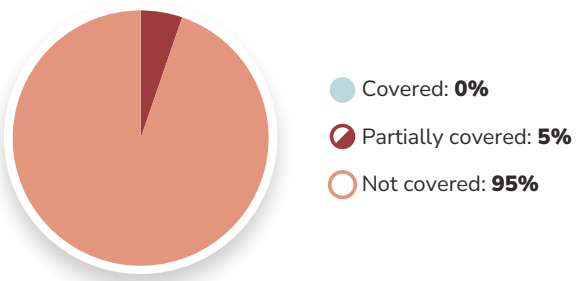
AIA-related Regulation References in Albania:

- Law on Electronic Government (Official Gazette of the Republic of Albania, No. 43/2022)
- Law on Personal Data Protection (Official Gazette of the Republic of Albania, No. 9887/2008)
- Instruction on defining rules to protect the security of personal data processed by large processing entities (No. 47/2018)
- Decision of the Council of Ministers

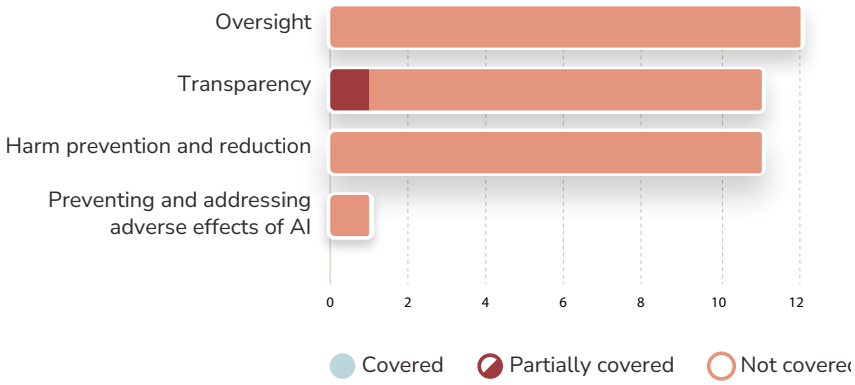
» In Albania, there are currently no laws or regulations that deal with AI systems use.

The only law that mentions AI is the Law on E-Government according to which artificial intelligence technology should be used wherever possible in the information and communication technology systems for purposes of enhancing and innovating the digital economy. The methodology and technical standards for AI use should be established upon the Decision of the Council of Ministers, which has still not been issued.

The law that regulates personal data protection would govern any use of personal data in the context of AI uses, so any values related to AI regulation in Albania would be covered from that angle. This includes the obligation of the data controller to perform a data protection impact assessment prior to any personal data processing activity.



Coverage of AIA-related rules in BiH regulation



Coverage of AIA-related values in BiH regulation, by rules

AIA-related Regulation References in BiH:

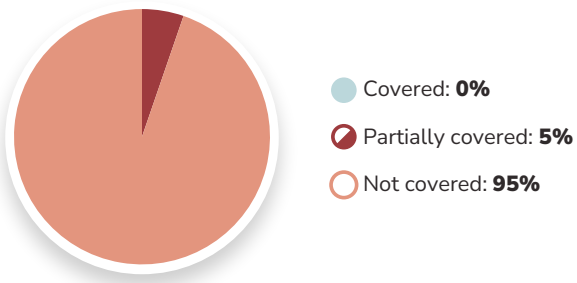
» Law on Protection of Personal Data (Official Gazette of BIH, nos. 49/06, 76/11 and 89/11)

In Bosnia and Herzegovina, there are currently no laws or regulations that deal with AI systems use.

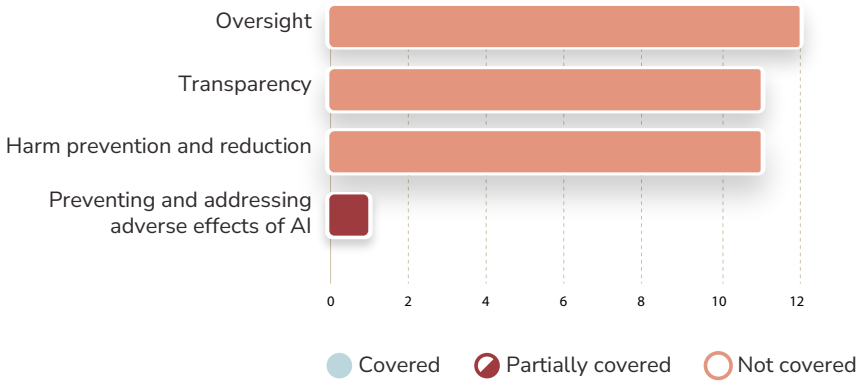
Same like in Albania, some AI-related values are regulated from a personal data protection angle. Namely, the Law on Protection of Personal Data

recognises situations when decisions about persons are based solely on the automatic processing of their personal data and provides rules on how and when such processing is permissible. These rules are similar to those contained in the GDPR, and do to some extent regulate the obligation for human intervention within AI systems.

In Republika Srpska, according to the Information Security Law, incidents that threaten public interest must be reported to National CERT, which should also include AI technology-related incidents.



Coverage of AIA-related rules in Kosovo regulation



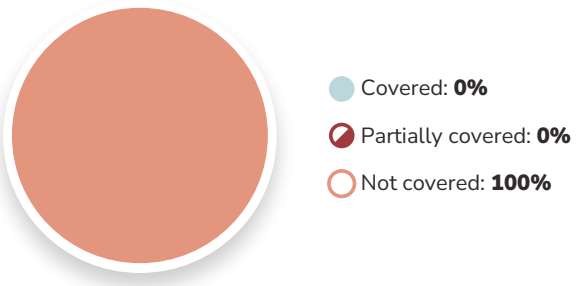
Coverage of AIA-related values in Kosovo regulation, by rules

AIA-related Regulation References in Kosovo:

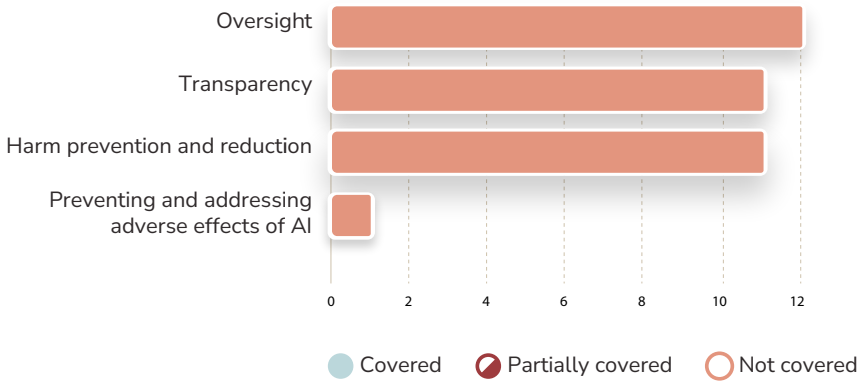
» Framework Agreement between the European Union and Kosovo on the general principles for the participation of Kosovo in Union programmes (published on July 27, 2017)

In Kosovo, there are currently no laws or regulations that deal with the use of AI systems.

