Teka Komisji Prawniczej PAN Oddział w Lublinie, vol. XVII, 2024, no. 2, pp. 625-635
https://doi.org/10.32084/tkp.9076

AI ACT AND PUBLIC PROCUREMENT LAW – AN OPPORTUNITY OR THREAT

Dr. Beata Zięba

Nicolaus Copernicus Superior School, Poland
e-mail: becia.zieba@gmail.com; https://orcid.org/0009-0007-7434-3910

Abstract. The risks named in the regulation and other European documents diverge significantly from those generally identified in management standards as "conventional" IT risk. In the context of operational risks associated with the activities of a given entity and the varying perceptions of those risks by participants in the broadly understood market, a pressing need has arisen to develop a comprehensive legal framework that would not only chart the course for future development but would also name most critical pain points and ensure minimum protection. The AI Act responds to the rapid and dynamic development of artificial intelligence which has penetrated many aspects of everyday life, from healthcare to transport and safety. These regulations aim to safeguard society from the potential risks arising from the unchecked development and implementation of AI while fostering innovation and providing a framework for the safe, ethical, and responsible use of this technology. The public procurement market is leveraging AI tools, both contracting authorities and contractors. In sectors involving the expending of taxpayers' money, including in public procurement, AI promises immense capabilities, particularly in areas where data is available, and processes and tasks can be automated.

Keywords: public procurement; artificial intelligence; IT risk; AI act; public procurement act.

INTRODUCTION

As early as in 2019, the European Banking Authority's Guidelines on ICT and Security Risk Management[1] highlighted the necessity of addressing a broad spectrum of risks associated with technology and ICT security [Nowakowski 2023, 67]. The risks named in the regulation and other European documents diverge significantly from those generally identified in management standards as "conventional" IT risk. There is no one-size-fits-all model, and each organization should independently assess how to carry

[1] EBA Guidelines on ICT and security risk management, EBA/GL/2019/04, EBA, of 29 November 2019, https://www.eba.europa/eu/sites/default/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf [accessed: 10.05.2024].

ISSN 1899-7694
e-ISSN 2719-7379

out this mapping. For institutions that conduct regular reviews of available solutions, this task appears to be more straightforward than for those which will embark on it for the first time [ibid.].

In the context of operational risks associated with the activities of a given entity and the varying perceptions of those risks by participants in the broadly understood market, a pressing need has arisen to develop a comprehensive legal framework that would not only chart the course for future development but would also name most critical pain points and ensure minimum protection.

1. "AI ACT"

On 8 December, 2023, the European Union made a landmark achievement in the regulation of artificial intelligence by unveiling the world's first thoroughly comprehensive legal document, officially referred to as the AI Act.[2] The European Parliament endorsed the new law on 13 March 2024.[3] The AI Act responds to the rapid and dynamic development of artificial intelligence which has penetrated many aspects of everyday life, from healthcare to transport and safety. These regulations aim to safeguard society from the potential risks arising from the unchecked development and implementation of AI while fostering innovation and providing a framework for the safe, ethical, and responsible use of this technology. The AI Act, therefore, represents a global paradigm shift in how AI is perceived and positioned within society. By introducing detailed guidelines for AI applications, anticipated by all stakeholders, the EU seeks to strike a balance between technological progress and the protection of civil rights, which if paramount in an era where technology intertwines with nearly every sphere of our lives.

As one of the first regulations of its kind, the AI Act, is poised to set the bar for other countries around the globe. Non-EU countries might follow by adopting similar rules, which could shape the global landscape for AI development and use. Companies based outside the EU and willing to gain a foothold in the European market will need to align their AI products with the AI Act's requirements. This could affect the competitive landscape as businesses will be forced to invest more resources in ensuring their AI solutions are secure and compliant. The AI Act could also open the door to greater international collaboration on AI regulation. Countries might join forces in aligning their laws, which would help smooth the way for international trade and bolster cooperation in the AI domain. For international

[2] Press release: https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law [accessed: 29.08.2024].

