

Szanowny Pan
Dariusz Standerski
Sekretarz Stanu,
Ministerstwo Cyfryzacji

Szanowny Panie Ministrze,

W odpowiedzi na zaproszenie do składania propozycji uproszczeń przepisów Unii Europejskiej, w imieniu krajowego sektora cyfrowego reprezentowanego przez Związek Cyfrowa Polska, pragnę przekazać zbiór rekomendacji dla Komisji Europejskiej.

Z dużym entuzjazmem przyjmujemy starania polskiej prezydencji w Radzie Unii Europejskiej na rzecz redukcji barier prawnych dla działalności przedsiębiorstw, uproszczenia procedur i harmonizacji prawa na jednolitym rynku cyfrowym. Jesteśmy przekonani, że starania te doskonale wpisują się w dzisiejsze potrzeby Polski i Unii Europejskiej i stanowią podstawę dla umacniania naszej konkurencyjności i innowacyjności. Usuwanie przeszkód i biurokracji jest niezbędnym wymogiem poprawy inwestycji w Europie.

W istocie, w agendzie na rzecz lepszego stanowienia prawa Komisja Europejska zobowiązuje się do zapewnienia, że tworzenie polityki opiera się na dowodach, do uproszczenia i ulepszenia przepisów UE, unikając jednocześnie niepotrzebnych obciążeń. Inicjatywa polskiej prezydencji może pozwolić osiągnąć te cele.

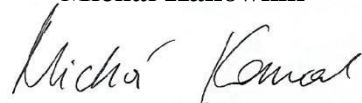
Jako, że część unijnych przepisów — zarówno obowiązujących, jak i dopiero planowanych — nie spełnia powyższych założeń, ograniczając przejrzystość prawa, pragnę przekazać pakiet sugestii i rekomendacji, które dotyczą przede wszystkim następujących regulacji, a szczególnie obszarów, w których ich przepisy zachodzą na siebie lub są ze sobą sprzeczne:

- AI Act
- GDPR
- DSA
- Data Act
- ePrivacy Directive

Szczegółowe rekomendacje dla Komisji Europejskiej w języku angielskim zebrane zostały w załączonej tabeli. Pozostaję do Pana pełnej dyspozycji w razie pytań i ponownie wyrażam uznanie wobec inicjatywy polskiej prezydencji w Radzie Unii Europejskiej.

Z wyrazami szacunku,

Michał Kanownik



**Prezes Zarządu
Związek Cyfrowa Polska**

No	Name of act and number of specific article	Description of the diagnosed problem	Simplification proposal
1	EU AI Act, Chapter V on General-Purpose AI Models (Articles 51-56 and accompanying recitals)	<p>During the final stages of negotiations, obligations for General Purpose AI (GPAI) models were introduced into the AI Act, primarily due to unforeseen advancements in AI technology. This addition sparked significant controversy. The original intent of the AI Act was to regulate high-risk AI applications rather than the technology itself, which has led to conflicts with existing regulations such as the GDPR. Furthermore, the inclusion of the copyright provisions has complicated the legislation, creating a mismatch with the inherently territorial nature of copyright rules.</p> <p>GPAI models are foundational to the AI ecosystem, and excessive regulation could stifle innovation and reduce the EU's competitiveness. Also, the shortcomings of the AI Act's GPAI regime highlight the challenge of regulating rapidly evolving technology. This is for instance evident in the Act's provisions on systemic risk indicators, like FLOPS, which became outdated before implementation. The process around the Code of Practice further illustrates these issues. Even in its third draft of a four-part series, the draft Code includes provisions that suggest regulatory overreach, are technically impractical, lack a basis in current research, and do not align with global standards.</p> <p>To address these issues, the AI Act should return to its</p>	Remove Chapter V from the AI Act