In the absence of any legal rules or guidance, it might be worth mentioning that Kosovo is participating in the European Union's Digital Europe Programme that aims to enhance access to digitalisation for citizens, businesses, and institutions, as well as in the area of artificial intelligence through strategic grants.



Coverage of AIA-related rules in Montenegrin regulation

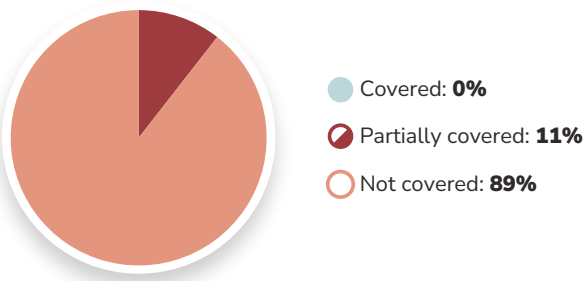


Coverage of AIA-related values in Montenegrin regulation, by rules

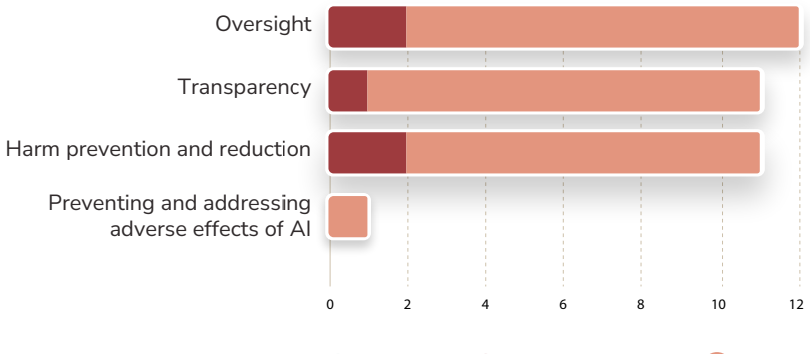
AIA-related Regulation References in Montenegro:

» No relevant references

In Montenegro, there are currently no laws or regulations that deal with AI systems use.



Coverage of AIA-related rules in North Macedonian regulation



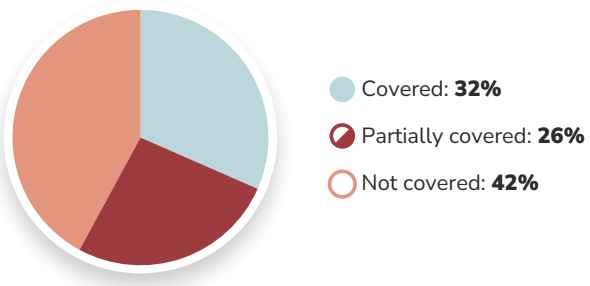
Coverage of AIA-related values in North Macedonian regulation, by rules

AIA-related Regulation References in North Macedonia:

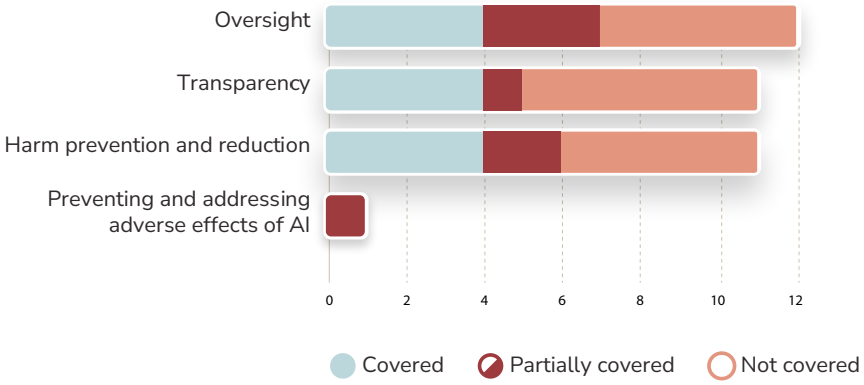
- Law on Protection of Consumers (Macedonian Official Gazette No. 236/2022)
- Personal Data Protection Law (Macedonian Official Gazette No. 42/2020 and 294/2021)

In North Macedonia, there are currently no laws or regulations that deal with AI systems use.

As in other Western Balkan countries in this study, some rules in personal data protection regulation might be relevant for some aspects of AI use. For example, the Law on Personal Data Protection might be relevant in scenarios of post-remote biometric identification, as it specifically recognises biometric data which are defined as a 'special personal data category'.



Coverage of AIA-related rules in Serbian regulation



Coverage of AIA-related values in Serbian regulation, by rules

AIA-related Regulation References in Serbia:

- Ethical guidelines for the development, implementation and use of reliable and responsible artificial intelligence (Official Gazette of RS no. 23/2023)
- Artificial Intelligence Development Strategy in the Republic in Serbia for period 2020-2025 (Official Gazette of RS no. 66/2019)
- Action plan for the period 2020–2022 for the implementation of the Artificial Intelligence Development Strategy in the Republic of Serbia for the period 2020-2025 (Official Gazette of RS no. 81/2020)

- Decision on the establishment of the Research and Development Institute for Artificial Intelligence of Serbia (Official Gazette of RS no. 24/2021 and 38/2021)
- Memorandum of Understanding between the Cabinet of the Minister in Charge of Innovation and Technological Development in the Government of the Republic of Serbia and the Ministry of Industry and Trade of the Czech Republic on cooperation in the field of innovation, artificial intelligence and robotics (Official Gazette of RS no. 12/2019)
- New Artificial Intelligence Development Strategy announced by a Government PR until mid-2024 (no draft is available yet)

Most relevant rules regarding the production and use of AI systems in Serbia are to be found in a soft law instrument called "Ethical guidelines for the development, implementation, and use of reliable and responsible artificial intelligence" (Guidelines) that were issued by the Serbian Government in February 2023. These Guidelines came out as one output from the "Artificial Intelligence Development Strategy in the Republic in Serbia for the period of 2020-2025" (Strategy) which was adopted by the Serbian Government in December 2019. The Strategy is accompanied with the "Action plan for the period 2020–2022 for the implementation of the Artificial Intelligence Development Strategy in the Republic of Serbia for the period 2020-2025" (Action Plan), adopted by the Serbian Government in June 2020.

The Guidelines first set out the four basic principles that should serve as a starting point for creation, application and use of AI systems. These are: explainability and verifiability, dignity, prohibition of damages, and fairness. In the next chapter it moves on to regulate "Conditions of Reliable and Responsible Artificial Intelligence". According to these rules, the construction and creation of a reliable and responsible AI system require the fulfilment of conditions, which are based on the established principles, and which are determined through: (i) action (mediation, control, participation) and supervision; (ii) technical reliability and safety; (iii) privacy, personal data protection, and data management; (iv) transparency; (v) diversity, non-discrimination, and equality; (vi) social and environmental well-being; and (vi) liability.