[3] AI Act: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf [accessed: 29.08.2024].

startups and small to medium-sized enterprises, adapting to the requirements of the AI Act may pose a challenge due to limited resources. However, compliance with the high standards set by the EU could also pave the way to a broader European market. Along with the AI Act, the demand for compliance experts is set to grow, both within the EU and on a global scale.

The introduction of the AI Act by the EU marks a watershed moment in the regulation of artificial intelligence. This groundbreaking legislation aims to set the stage for the future of AI, ensuring that its development and use will be secure, ethical but will also uphold fundamental human rights. In practical terms, for AI professionals and specialists, a thorough understanding of the AI Act is absolutely essential. This goes beyond mere legal compliance: it is also a critical element in building trust and reputation in the digital era.[4]

The document referred to above is one of the cornerstones of the EU's policy as regards the fostering and utilizing secure and lawful artificial intelligence across the entire single market without compromising fundamental rights [Bujalski 2023]. The AI Act follows a risk-based approach and establishes uniform and horizontal legal frameworks for AI to ensure legal certainty. It is designed to spur investment and innovation in the AI domain, enhance governance and the effective enforcement of existing regulations on security and fundamental rights, and facilitate the growth of a unified market for AI applications.[5]

2. DEFINITION OF THE CONCEPT OF "ARTIFICIAL INTELLIGENCE"

Many approaches to the concept of AI have emerged over the last few years, hence the need for a universal definition of the phenomenon. One developed by the OECD (Organisation for Economic Cooperation and Development) and considering artificial intelligence in terms of a system model is seen as an attempt to reach international consensus on how to frame AI. In accordance with the definition proposed by the OECD and contained in the Recommendation of the Council on Artificial Intelligence,[6] AI is

---

[4] See *Sztuczna inteligencja regulacje – Unia Europejska i pierwsze regulacje AI*, https://leadakademia.pl/sztuczna-inteligencja-regulacje-unia-europejska-i-pierwsze-regulacje-ai/?gad_source=1&gclid=Cj0KCQjw6PGxBhCVARIsAIumnWaHD109ex5UexsRTZZdrxafjD-EsMpIWaBV9NFTDrTQwZxLqXGjWhAaArbJEALw_wcB [accessed: 09.05.2024].

[5] More on the diagnosis on AI systems and risks that exist in the area of management of a public institution in, see: Drogkaris and Adamczyk 2022, 10ff; Bourka and Drogkaris 2021, 14ff; *Realizing the Potential of AI in Financial Services. Overcome challenges and deliver on the full promise of AI with the NVIDIA AI Enterprise software suite*, https://www.vmware.com/docs/vmw-nvidia-ai-enterprise-ebook [accessed: 29.08.2024]; EBA Analysis of the RegTch in the Financial Sector. EBA/REP/2021/17 (EBA, June 2021), 31, after: Nowakowski 2023, 66.

[6] OECD, Recommendation of the Council on Artificial Intelligence (adopted by the Council at Ministerial Level on 22 May 2019), http://legalinstruments.oecd.org/en/instruments/

a machine-based system that, in response to certain human-input objectives, infers how to generate predictions, content, recommendations, or decisions that can influence physical or virtual environments. Therefore, in simple terms, artificial intelligence operates in a manner that mimics aspects of human thinking processes. It also harnesses the ability of machines to perform tasks that have traditionally required human reasoning and information processing capacity. Owing to machine learning algorithms, AI possesses the capability to analyse vast datasets, learn from them, and make decisions on its own.

In its negotiating position, the European Parliament adopted the definition of artificial intelligence as a system, as agreed upon by the OECD. It reads that an AI system means "a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments." Moreover, the MEPs proposed that the Council's definition of "general purpose AI system" should be reworded as "an AI system that can be used in and adapted to a wide range of applications for which it was not intentionally and specifically designed." Finally, the European Parliament introduced a definition of the "foundation model" as "an AI system model that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks." The position of the European Parliament was adopted in the AI Act as final.[7]

3. REGULATIONS OF AI ACT

The new AI Act provisions ban certain uses of artificial intelligence that could jeopardize citizens' rights. General-purpose AI systems and the AI models behind them must adhere to specific transparency standards and comply with EU copyright law, including providing accurate summaries of the input materials used for training their models. The most advanced general-purpose AI models that pose systemic risks will face additional requirements. Furthermore, inauthentic or manipulated images, audio, and video content must be clearly labelled as such.