		<p>original focus on regulating high-risk applications and remove redundant technology regulations. It is important to note that existing EU laws already govern the development and use of AI models, making additional regulation unnecessary.</p>	
2	<p>EU AI Act, Chapter VII (eg Article 70)</p>	<p>The current AI Act lacks explicit provisions to ensure that competent authorities balance fundamental rights with regulatory goals such as competition, innovation, privacy, and security. Without clear guidance, there is a risk that regulators might focus too narrowly on one aspect, neglecting other important considerations. To address this gap, the Act should explicitly mandate regulators to foster and protect innovation. This would create a regulatory environment that not only safeguards fundamental rights but also ensures that innovation enhances these rights rather than undermining them. By doing so, the Act can fully achieve its objectives, leading to improved living standards, healthcare, education, and sustainability,</p>	<p>The Omnibus review should give regulators a clear mandate to support innovation, fostering technological advancements while protecting individual rights. This balanced approach will enhance the AI Act's effectiveness and contribute to a dynamic economy.</p>

		and supporting a more prosperous society. Innovation is crucial for exercising fundamental rights like health, education, and freedom of expression, and is protected by the EU Charter. It drives economic growth and social progress.	
3	EU AI Act, Chapter VII	<p>The AI Act currently lacks a clear mechanism for managing cross-border cases, which is essential for establishing a unified regulatory framework across the EU. This absence creates barriers to market entry and contributes to a fragmented digital market. The Act's complex oversight structure leads to jurisdictional challenges, with multiple regulators having overlapping enforcement powers, complicating compliance and notification processes.</p> <p>Unlike previous EU strategies that provide regulatory clarity through centralized authority or the country of origin principle, the AI Act does not offer such guiding frameworks. This omission increases complexity for organizations operating in the EU, as they may need to notify over 100 different bodies for incidents, underscoring the need for a more streamlined approach.</p>	<p>The governance framework in the AI Act should include a streamlined mechanism to handle cross-border cases. This would ensure that organizations communicate with and are enforced by a single main regulator, simplifying compliance and enforcement processes. Without such a mechanism, organizations face the risk of dealing with multiple regulators on the same matter, receiving contradictory guidance, and navigating a fragmented regulatory landscape. Some may even choose to avoid these challenges by focusing on non-EU markets, which undermines the goal of a harmonized approach and stifles innovation within the EU. By implementing a cohesive and efficient regulatory framework, the EU can better support organizations, attract investment, and foster a dynamic and integrated digital economy.</p>

4	GDPR (Article 1)	<p>Issue: Lack of Balance with Economic Interests, Innovation, and other Rights 1) Companies may face restrictions on business operations and innovation due to an overemphasis on data protection; 2) Legal uncertainty and potential conflicts with other rights and related interests, such as freedom of expression and to conduct a business.</p>	<p>Improvements / Simplifications: Clarify the need to balance data protection with other policy objectives, interests and fundamental rights by introducing in Article 1, innovation and economic interests as the GDPR's objectives next to "the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data"</p> <p>Implementation in National law: Ensure national GDPR implementation is consistent or otherwise adjusted to this GDPR modification.</p> <p>Consolidation with further requirements: Align with other EU legislation to support innovation and competitiveness.</p>
5	GDPR (Recital 4)	<p>Issue: Misinterpretation of data protection as an absolute right, neglecting the balance with other; 1) Companies may face restrictions on business operations and innovation due to an overemphasis on data protection; 2) Legal uncertainty and potential conflicts with other rights, such as freedom of expression and business.</p>	<p>Improvements / Simplifications by EU: Include the contents of Recital 4 on balancing rights in Art 1 to ensure full legal certainty about this key duty of regulators and regulatees.</p> <p>Implementation in National law: Ensure national GDPR implementation is adjusted to this GDPR modification.</p> <p>Consolidation with further requirements: Align with other EU legislation to support innovation and competitiveness.</p>