These conditions consist of verifiable parameters via technical and non-technical methods, which confirm and prove the fulfilment of the principles. The goal of technical methods is to guide the development, application and use of AI systems to behave reliably, minimising potential unintentional and unpredictable damage to humans and society as a whole. Technical methods are presented in the form of recommendations. Non-technical methods refer to the examination of organisational and other non-technical elements important for the development and use of AI systems. These methods are given in the form of a questionnaire that is intended to evaluate individual AI systems in terms of the fulfilment of the basic principles and the conditions.

This detailed reasoning of the Guidelines is based on the goals outlined in the Strategy, in particular the special goal named “Ethical and safe application of artificial intelligence”.

In addition, there is an institution in Serbia called the “Research and Development Institute for Artificial Intelligence of Serbia” (AI Institute) which was founded by the Serbian Government in March 2021. It does not have legislative powers but could participate with its expertise in various regulatory efforts.

The indication for regulatory efforts in Serbia in the area of artificial intelligence can also be found in the fact that Serbia has international treaties with the Czech Republic and UAE on cooperation in the field of artificial intelligence.

In May 2024 the government established a working group with the mandate to prepare a draft law that regulates AI systems for public discussion until the end of March 2025.

Transparency

The Guidelines regulate various aspects of transparency value in the contact of AI systems use and production. Transparency is one of the explicitly regulated conditions that any AI system should fulfil according to the Guidelines. It is operationalised via a set of questions in the Questionnaire and transparency-related Recommendations. The transparency rules revolve around traceability, explainability and notification requirements for end users.

With respect to the training phase, use of data sets and data management, training of AI systems is in the Guidelines specifically regulated under the Recommendations for "technical reliability and safety". It is also touched upon in other related parts of the Guidelines.

In the Strategy, one of the goals is "Ethical and safe application of artificial intelligence" one of the planned measures within this goal is "Protection of personal data in the field of artificial intelligence". Within this measure, the aims are: (i) the development of a practical diagram of the necessary steps that need to be implemented in relation to the protection of personal data in the development of solutions based on AI, to be applied equally in all sectors of society and (ii) certification of AI products and solutions to ensure the protection of personal data and compliance with international ethical standards.

In the Action Plan, there were two activities related to these Strategy measures that are planned for 2021: (i) the development of a methodology for the application of personal data protection standards in the field of artificial intelligence, and (ii) the application of personal data protection standards in software solutions based on artificial intelligence. Based on publicly available information, these activities were not completed at the time of writing.

The processing of the personal data for the purpose of AI system training could be done only in accordance with the general rules from the personal data protection law.

There are currently no registration or notification obligations, when it comes to AI systems generally or reporting of incidents. Incidents regulated under the Information Security Law that threaten public interest must be reported to the National CERT. According to the Personal Data Protection Law, incidents related to personal data must be reported to the Serbian supervisory body (the rules are essentially the same as those in the GDPR).

At the moment, the only institution that is established in Serbia to specifically deal with AI development and deployment is the AI Institute. According to the Decision on its establishment, its activities are primarily directed to research,

publishing, and educational purposes. In that capacity, the AI Institute is not well suited to act as a regulatory or registration body.

Harm prevention and reduction

The Guidelines recognise harm- and risk-based approach of AI systems regulation. They contain a detailed explanation of the high-risk AI system. According to the Guidelines, a high-risk system is a system that has a tendency to directly or indirectly violate the principles and conditions established by the Guidelines, but does not necessarily do so. In practical terms, the Guidelines list the types of such AI systems, in a manner clearly inspired by the AI Act draft that was available at the time the Guidelines were issued.

In the definitions part of the Guidelines it is stated that "from the point of view of the Guidelines, high-risk systems are not considered undesirable, but precisely because of the mentioned impact, the importance of the areas of life in which they are applied, and the possibilities and range of influence on man and his integrity, it is necessary to analyse them separately and evaluate their impact". However, the text of the Guidelines does not clearly spell out if it is only applicable to high-risk AI systems (or to any AI system), nor does it further make distinction between high-risk and other AI systems.

No AI system is specifically prohibited, but the Guidelines stipulate that they are not applicable to AI systems that are forbidden by some special law. Thus, there is a presumption in the Guidelines that some AI systems may or ought to be prohibited (with no further guidelines or rules to that effect).

Considering obligations of the various participants in AI system development and use, there are no rules in the Guidelines differentiating between the operators in the manner done in the AI Act. However, there are detailed rules for management on documenting obligations under the Recommendations for "action (mediation, control, participation) and supervision" condition. It is also touched upon in other related parts of the Guidelines. Keeping the logs is not specifically mentioned.

On the other hand, the Guidelines explicitly mention the obligation to prepare Data Protection Impact Assessment, as is regulated in the Serbian

Data Protection Law. Also, throughout the Questionnaire there are questions about whether the provider made assessment of impacts on the environment, interested stakeholders, and the society as a whole. One of the Recommendations under the condition "social and environmental well-being" is for providers to establish a standardised approach to assessing the impact on people, organisations, the whole society, democracy, and the environment. The provider is expected to have assessment mechanisms in place throughout the lifecycle of the AI system.

In Serbia, there are still no rules or practices regarding the general-purpose AI models.

There are also no rules regarding post-remote biometric identification. However, there were several proposals of such rules in the past (2022 and 2023) put out by the Ministry of Internal Affairs, via proposals for amendments of the policing laws and the Criminal Procedure Law. On both occasions they were withdrawn under public pressure because the Ministry of Internal Affairs didn't produce an acceptable Data Protection Impact Assessment, necessary under the Personal Data Protection Law.

Oversight

As mentioned, when it comes to obligations to be fulfilled for AI system use and production, there is no distinction in the Guidelines between providers, deployers, importers, or distributors. There are different sets of obligations for providers as well as parameters for regulating the methods for demonstrating compliance with ethical principles. These are outlined in a direct or indirect manner, but jointly they constitute a sort of "to-do" list for a provider that develops AI systems.

There are no conformity assessment rules in an explicit manner, but application of the Guidelines and answering the questions from the Questionnaire can serve for conformity verification purposes.

When it comes to human oversight, the Guidelines contain definitions of: (i) human intervention (human in the loop); (ii) human supervision (human of the loop); and (iii) human decision-making (human in command). These concepts

are further developed within the Questionnaire under the condition for “action (mediation, control, participation) and supervision”, but there are no specific Recommendations addressing them.

Currently, there are no penalties or other sanctions in the context of AI system development and use.

DSA-DMA-AIA: INSTITUTIONAL FRAMEWORK

All three Acts analysed in this study have established a specific institutional framework designed to ensure the implementation and consistent enforcement of the newly introduced rules. This diversified framework includes a variety of traditional institutions at both the EU and national levels, and it assigns institutional roles to various actors in the European digital ecosystem — from experts and expert bodies to citizens. This chapter outlines the core institutions and institutional roles defined in the DSA, DMA, and AIA.

DSA INSTITUTIONAL FRAMEWORK

DSA adopts a comprehensive and systemic approach, embodying a broad and diverse institutional framework marked by multistakeholderism and horizontality. This framework entails the involvement of various institutions at both national and EU levels. Some institutions predate this Act, while others are newly established under the DSA. Additionally, diverse actors, including recipients, users, researchers, and experts, play institutional roles alongside traditional authorities. They participate both individually and within various entities in enforcing the new DSA rules. Below are the institutions and bodies making up the institutional framework for the DSA.