---

oecd-legal-0449 [accessed: 14.05.2024].

[7] Recital 12 of the CORRIGENDUM to the position of the European Parliament adopted at first reading on 13 March 2024 with a view to the adoption of Regulation (EU) 2024/ ..... of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) P9_TA(2024)0138 (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) of 17 April 2024, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf [accessed: 11.05.2024].

Apparently, most of the responsibility lies with the providers (developers) of high-risk AI systems. General-purpose AI (GPAI): all providers of GPAI models must share technical documentation, user manuals, as well as complying with the relevant EU's copyright directives and publishing a summary of the content used for training such models. Providers of GPAI models that are released under a free and open-source licence need to adhere to copyright laws and publish a summary of the training data, unless they pose a systemic risk. All providers of GPAI models that present systemic risks, both open and closed, must also conduct model assessments, conduct adversarial testing, track and report serious incidents, and ensure that cybersecurity measures are in place.

Under the provisions of the AI Act (Article 61), providers are required to establish an appropriate monitoring system for high-risk AI systems launched on the market. Such a system should actively and systematically collect, document, and analyse relevant data submitted by users or collected from other sources and concerning the performance of high-risk AI systems throughout their life cycle [Nowakowski and Waliszewski 2022, 2].

Some AI systems are classified as "high-risk" under the EU AI regulations, thus placing additional obligations on their providers (Article 6 AI Act). These systems pose potential threats to health, safety, fundamental rights, environment, democracy, and rule of law. High-risk AI systems must follow stringent requirements regarding transparency, security, and human oversight. Detailed documentation on decision-making processes and algorithms is essential and needs to be collected. Such high-risk systems support various sectors, among them: Healthcare, Transport, and Automotive (the AI Act places specific requirements on autonomous vehicles, focusing on safety, reliability, and human intervention in critical situations. The act mandates risk assessments and safety testing), Finance and Banking (AI systems employed for credit risk assessment or algorithmic trading are considered high-risk, thus necessitating detailed assessments of their impact on fundamental rights and transparency in decision-making processes), Law (the use of facial recognition systems by law enforcement agencies is tightly regulated and must adhere to requirements for data protection and restrictions on mass surveillance. Judicial authorization is required for their use in specific situations, such as locating missing persons or preventing terrorist attacks. Before deploying such systems, the police force must conduct impact assessments on fundamental rights and register the system in the EU database; however, in justified and urgent cases, deployment may begin without registration, provided that it is registered later without undue delay), Education (AI used for tailored teaching processes and assessments must be transparent and unbiased. The act requires the developers of these systems to conduct regular ethical assessments and evaluations of their impact

on students' rights), Recruitment and Human Resource Management (AI used in recruitment and talent management must not discriminate against anyone. The act requires companies to assess the impact of these systems on fundamental rights and ensure transparency in their operations), Advertising and Marketing (AI systems used for personalized advertisement must comply with data protection and privacy regulations. The act requires companies to inform users explicitly about the use of algorithms for marketing purposes). Some law enforcement systems also rely on high-risk AI to manage migration and border security. It is employed in the justice system and democratic processes (e.g. to influence elections). These systems must be capable of assessing and mitigating risks and maintain event logs. They must also be transparent and accurate and subject to human oversight. Thanks to the AI ACT, citizens will have the right to file complaints regarding the operation of AI systems. They will also receive explanations for decisions made by high-risk AI systems that have an impact on their rights.

Artificial intelligence systems are deemed high-risk whenever they allow for the profiling of individuals, that is, for the automated processing of personal data to assess different facets of a person's life, including work performance, financial status, health condition, preferences, interests, reliability, behaviour, location, or movement. Providers who find that their AI system, which does not comply with the AI Act, does not pose a high risk must thoroughly document such an assessment prior to putting its deployment or putting it on the market (Articles 8-25 AI Act).