6	GDPR (Article 24)	<p>Issue: Lack of proportionality due to inconsistent and insufficient application of the risk-based approach, leading to a zero-risk mentality. 1) Companies face challenges in implementing proportionate compliance measures due to a lack of clear guidance on the risk-based approach; 2) Overly cautious interpretations can hinder innovation and competitiveness.</p>	<p>Improvements / Simplifications by EU: Reinforce the risk-based approach as a fundamental principle throughout the GDPR by adding the risk-based approach to the list of general principles in Article 5 GDPR (avoid zero risk interpretations and absolutism), explicitly in article 5(1) or 5(2) GDPR (in this latter case, consistently with article 24 GDPR). Implementation in National Law: Ensure national GDPR implementation is adjusted to this GDPR modification. Consolidation with Further Requirements: Align with other EU legislation to promote innovation and competitiveness</p>
7	GDPR (Article 51 par 1)	<p>Issue: Lack of Balance with Economic Interests, Innovation, and other Rights, and Lack of Proportionality (Risk-based approach) by DPAs. 1) DPAs fail to properly balance fundamental rights and other interests in the interpretation, application and enforcement of the GDPR resulting in a zero-risk approach and an absolute prevalence of data protection over any other competing equity, including other fundamental rights and freedoms, in particular, when economic considerations are at stake; 2) As a result, controllers are exposed to privacy absolutist approaches by DPAs, disproportionate compliance obligations, an excessive burden and legal uncertainty, hindering not only their ability to comply but also to innovate and be competitive.</p>	<p>Improvements / Simplifications by EU: Introduce in Art 51 (1), innovation and economic interests and the balancing of rights and interests to the responsibilities for DPAs in addition to being “responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union” Implementation in National Law: Ensure national DPA statutory regime is adjusted to the GDPR modification. Consolidation with further requirements: Align with other EU legislation to support innovation and competitiveness.</p>

8	AI Liability Directive (entirety)	The Product Liability Directive (PLD) and the AI Act already sufficiently address AI-liability and safety concerns. The AI Liability Directive would have added complexity to a crowded regulatory space. The AI Act introduces obligations for AI providers and users to increase the safety and trustworthiness of AI applications. There is no clear evidence of harm requiring additional regulation. The AI Act and the PLD should be implemented and assessed before creating new legislation.	We fully support the Commission's decision to withdraw the AI Liability Directive.
9	PSD3 (Article 87 (3))	The current regulatory framework provides Payment Service Providers with the choice and flexibility to determine how best to meet their regulatory obligations. As well as acknowledges the diverse ways in which Technical Service Providers contribute to the payments ecosystem. This diversified approach should be maintained. This is at risk most notably due to article 87 (3), which in its current proposed draft form would oversimplify the diverse ecosystem of Technical Service Providers (TSPs) and would change the liability regime considerably.	Aim to ensure diversified approach
10	FIDA	The DMA already sufficiently governs and restricts gatekeepers' use of data across services, including to counter potential network effects and data-driven advantages.	Overlaps with DMA should be avoided.
11	Data Act	The Data Act's restrictions on data sharing with DMA gatekeepers conflict with the GDPR's data portability rights. While GDPR Art. 20 lets users transfer their data between different tech services, the Data Act prohibits this to prevent unfair competitive advantages. For	Address overlaps and countereffective provisions between Data Act and GDPR

		example, the Data Act could restrict a user transferring their workout data from a small fitness app to a dominant tech platform's fitness service, preventing the gatekeeper from gaining a competitive edge. This runs counter to the data portability right as enshrined in GDPR art. 20.	
12	Data Act	To be able to fully benefit from the promise of public cloud, governments and businesses need to have flexibility and choice, interoperability of services and should be able to switch between cloud providers. The Data Act contemplates the establishment of European wide interoperability standards for data usage & transfers. The EC is identifying useful standards, and if it sees a gap with current standards, new standards will be encouraged. We are actively monitoring the EU switching cloud technology standards development and supporting the EC in their current study on standards and common specifications.	For coherence and simplification, relying on already existing and internationally recognised standards is recommended.
13	DSA (Article 21)	Article 21 of DSA does not clarify what type of information sharing is entailed in the good faith engagement obligation with the out-of-court dispute settlement body. Acknowledging that Article 21 DSA will inevitably involve sharing of personal data subject to GDPR requirements (including in some cases special category data and criminal data) relating to the user/complainant, the lack of certainty has made it challenging to operationalise in some respects, particularly against the backdrop of GDPR requirements and the question of the breadth and volume of data which should be shared with ODS bodies.	Overlaps with GDPR should be avoided.