EU

European Commission

The European Commission plays a crucial role in the DSA enforcement mechanism. Firstly, the Commission designates the status of very large online platforms and very large online search engines (VLOPSE) for those online platforms and search engines with an average of 45 million or more monthly active recipients within the Union (Article 33). As of now, there is no official

methodology for counting monthly active recipients in the EU, and therefore, the designation fully relies on self-declared numbers by VLOPs and VLOSEs. According to Article 43, VLOPSEs are required to pay an annual supervisory fee to the Commission, which also determines the amount. Furthermore, the Commission has the authority to supervise and enforce the DSA concerning VLOPSEs (Article 56) and to monitor the assessment of systemic risks and infringements (Articles 64, 65, 66).

As elaborated in Article 57 of the DSA, the Commission cooperates with the Board. For instance, in collaboration with the Board, it publishes comprehensive reports on the most prominent systemic risks (Article 35) and can initiate certain crisis response mechanisms (Article 36). Additionally, the Board can refer issues of disagreement or lack of communication to the Commission if necessary (Articles 59, 60). The Commission holds a specific role within the structure of the Board. The Commission holds a specific role within the structure of the Board. While the Board is chaired by the Commission, the Commission does not have voting rights. Furthermore, the Commission provides administrative and analytical support to the Board. Any rules and procedures adopted by the Board must have the consent of the Commission (Article 62).

Furthermore, the Commission supports the development and implementation of voluntary standards (Article 44) and voluntary codes of conduct that contribute to the implementation of the Act (Article 45). It also facilitates transparent advertising (Article 46) and ensures online services are accessible to persons with disabilities (Article 47). Additionally, the Commission has a role in initiating crisis protocols for VLOPSEs concerning public security and public health (Article 48).

According to the DSA, the Commission has significant investigative and sanctioning powers. It can request information in cases of suspected infringement or non-compliance with the DSA (Article 67), conduct interviews with any natural or legal person for the purpose of investigation (Article 68), and conduct inspections at the premises of VLOPSEs (Article 69). If necessary, the Commission can order interim measures against VLOPSEs (Article 70). Non-compliance can result in fines up to 1% of the worldwide annual turnover

of the provider. Additionally, periodic penalties up to 5% of the average daily worldwide turnover can be imposed for each day of delay in responding to requests for information or allowing inspections.

The Commission is authorised to take necessary actions to monitor compliance by VLOPSEs (Article 72), adopt "non-compliance decisions" (Article 73), and impose fines. Starting from 17 February 2024, the Commission can apply fines of up to 6% of the worldwide annual turnover and impose periodic penalties of up to 5% of the average daily worldwide turnover for each day of delay in complying with remedies (Articles 74, 76). On the other hand, VLOPSEs have the right to be heard (Article 79). The period for the imposition and enforcement of penalties is limited to five years (Articles 77, 78). Additionally, the Commission may adopt implementing acts concerning the practical arrangements for its intervention (Article 83).

According to DSA, the Commission is mandated to establish and maintain a reliable and secure information-sharing system to facilitate communication between Digital Services Coordinators, the Commission, and the Board (Article 85). Additionally, the Commission is granted the power to adopt delegated acts, subject to specific conditions (Article 87).

Finally, according to the DSA, the Commission may develop guidelines on several key areas: online interface design and organisation (Article 25), online protection of minors (Article 28), the methodology for calculating the number of average monthly active recipients of the service (Article 33), and the structure, organisation, and functionalities of the repository of information about advertisements (Article 39).

European Board for Digital Services

The European Board for Digital Service is an independent advisory group consisting of Digital Services Coordinators (DSCs) that advises DCSs and the Commission in order to contribute to the consistent application of the DSA rules and effective cooperation of the DSCs and the Commission. The Board assists the DSCs and the Commission in the supervision of very large online platforms, coordinates and contributes to guidelines and analysis regarding standards and emerging issues. (Article 61 and 63) As stated in Article 62,

the Board is composed of national DSCs and is chaired by the Commission, which does not have voting rights.

Court of Justice of the European Union

In accordance with Article 261 TFEU, The Court of Justice of the European Union has unlimited jurisdiction to review decisions by which the Commission has imposed fines or periodic penalty payments. According to Article 81, it may cancel, reduce, or increase the fine or periodic penalty payment imposed.

MEMBER STATES

Digital Services Coordinators

Articles 49, 50, and 51 delineate the roles, requirements, and powers of Digital Services Coordinators (DSCs). These coordinators are national-level institutions tasked with supervising, enforcing, and monitoring the DSA within their respective Member States. Their responsibilities encompass coordinating DSA enforcement nationally while contributing to consistent supervision and enforcement across the Union. DSCs collaborate with each other, other national authorities, the Board, and the Commission. They possess the authority to request data access, conduct inspections, and impose fines on intermediary service providers within their jurisdiction in case of infringements. Additionally, DSCs are tasked with certifying “trusted flaggers” and overseeing out-of-court dispute resolution bodies.

The Digital Services Coordinator of establishment refers to the DSC of the Member State where the main establishment of an intermediary service provider is located, or where its legal representative resides or is established. The Digital Services Coordinator of the destination is the DSC of a Member State where the intermediary service is provided (Article 3).

Certified out-of-court dispute settlement bodies

Certified out-of-court dispute settlement bodies are independent third parties, certified by national DSCs, which resolve disputes related to decisions taken by the provider of the online platform service. (Article 21)

INTERMEDIARY SERVICES PROVIDERS

Points of Contacts

All intermediary services must designate two points of contact. The first point of contact is designated by providers of intermediary services to enable their communication with Member States' authorities, the Commission, and the Board (Article 11). It enables a formal, certain, efficient, institutionalised communication between providers and authorities, overcoming issues arising from various contacts, inaccessibility, or avoidance of communication by providers. The other one enables recipients of the service to communicate directly with providers of intermediary services (Article 12). It enables user-friendly, not entirely automated, direct and rapid communication between recipients and the service provider, which makes a provider open and accessible for citizens who use an intermediary service.

Legal Representative

Legal representative is a legal or natural person designated by providers of intermediary services which do not have an establishment but offer services in the EU, to act as their legal representative in one of the Member States where the provider offers its services. (Article 13)

Compliance Officer

According to Article 41, VLOPSEs must establish compliance officers. They are assigned to monitor the compliance of the provider with the DSA. The head of the compliance function raises concerns regarding risks or non-compliance and ensures that risk-mitigation measures are taken. Additionally, they cooperate with the DSC of establishment and the Commission.

EXPERTS AND AUDITORS

Trusted flaggers

Trusted flaggers are independent entities awarded by Digital Services Coordinators with particular expertise and competence for detecting,

identifying and notifying illegal content. The notices regarding illegal content submitted by them must be treated with priority as they are expected to be more accurate than notices submitted by an average user. According to Article 22, trusted flaggers publish, at least once a year, easily comprehensible and detailed reports on submitted notices.