4. THE EUROPEAN OFFICE FOR ARTIFICIAL INTELLIGENCE

The European Commission has established a new EU-level regulator, the European Office for Artificial Intelligence. It will be structurally set within the European Commission's Directorate-General for Communication Networks, Content and Technology (DG CNECT). The AI Office will monitor, supervise, and enforce the AI Act requirements concerning general purpose AI (GPAI) models and systems across the 27 EU member states. The process will cover the analysis of emerging unforeseen systemic risks stemming from GPAI development and deployment, as well as developing capabilities evaluations, conducting model evaluations and investigating incidents of potential infringement and non-compliance. The AI Office will draw up codes of practice, adherence to which would create a presumption of conformity. They will also lead the EU in international cooperation on AI and strengthen bonds between the European Commission and the scientific community, including for the forthcoming scientific panel of independent experts. The Office will help the 27 member states cooperate on law enforcement, including on joint investigations, and will act as the Secretariat

of the AI Board, the intergovernmental forum for coordination between national regulators. It will support the creation of regulatory sandboxes where companies can test AI systems in a controlled environment. It will also provide information and resources to small and medium businesses (SMEs).[8]

The AI Act also commits EU member states to establishing, at national level, an environment that facilitates the development and pre-market testing of innovative AI systems. Such testing should be carried out in real conditions.

Harmonised rules applicable to the placing on the market, the putting into service and the use of high-risk AI systems, in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council, Decision No 768/2008/EC of the European Parliament and of the Council and Regulation (EU) 2019/1020 of the European Parliament and of the Council should apply across sectors. Under the new legal framework, they should be without prejudice to existing EU law, in particular on data protection, consumer protection, fundamental rights, employment, protection of labour, and product safety, to which the regulation is complementary.[9]

The AI Act will take effect 24 months after entry into force, yet with the exception of the following deadlines:[10] 6 months for provisions on prohibited AI systems (prohibited practices), 12 months for GPAI provisions, including concerning management, 36 months for high risk AI systems and obligations related thereto; codes of practice for providers must be ready 9 months after entry into force.

The public procurement market is leveraging AI tools, both contracting authorities and contractors. Over time, the ratio between human input and AI contribution will evolve. This will certainly expedite and streamline the processes of organizing, conducting, and auditing procurement procedures. However, AI is not envisaged to eliminate the human factor completely, primarily due to the fact that its reliability and output cannot always be trusted. Still, AI can assist people in relatively easy and repetitive tasks. Already today, both contracting authorities and contractors are employing technological solutions in public procurement procedures, such as during

---

[8] See https://artificialintelligenceact.eu/the-ai-office-summary/ [accessed: 12.05.2024].

[9] Recital 9 of the CORRIGENDUM to the position of the European Parliament adopted at first reading on 13 March 2024 with a view to the adoption of Regulation (EU) 2024/ ..... of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) P9_TA(2024)0138 (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) of 17 April 2024, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_PL.pdf [accessed: 11.05.2024].

[10] Source: https://artificialintelligenceact.eu/high-level-summary/ [accessed: 29.08.2024].

electronic auctioning or in managing electronic document workflows. Experts are of the opinion that public procurement may not necessarily be among the first sectors to widely adopt AI capabilities [Jóźwiak 2023].

5. AI ACT AND PUBLIC PROCUREMENT

Opportunities for utilising AI in public procurement procedures at the specific stages of awarding public contracts [Skórzewska 2023]:

1. *Support at the stage of preparing the procurement process*: AI can help better understand the contracting authority's needs and can be useful in preparing the entire procurement process. By analysing historical data and previously awarded contracts, AI can draw valuable conclusions and predict future needs of the contracting authority (especially that some of the needs are recurring). It can also categorise awarded contracts and develop contract award procedure plans.
2. *Need and requirement analysis*: AI systems may support an analytical process aimed to pinpoint the contracting authority's actual needs and align them with available market solutions. Besides, it could help ensure the effective and reasonable spending of public money. When exploited in this domain, AI could help perform risk analyses for different solutions and recommend optimal actionable strategies. Owing to access to relevant data sources, AI could also assist in assessing various cost scenarios, thus identifying the most cost-effective and efficient solutions, as well as selecting eco-friendly options.
3. *Estimation of contract value*: AI can support the contracting authority in data analysis by sifting through databases of previous contracts with a view to identify historical costs and average prices. It will help the contracting authority to gauge the average value of similar contracts awarded in the past. With access to proper data sources, advanced AI algorithms could help analyse current market prices, predict potential risks based on price fluctuations or regulatory changes, which might impact the ultimate contract value, and update contract value estimates.
4. *Auto-generation of documents and solution suggestion mechanisms*: AI tools can streamline the generation of contract documentation and spot gaps or deficiencies concerning compliance. Based on existing document samples and data input by the contracting authority, AI can generate standard procurement documents, such as Terms of Reference, bid forms, requests, or public contract templates. This is likely to enhance the quality of documentation, reduce error prevalence, save time, and expedite the contract award procedure as a whole. Drawing on prior tender experience, AI can also suggest, depending on the type of contract, strategies

and decisions concerning bid assessment criteria, participation terms, selection of procedures, or the use of specific contract clauses. AI can also serve to systematise and categorise specific data types for the preparation of tender proceedings.

5. *Electronic bidding systems*: The use of electronic systems in bidding process offers numerous advantages, including increased operational efficiency owing to faster and better organized bid management. It also enhances transparency, which is essential in counteracting corruption and abuse attempts. However, it is pivotal to ensure top-class cybersecurity and users must be ready to adopt the new technology, although they may be lacking proper resources.
6. *Documentation analysis and error detection*: AI could also be a huge help for contracting authorities in reviewing bids and procurement documents. AI can rapidly validate and compare numerous documents to extract key information and identify any inconsistencies.
7. *Bid analysis and comparison*: AI can assist contracting authorities in analysing and comparing bids. It is able to flag inconsistencies or omissions, such as discrepancies between bid prices, competitor prices, or market prices. This can help identify bids with abnormally low prices or unrealistic cost components. AI would also be able to automatically assign scores to individual bids, summarize results, and even create rankings based on all evaluation criteria.
8. *Contract execution monitoring*: The use of AI in the performance of awarded contracts, that is, in the monitoring of progress, alignment of contract terms with financial settlements, compatibility of documentary material developed during the life of the contract with contractual provisions, etc. will allow faster and more accurate decision-making, which is invaluable for complex and high-value public contracts.
9. *Advanced analysis for procurement strategies* – in the contractor selection process. AI can support more profound bid analysis, assessment of contractor's capacity, and can even predict potential issues. This results in more informed and strategic decision-making.
10. *Information retrieval from databases*: advanced AI-powered systems could also enable quick searches within databases and document repositories, as well as helping contracting authorities in market analysis and monitoring.
11. *Monitoring the overall procurement process*: in the long term, AI could possibly play a key role in the monitoring and reporting on the entire public procurement process. This would create even greater transparency and control over how public funds are spent.

As of now, AI tools are chiefly perceived as supplementary measures. However, considering the rapid advancement of technology, it can be reasonably anticipated that, over time, AI will be gaining in importance, both in public procurement and across the entire public sector. While it is not easy to tell the exact AI adoption timeline, it is commonly held that its automation, data analysis, and prediction capabilities are more than likely to produce significant benefits within the public procurement domain by streamlining procedures. The extent to which AI will be employed in public procurement will depend on a range of factors, among them, technological progress, access to capable infrastructure, the reliability of data stored in databases, financial resources, the costs of implementing sophisticated systems, and the presence of legal solutions that will ensure transparent, secure, and traceable use of AI.[11]