14	DSA (Article 40)	Similar concerns regarding GDPR overlaps exist regarding researcher data access under Article 40 DSA (e.g. how to access the data; whether to anonymise/pseudonymise the data; etc).	Overlaps with GDPR should be avoided.
15	DSA	In the frame of the EU content legislation, there are 8 different overlapping reporting obligations: 2 DSA report for VLOPs per year, 1 annual DSA report for non VLOPs, 2 DSA reports on Information about monthly active recipients per year, 2 EU Code of Practice of Disinformation per year and 1 annual Terrorist content online. These reports should be combined or at the very least have consistent taxonomy, timeframe and metrics. In some cases, there are inconsistent overlaps (e.g: in referral requests to authorities under Article 18 of the DSA, and Article 14(5) of the TCO). Also the EU Cyber Resilience Act will soon require that we submit a report on cyber attacks which we already report under the DSA.	Simplify EU reporting requirements (compliance and reporting procedure) by harmonising obligations in disinformation, cybersecurity, sustainability and data processing. Reporting and sustainability requirements for data centres under the Energy Efficiency Directive, Taxonomy, Corporate Sustainability Reporting Directive and the AI Act should also be harmonized to avoid duplicative obligations.
16	ePrivacy Directive (Article 5(3))	<p>The cookie provision particularly has generated generalised frustration (cookie fatigue) with organisations and internet users alike, without offering significant protection. Because of the consent-cookie provision, people become de-sensitised to meaningful consent requests and investment on privacy enhanced technologies is discouraged. Innovation through connected devices/cars/appliances will be increasingly hindered.</p> <p>ePD is implemented in a very different manner among Member States (in some, more strictly), for instance</p>	Remove Art 5(3) ePD. Ensure national ePD implementation is adjusted to the ePD modifications

		<p>regarding direct marketing and is enforced by DPAs and non-DPAs.</p> <p>Application by Administration: Some regulators adopt stricter interpretations than needed. DPAs have created guidelines, disregarding the opinion of the remaining ePD enforcers, in a manner that makes basic Internet operations and privacy enhanced technologies impossible.</p> <p>Cumulative Effect: ePD is outdated as the last update occurred in 2009. The ePD generates overlap and conflicts with the GDPR and the Data Act (substantive provisions and enforcement regimes).</p>	
17	ePrivacy Directive (Article 6)	<p>Traffic Data - Connected devices are key to innovation in the EU, and modern vehicles are essentially computers on wheels, constantly collecting and transmitting data via embedded SIM cards (e.g., for navigation, diagnostics, infotainment, emergency calls, etc.). This communication is often routed over mobile networks, meaning it generates traffic data as defined by ePD.</p> <p>Some regulators adopt stricter interpretations than needed, for instance, regarding what constitutes traffic data. The ePD is outdated as the last update occurred in 2009. The ePD generates overlap with the GDPR and the Data Act (substantive provisions and enforcement regimes)</p>	<p>Remove reference to “and related traffic data”.</p> <p>Remove traffic Art 6 on traffic data.</p> <p>Ensure national ePD implementation is adjusted to the ePD modifications.</p> <p>Align the interpretation of data minimization and purpose limitation to ensure consistency across GDPR provisions and related EU legislation.</p>

18	ePrivacy Directive (Article 13)	<p>The ePD's direct marketing provisions were originally intended to protect against unsolicited 1:1 communications from advertisers to their actual and potential clients through the use of the latter's email or sms for marketing campaigns. The ePD's rules on direct marketing differ per how Member States have implemented them and its regime is redundant and inconsistent with GDPR (direct marketing in GDPR falls under the legitimate interest legal basis as per Recital 47; but is subject to consent under ePD), which creates legal uncertainty and hinders the economic viability of many online services.</p> <p>ePD direct marketing rules are implemented differently depending on the Member State. Some regulators adopt stricter interpretations beyond the letter and the spirit of ePD.</p>	<p>Remove Art 13(3) on unsolicited communications. GDPR would continue to apply to direct marketing, as long as it involves the use of personal data).</p> <p>Ensure national ePD implementation is adjusted to the ePD modifications.</p>
Policies planned in the new Mandate			
19	Digital Networks Act (DNA)	<p>A solid legislative framework already exists in this field, with the revision of the European Electronic Communications Code (EECC) due in 2025, and the Gigabit Infrastructure Act (GIA) that has just been adopted and requires national implementation to deliver results.</p>	<p>Any pending issues can be addressed in this framework, if we remain consistent with the Draghi report on reducing regulation to support growth.</p>