Independent auditors

The role of independent auditors is to assess compliance of VLOPSEs with DSA obligations at least once a year (Article 37). Mandatory templates of the audits' report and VLOPSEs implementation reports provide their comparability. VLOPSEs afford carrying out the audits, as well as cooperation and assistance necessary to conduct audits in an effective, efficient and timely manner. They must provide access to relevant data and premises, and answer all questions if needed, without any influence or undermining the independence of the auditor.

CONSUMERS AND RECIPIENTS OF SERVICES

Recipient of the service

According to Article 3, recipients of the service are natural or legal persons who use an intermediary service, in particular for the purposes of seeking information or making it accessible. As clarified in Recital 2, the intention or purpose of using an intermediary service does not impact the recipient of the service status: Business users, consumers, and other users are all considered to be recipients of the service under the DSA (Recital 2).

Active recipient of an online platform is recipient of the service that has engaged with an online platform by either requesting the online platform to host information or being exposed to information hosted by the online platform and disseminated through its online interface. Active recipient of an online search engine recipient of the service that has submitted a query to an online search engine and been exposed to information indexed and presented on its online interface. (Article 3)

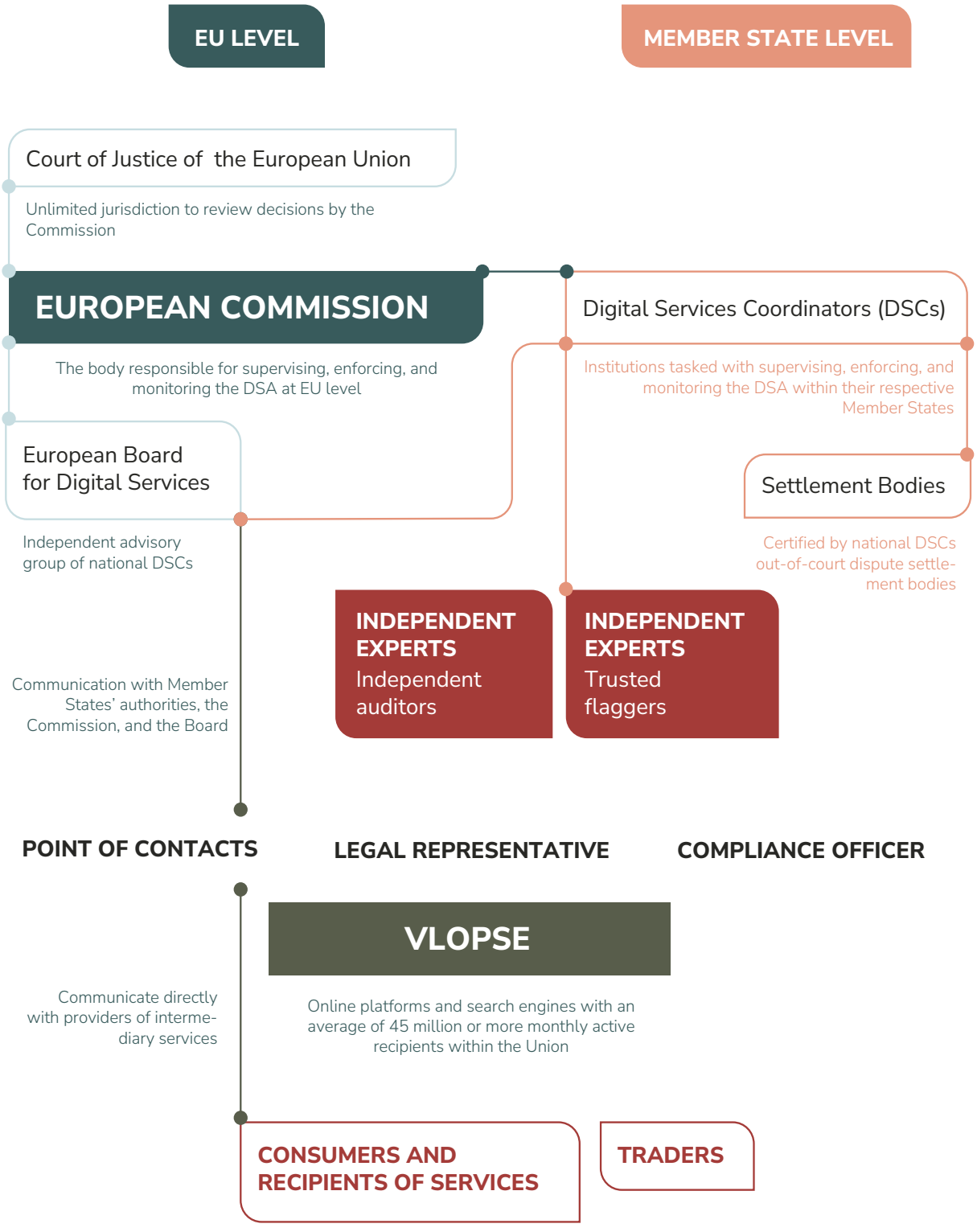
Consumer

According to DSA, a consumer is any natural person who is acting for purposes which are outside his or her trade, business, craft, or profession (Article 3).

Trader

Trader is defined as any natural or any legal person, who is acting for purposes relating to his or her trade, business, craft or profession (Article 3).

DSA INSTITUTIONAL FRAMEWORK



DMA INSTITUTIONAL FRAMEWORK

EU

European Commission

The Commission has the authority to designate gatekeepers and impose sanctions for non-compliance to Regulatory rules. The Commission is also the highest body that liaises with all other enforcement bodies and it holds the executive decision-making power. The Commission also has the oversight in regards to the consultation on implementation with member states (Article 37), providing information on respective enforcement and transmitting information or opinions (Article 38), submitting written observations to national courts (Article 39), establishing high level group (Article 40), providing secretariat services (Article 40), opening market investigations upon request of Member States (Article 41), publication of decisions (Article 44), and implementing acts (Article 46).

European Data Protection Supervisor

The European Data Protection Supervisor (EDPS) is a member of the High-level group for the Digital Markets Act. The Commission will consult the EDPS when drafting implementing acts, methodologies and procedures for company audits. The EDPS was also consulted before the Regulation was put into effect. (Articles 40 and 46)

European Data Protection Board

The Board is composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives. The Board will communicate its activities with the Commission and will have voting rights with respect to decisions which concern principles and rules applicable to the Union institutions, bodies, offices, and agencies which correspond in substance to those of this Regulation.

European Competition Network

The network consists of the 27 competition authorities within the EU and the DG Competition of the European Commission. The ECN has no new authority and has consequently no rights over its members. (Articles 38 and 40)

MEMBER STATES

National courts

National courts of Member States are poised to have oversight in instances where private litigants take action regarding the violation of rules related to the DMA. This can also include class action lawsuits. National courts cooperate with the Commission to ensure the adequate enforcement of the Regulation as well as to alert the Commission in cases where national litigation is being taken in regards to the DMA. In cases where national courts determine it is impossible to rule, the cases will be presented to the Court of Justice of the European Union.