CONCLUSION

In summary, in sectors involving the expending of taxpayers' money, including in public procurement, AI promises immense capabilities, particularly in areas where data is available, and processes and tasks can be automated. Certain limitations will continue to exist, such as the reliability and accuracy of data, as well as rules and regulations which undoubtedly influence how public institutions approach new technologies. The rapidly evolving legal and regulatory setting may serve both as an incentive for tests but may also represent a potential barrier to further development. Any decision to deploy AI must be preceded by a thorough analysis of the institution's capabilities and limitations and should also consider the tangible benefits for the organization and its users. The area of ICT risk management is now becoming crucial for many institutions as well as regulators and legislators, as one "IT architecture incident" can have an adverse impact on other systems. Artificial intelligence is evolving rapidly. Any experimentation and deployment of AI solutions should respect the legal, technical, ethical, and human aspects that are behind a safe and effective artificial intelligence that is expected to produce results for organisations and their clients. Building new quality often requires the organisational structure, policies, procedures and processes, and contractor agreements to be reviewed, let alone meeting legal and regulatory requirements. Therefore, it is crucial to acquire knowledge about new solutions and to build infrastructure that will adopt future implementations of new products and services.[12]

---

[11] Source: file:///U:/14_artyku%C5%82y%202023-2024/AI%20ACT/Raport-Fundacji-Moje-Panstwo-AI-wersja-PL.pdf [accessed: 29.08.2024].

[12] Fr more see: https://www.nask.pl/download/30/4575/AIDApublikacja-analiza-danych.pdf [accessed: 15.09.2023]; https://w w w.knf.gov.pl/dla_rynku/fin_tech/aktualnosci?articleId=73633&p_id=18

REFERENCES

Bourka, Athena, and Prokopios Drogkaris (eds.). 2021. *Technical analysis of cybersecurity measures in data protection and privacy*. ENISA.

Bujalski, Rafał. 2023. "Akt o sztucznej inteligencji [projekt UE]." Lex el.

Drogkaris, Prokopios, and Monika Adamczyk (eds.). 2022. *Data Protection Engineering. From Theory to Practice*. ENISA.

EBA Analysis of the RegTch in the Financial Sector. EBA/REP/2021/17 (EBA, June 2021).

Jóźwiak, Zofia. 2023. "Sztuczna inteligencja zorganizuje przetarg? To wcale nie takie pewne." https://www.prawo.pl/biznes/wykorzystanie-sztucznej-inteligencji-w-zamowieniach-publicznych,522495.html [accessed: 11.05.2024].

Nowakowski, Michał. 2023. "2.8. Inne obowiązki." In *Sztuczna inteligencja. Praktyczny przewodnik dla sektora innowacji finansowych*, 67. Warszawa: Wolters Kluwer Polska.

Nowakowski, Michał, and Krzysztof Waliszewski. 2022. "Ethics of artificial intelligence in the financial sector" *Przegląd Ustawodawstwa Gospodarczego* 1:2-9.

Realizing the Potential of AI in Financial Services. Overcome challenges and deliver on the full promise of AI with the NVIDIA AI Enterprise software suite, https://www.vmware.com/docs/vmw-nvidia-ai-enterprise-ebook [accessed: 29.08.2024].

Skórzewska, Paulina. 2023. "Czy sztuczna inteligencja zrewolucjonizuje zamówienia publiczne." https://dsk-kancelaria.pl/blog/czy-sztuczna-inteligencja-zrewolucjonizuje-zamowienia-publiczne/ [accessed: 10.05.2024].

Sztuczna inteligencja regulacje – Unia Europejska i pierwsze regulacje AI, https://leadakademia.pl/sztuczna-inteligencja-regulacje-unia-europejska-i-pierwsze-regulacje-ai/?gad_source=1&gclid=Cj0KCQjw6PGxBhCVARIsAIumnWaHD109ex5UexsRTZZdrxafjD-EsMpIWaBV9NFTDrTQwZxLqXGjWhAaArbJEALw_wcB [accessed: 09.05.2024].

[accessed: 15.09.2023]; European Declaration on Digital Rights and Principles for the Digital Decade, European Commission, 26.01.2022, COM(2022) 28 final, https://ec.europa.eu/newsroom/dae/redirection/document/94370 [accessed: 23.09.2023]; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU, European Commission, 24.09.2020, COM(2020) 591 final, https://eur-lex.europa.eu/legal-content/EN-PL/TXT/?from=PL&uri=CELEX%3A52020DC0591 [accessed: 15.09.2023]; https://www.gov.pl/attachment/0986958f-830d-409c-8301-32ebae3ff6ef [accessed: 31.07.2023].