		<p>In the context of a DNA, the circulated proposal to create a 'dispute resolution mechanism' between telecom providers and content application providers (CAPs) appears burdensome, redundant and would undermine net neutrality. It is also opposed by a large number of European stakeholders: this feedback was overwhelmingly clear in two subsequent EU consultations and the fresh Council Conclusions on the White Paper. BEREC in particular emphasizes that IP interconnection is a well-functioning market where peering agreements are made free of charge and because they are mutually beneficial.</p> <p>Similarly, there is no regulatory gap for cloud service providers (CSPs) that would need to be addressed via a DNA and extension of the Code. There is no convergence between the two industries and therefore no uneven playing field or market failure. CSPs and telecoms work in partnerships and provide adjacent, if sometimes overlapping services - far from convergence however. Cloud is an important provider to the sector to drive digital innovation.</p>	
20	Digital Fairness Act (DFA)	<p>Fragmented regulations, particularly in areas like data protection as highlighted in the Draghi report, create barriers to innovation and growth, contrary to the EC's goal of encouraging investments by removing obstacles and red tape. European citizens can already count on the strongest consumer and data protection standards in the world.</p>	<p>Policymakers should carefully assess the necessity of any new laws which could stifle innovation and harm business large and small, and instead focus of the enforcement of the wide array of regulations which already govern areas mentioned as priorities for the Digital Fairness Act - including:</p> <ul style="list-style-type: none"> ▪ GDPR: rules on processing of personal data;

			<ul style="list-style-type: none"> ▪ DSA: restrictions on targeting of known minors and targeting based on sensitive data. ▪ DMA: new rules on cross-product data sharing; ▪ Consumer Rights Directive: rules on disclosure of personalized prices
21	AI Act Codes of Conduct	<p>AI promises to boost Europe’s productivity, and as a foundational technology promises to elevate not only new but also established industries, helping manufacturing, scientific discovery, public services and many more. However, uptake and effectiveness of this technology depends on whether companies and users have a clear and reliable regulatory framework to invest in AI and train their workforce. The AI Act has the objective to enable the uptake of AI in a safe and responsible manner, while at the same time not stifling a nascent and rapidly evolving technology</p>	<p>To square the circle, the AI Act Code of Practice for Providers of General Purpose AI Models is meant to ensure effective compliance, enabling better protection of users, while reducing bureaucracy and compliance burden. To this end:</p> <ul style="list-style-type: none"> i. The Code should operate within the legal framework provided by the AI Act and copyright law, while also considering the AI Act’s objectives, the EU’s competitiveness goals, and the need to minimize compliance costs and bureaucratic burdens. ii. The EU needs to collaborate with AI model providers to ensure the draft code of Practice is practical and enforceable by the August deadline. iii. Political oversight and control over the drafting process of the Code is necessary to avoid excessive bureaucracy and drive work towards more practical and innovation friendly solutions.

22	Potential DSA Codes overlapping with recent legislations	<p>Additional Codes are explicitly encouraged under the DSA that correspond or overlap with recently adopted legislation - for example:</p> <ul style="list-style-type: none"> i. a potential Code of Conduct for Accessibility would be duplicating the recently adopted EU Accessibility Act (Article 47 DSA) contradicting the approach of better regulation and simplification. ii. A potential Code of Conduct for Online Advertising (Article 46 DSA). 	Avoid more overlaps
23	Audiovisual Media Service Directive (AVMS) assessment	AVMS has very recently been fully implemented in some key Member States. It is important to assess its effectiveness before taking any steps in the direction of a review.	Provisions around child safety, influencers and protection from harm are already extensive and arguably sufficient in other pieces of legislation, such as the Digital Services Act (DSA).
24	European Union Copyright Directive (EUCD) assessment	<p>EUCD was adopted in 2019 but implementation across Member States was only completed in 2024.</p> <p>The application of the Text and Data Mining (TDM) to AI and GAI use cases - as set out in Article 4 of EUCD - has been clarified by the newly adopted AI Act. This balanced framework protects the rights of rightsholders (via rights reservation) while paving the way for AI innovation. This is key to Europe's success with respect to AI and it is critical this underlying framework is maintained.</p> <p>Issues related to AI and copyright are being actively discussed in the AIA Code of Practice with respect to both rights reservations and transparency. Work in this regard should be concluded before any consideration is given to reopening this file.</p>	For legal and market certainty it is important that time is given to allow national laws to bed in before reopening & amending provisions.