National competent authorities

According to Article 37, the National competent authorities (NCA) are tasked with supporting the Commission in its enforcement responsibilities. The NCA can collect and forward complaints to the Commission, as well as upon request assist with providing expertise and experience to the Commission for further rulings. NCAs can also assist in market investigations and have a binding transparency agreement with the Commission and thus have insight into all data collected by the Commission which is obtained through gatekeepers. NCAs can also initiate taking action against gatekeepers if they observe violations to specific national competition laws. They can also in certain cases conduct independent investigations if authorised by national legislation and upon notifying the Commission beforehand.

EXPERTS

Digital Markets Advisory Committee

As outlined in the Article 50, the DMA Committee holds the authority to investigate potential infringements and is consulted by the Commission before making decisions related to the Regulation. The Committee is made up of representatives from Member States, including among others, relevant experts that can speak to the issues the Committee might face in its assessment.

High-level group for the Digital Markets Act

The High-level group for the Digital Markets Act is composed of national experts and has a consultative role to the Commission. Beyond observations and consultations, the group can also recommend additions, modifications or removal of rules based on observations of their real-world applications in the sector. The group also submits a yearly report to the Commission and EU Parliament which is based on the efficacy of the Regulation as well as an assessment of its interaction with current sector rules. (Article 40)

BUSINESS AND END USERS

Gatekeepers

A company is designated as a gatekeeper if it (1) has significant impact on the market, (2) provides a specified service that is an important gateway for business users to reach end users like app stores, search engines, and web browsers and (3) enjoys an entrenched and durable position (or it is foreseeable that it will enjoy such position in the near future).

Any company with more than 45 million monthly active users and a market capitalisation of 75 billion euros ($82 billion) is considered the gatekeeper providing a core platform service.

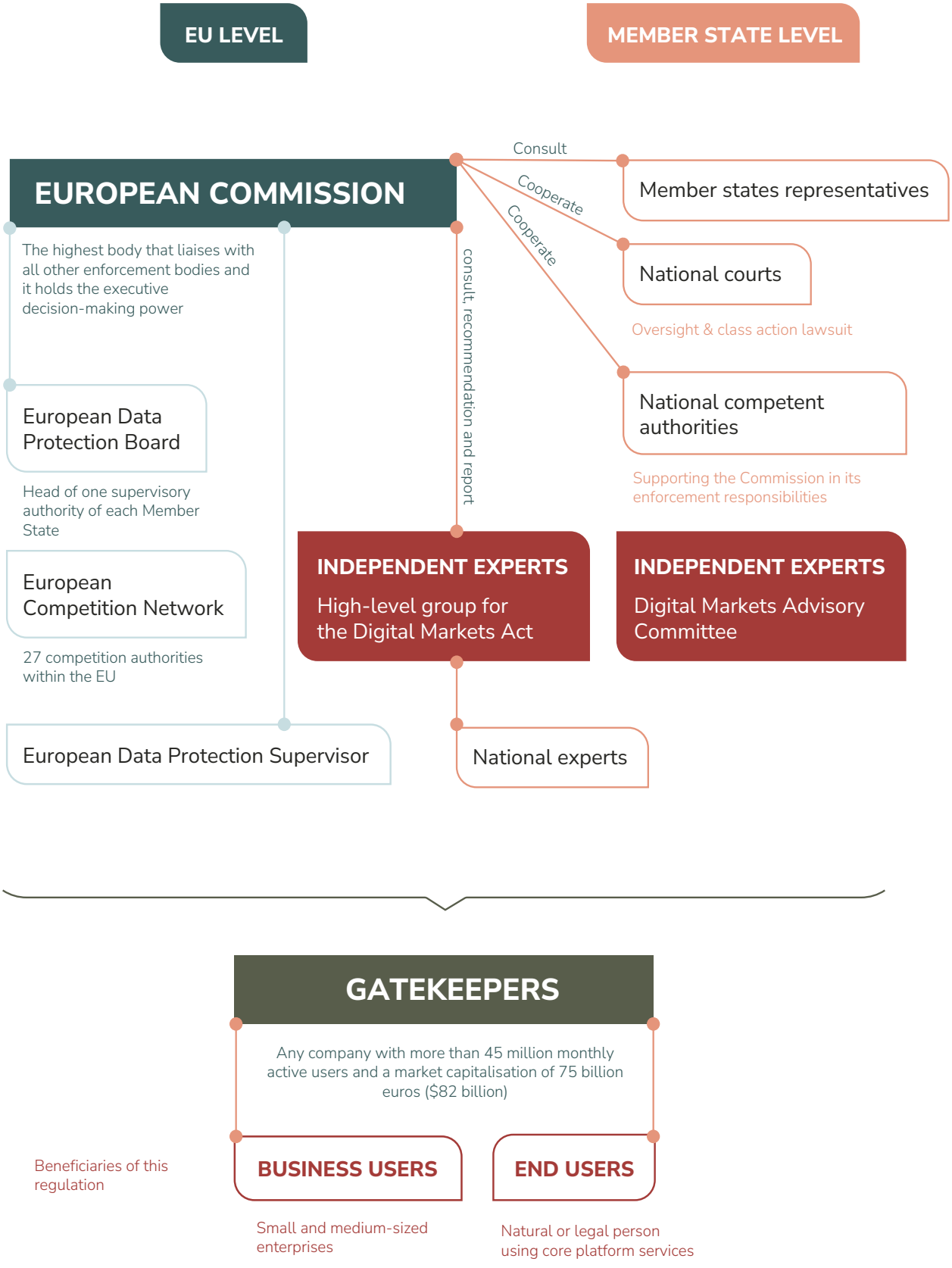
Business users

In order to ensure fair business practices on the digital market, business users are also expected to act according to the DMA rules while also benefiting from gatekeepers' compliance at the same time. Small and medium-sized enterprises or small and medium-sized businesses are businesses whose personnel and revenue numbers fall below certain limits and they represent 99% of all businesses in the EU.

End users

End users represent any natural or legal person using core platform services other than as a business user. Next to business users, end users are the main beneficiaries of this regulation. The DMA aims to improve and increase end users' rights by enhancing transparency, accountability, plurality of choice and mobility of information in regards to business users and gatekeepers' practices.

DMA INSTITUTIONAL FRAMEWORK



AIA INSTITUTIONAL FRAMEWORK

Although there are institutions both on the EU and Member State level which are authorised to oversee various matters related to other legislation, for example data protection and fundamental rights, the AI Act prescribes the formation of new bodies to make enforcement of the AI Act more efficient. Since the AI Act is a comprehensive legislation regulating a new and complex area, Member States will require particular support and assistance from the wider institutional framework, especially given the level of expertise required for efficient oversight and enforcement. Below are the institutions and bodies making up the mapped institutional framework for the AI Act.

EU

European Artificial Intelligence Office (AI Office)

One of the main new bodies envisaged by the new AI legislative framework is the European Artificial Intelligence Office, or AI Office for short. The AI Office was established in January 2024 within the European Commission's Directorate-General for Communication Networks, Content and Technology (DG Connect).[22] The Office was created for the Commission to take on a proactive regulatory role for AI-related matters, similar to the approach laid out in the DSA and the DMA.

According to the Commission's Decision on establishing the AI Office, it will have a wide range of tasks and responsibilities, such as:

- Developing tools, methodologies and benchmarks for evaluating capabilities of general-purpose AI models.
- Monitoring the implementation and application of rules on general-purpose AI models and systems.
- Monitoring the emergence of unforeseen risks stemming from general-purpose AI models.

22 European Commission Decision C(2024) 390 Establishing the European AI Office, 24 January 2024, https://digital-strategy.ec.europa.eu/en/library/commission-decision-establishing-european-ai-office

- Investigating possible infringements of rules on general-purpose AI models and systems, including by collecting complaints and alerts.
- Ensuring that when an AI system falls under the scope of EU legislation where the Commission has supervision and enforcement powers, such as the DSA or the DMA, the supervision and enforcement tasks are coordinated.
- Supporting the implementation of rules on prohibited AI practices and high-risk AI systems in coordination with relevant bodies, etc.

The Commission has also foreseen additional enforcement tasks for the AI Office, such as assisting the Commission with preparing decisions, implementing and delegation acts, and facilitating the uniform application of the AI Act. Having in mind that the AI Act prescribes many technical requirements and that implementation oversight will be quite challenging, the AI Office will also assist the Commission in the preparation of guidance and guidelines to support the practical implementation of the AI Act and contribute to the provision of technical support, advice, and tools for the establishment and operation of AI regulatory sandboxes and coordination with national competent authorities. Given its institutional position, the AI Office should also encourage and facilitate the drawing up of codes of practices and codes of conducts at Union level.

In addition, the Office will also be the key body for cooperation within the Commission, as well as with other EU bodies and institutions and stakeholders (providers of AI models, experts from the scientific community and the educational sector, citizens, civil society, open source community, etc.) in line with applicable competition rules.

European Artificial Intelligence Board

Another new body envisaged to help with the implementation of the AI Act is the European Artificial Intelligence Board, i.e. the AI Board. Established in accordance with Article 65 of the AI Act, it consists of representatives from each EU Member State, as well as the European Data Protection Supervisor in observer capacity. In addition, representatives of the AI Office can also attend

the Board's meeting without taking part in voting. Representatives of other national and EU authorities, bodies or experts may be invited to the meetings by the AI Board if the matters are relevant for them.

Tasks of the AI Board are outlined in Article 66 of the AI Act. The main activity of the Board is to advise and assist the Commission and the Member States in order to facilitate the consistent and effective application of the AI Act. Some of the most important tasks of the Board include contributing to the coordination among national competent authorities responsible for the application of the AI Act and supporting joint activities of market surveillance authorities, collecting and sharing technical and regulatory expertise and best practices among Member States, providing advice in the implementation of the AI Act, in particular regarding the enforcement of rules on general-purpose AI models, etc. The Board can also issue recommendations and opinions by its own initiative or upon request from the Commission.

Advisory forum

In order to provide a multi-stakeholder approach, Article 67 of the AI Act prescribes the establishment of an Advisory forum, which will comprise of "a balanced selection of stakeholders, including industry, start-ups, SMEs, civil society and academia" appointed by the EU Commission. Several key EU bodies and agencies (e.g. Fundamental Rights Agency, European Union Agency for Cybersecurity - ENISA) will have permanent representatives in the forum.

The key task of the Forum is to advise and provide technical expertise to the AI Board and the Commission in order to contribute to their tasks under the AI Act. The Advisory forum can also prepare opinions, recommendations, and written contributions upon request of the AI Board or the Commission.

Scientific panel of independent experts

In accordance with Article 68 of the AI Act, the Commission will establish a panel of independent experts intended to support enforcement activities. Article 68 in paragraph 3 prescribes that the scientific panel will shall advise and support the European AI Office, particularly in context of tasks such

as supporting the implementation and enforcement as regards general-purpose AI models and systems, supporting the work of market surveillance authorities at their request, supporting cross-border market surveillance activities, as well as supporting the AI Office when carrying out its duties in the context of the safeguard clause pursuant to Article 81. Article 69 contains provisions to allow Member States access to the pool of experts to support their enforcement activities. In addition, the scientific panel may provide an alert to the AI Office in regards to potential systemic risks of general-purpose AI systems in line with Article 90.

European Data Protection Supervisor

As one of the existing institutions fitting into the new AI regulation framework, the European Data Protection Supervisor (EDPS) is the data protection supervisory authority for EU institutions, bodies or agencies, in accordance with Regulation (EU) 2018/1725.[23]

When EU entities (institutions, bodies, or agencies) fall within the scope of the AI Act, the EDPS acts as their supervisory authority (Article 3(48), Article 70, paragraph 9 of the AI Act). In accordance with Article 57, paragraph 3, the EPDS can also set up an AI regulatory sandbox for EU entities and exercise the roles and the tasks of national competent authorities. In addition, the EDPS acts as the EU entities' market surveillance authority, except in relation to the Court of Justice acting in its judicial capacity (Article 74, paragraph 9). Based on Article 43 paragraph 1, the EDPS shall be the notified body for conformity assessment when the system is intended to be put into service by EU entities. The EDPS can also issue administrative fines to EU entities (Article 100).

MEMBER STATES

National competent authorities - market surveillance authorities

Article 70 of the AI Act outlines the designation of national competent authorities by the Member States, i.e. at least one notifying authority and at

23 Regulation (EU) 2018/1725 of the European Parliament and of the Council, 23 October 2018, https://eur-lex.europa.eu/eli/reg/2018/1725/oj

least one market surveillance authority. The Member States are obliged to designate a market surveillance authority to act as a single point of contact for the AI Act and notify the Commission of this.

In accordance with Article 73, providers of high-risk AI systems need to report any serious incident to the market surveillance authority of the Member States where the incident occurred. Also, Article 74 (paragraphs 12 and 13) prescribes that market surveillance authorities can have access to the documentation in regards to high-risk AI systems, training, validation and testing datasets, as well as source code in exceptional cases. When the national market surveillance authority is unable to conclude its investigation on the high-risk AI system because of its inability to access certain information related to a general-purpose AI model, it may request from the AI Office to be granted access pursuant to Article 75, paragraph 3. When it comes to real world testing of AI models, the market surveillance authorities have the competence and powers to ensure that testing in real world conditions is in accordance with the AI Act (Article 76).

Additional important roles of the market surveillance authorities include dealing with AI systems presenting a risk at national level (Article 79), dealing with AI systems wrongly classified by the provider as a not high-risk (Article 80) and ordering corrective measures for compliant high-risk AI system that still present a risk for health or safety of persons, fundamental rights, or to other aspects of public interest protection (Article 82). The market surveillance authorities also serve as bodies to which natural and legal persons can lodge complaints in case they suspect an infringement of the provisions laid out by the AI Act (Article 85).

The competent authorities should also establish at least one AI regulatory sandbox at national level, operational 24 months after entry of the AI Act into force. This sandbox may also be established jointly with one or several other Member States' competent authorities (Article 57).

National competent authorities - notifying authorities

According to Article 3(19), the notifying authority is the national authority responsible for setting up and carrying out the necessary procedures for the

assessment, designation and notification of conformity assessment bodies and for their monitoring, further outlined in Art. 28-39. As noted above, the competent authorities should also establish at least one AI regulatory sandbox at national level, operational 24 months after entry of the AI Act into force. This sandbox may also be established jointly with one or several other Member States' competent authorities (Article 57).

Conformity assessment bodies - notified bodies

According to Article 3(21), conformity assessment bodies are legal entities that perform third-party conformity assessment activities, including testing, certification and inspection when it comes to requirements for high-risk AI systems laid out in Chapter III, Section 2 (Art. 9-15) of the AI Act (Risk management system, Data and data governance, Technical documentation, Record-keeping, Transparency and provision of information to deployers, Human oversight, Accuracy, robustness, and cybersecurity).

In order to become notified bodies, the conformity assessment bodies must submit an application to the national notifying authority of a Member State in which they are established, in line with Article 29. However, as per Article 39, the bodies can also be established in third countries with which the EU has a concluded agreement, provided that they meet the requirements in Article 31 or ensure an equivalent level of compliance.

National authorities protecting fundamental rights

AI systems have a potentially profound effect on human rights and therefore it was necessary to include national authorities protecting fundamental rights (e.g. independent antidiscrimination bodies and agencies) in the AI Act institutional framework. Article 77 of the AI Act provides national fundamental rights authorities the possibility to access information about high-risk AI systems. More specifically, Article 77 prescribes that the national public authorities or bodies which supervise or enforce the respect of fundamental rights, i.e. equality bodies which have a mandate only on non-discrimination and equality and national human rights institutions (NHRIs) which have a remit for all human rights, have the power to request and access any documentation created or maintained under the AI Act in relation to the use of high-risk AI

systems referred to in Annex III when it is necessary for effectively fulfilling their mandate within the limits of their jurisdiction. The relevant public authority or body needs to inform the market surveillance authority of the Member State concerned of any such request. When the documentation is deemed as insufficient to determine whether a breach of fundamental rights has occurred, the national authority protecting fundamental rights may ask the market surveillance authority to organise a testing of the high-risk AI system through technical means (Article 77, paragraph 3).

National data protection supervisory authorities

Given that EU Member States are already bound to provisions of the GDPR[24] and the Law Enforcement Directive,[25] their national data protection supervisory authorities (DPAs) would be included in the AI Act taking into account the effects of AI on personal data processing. Based on Article 74, paragraph 8, for high-risk AI systems listed in point 1 (Biometrics) of Annex III, if the systems are used for law enforcement purposes, border management and justice and democracy, and for high-risk AI systems listed in points 6, 7 and 8 of Annex III (6. Law enforcement, 7. Migration, asylum, and border control, 8. Administration of justice and democratic processes) the Member States should designate competent data protection supervisory authorities as market surveillance authorities. Article 43, paragraph 1 prescribes that the national DPAs shall be the notified bodies for conformity assessment when the system is intended to be put into service by law enforcement, immigration or asylum authorities.

AI INDUSTRY

Providers of high-risk AI systems

Providers of high-risk AI systems have a pivotal role given that their obligations (Articles 16-22) are key for the successful application of the AI Act's provisions. They need to demonstrate their compliance through fulfilling several key

24 Regulation (EU) 2016/679 of the European Parliament and of the Council, 27 April 2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj

25 Directive (EU) 2016/680 of the European Parliament and of the Council, 27 April 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680

obligations, such as a quality management system, keeping the necessary documentation on the system, keeping logs automatically generated by their system, corrective actions and duty of information, cooperation with competent authorities, as well as to appoint an EU representative if they are established in a third country.

Deployers of high-risk AI systems

As per Article 26, deployers of high-risk systems have a multitude of obligations. For example, they are required to take appropriate technical and organisational measures to make sure that the systems are used in accordance with the instructions, to assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support, monitor the operation of the high-risk AI system, keep automatically generated system logs, cooperate with competent authorities, etc. Deployers who are employers should also notify workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system. An additional obligation for public institutions and EU bodies is to register the high-risk AI systems in line with Article 49.

Where applicable, deployers need to carry out a data protection impact assessment as per the GDPR and the Law Enforcement Directive, as well as a fundamental rights impact assessment (Article 27 of the AI Act). Deployers using systems for "live" and "post" biometric remote identification have an additional set of obligations. For transparency purposes, deployers need to inform the natural persons that they are subject to the use of the high-risk AI system.

Providers of general-purpose AI (GPAI) models

Based on Articles 53-55, providers of general-purpose AI (GPAI) models have a range of obligations which mostly concern providing necessary technical documentation and information about their models, as well as cooperating with the Commission and national competent authorities when it comes to the enforcement of the AI Act. Providers established in third countries also need to appoint their EU representatives. When it comes to providers of GPAI models which are deemed to have systemic risks, they have additional

responsibilities related to model evaluation, assessment and mitigation of possible systemic risks, tracking and reporting of serious incidents to the AI Office and where appropriate to the national competent authorities, and employing adequate cybersecurity protection measures.

Providers and deployers of certain AI systems

Providers and deployers of AI systems which are intended for interaction with people, i.e. natural persons, have transparency obligations as per Article 50. The natural persons must be informed that they are in fact interacting with an AI system, unless it is "unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use". The providers of generative AI systems, including those based on general-purpose models, are required to ensure that the outputs of their AI systems are marked in a machine-readable format and detectable as artificially generated or manipulated. In line with this, the deployers of systems that manipulate images, videos, audio or text need to mark such content as artificially generated or manipulated. Finally, deployers of emotion recognition or biometric categorisation systems should inform the persons exposed to such systems and process their personal data in accordance with the GDPR and the Law Enforcement Directive. It is also required that the necessary information is presented to citizens in a clear and distinguishable manner, at the latest at the time of the first interaction or exposure.

Importers of high-risk AI systems

The obligations of importers of high-risk AI systems are outlined in Article 23 and they mostly concern making sure that the system is in conformity with the standards outlined in the AI Act before they place it on the EU market. They are also required to supply relevant competent authorities with all the necessary information and documentation regarding the AI system placed on the market and cooperate with them on any action they take in connection with the system in question.

Distributors of high-risk AI systems

According to Article 24, the distributors of high-risk AI systems are required to make sure that the system is in conformity with the AI Act requirements and that the provider and importer of the system have complied with their respective obligations. When the distributor considers or has a reason to consider that the AI system they placed on the EU market is not in conformity with the requirements, it should take corrective actions necessary to bring that system into conformity, withdraw or recall it, or ensure that the provider, importer, or any relevant operator takes those corrective actions. Distributors are also required to supply relevant competent authorities with all the necessary information and documentation regarding the AI system placed on the market and to cooperate with them.

INDIVIDUALS

In this context the term “individuals” relates to people affected by the deployment of AI systems and the general public, their role mostly concerning aiding the transparency of the use of AI. For example, the persons affected by a high-risk AI system can ask for an explanation of individual decision making (Article 86) by such a system if it has an legal impact on them or otherwise adversely affects them, as well as lodge a complaint with market surveillance authorities in accordance with Article 85 if they suspect that an infringement of the provisions of the AI Act has occurred.

AIA INSTITUTIONAL FRAMEWORK