Polchanov A., DSc., Prof.,
Professor of Department of Finance,
Zhytomyr Polytechnic State University,

EU DIGITAL MARKET REGULATION: IMPLICATIONS FOR UKRAINIAN BUSINESSES

The economy of the European Union is one of the largest in the world. According to World Bank data, in 2025, the EU's gross domestic product (GDP) amounted to USD 21.24 trillion, exceeding that of China (USD 19.5 trillion) but remaining below that of the United States (USD 30.77 trillion) [7]. The value added generated by the EU information and communication technology (ICT) sector amounted to EUR 816 billion in 2023, accounting for 5.24% of the EU's total value added [1]. Ukraine's physical and economic integration into Europe increases the relevance of studying the legal regulation of digital business, given its scale and prospects for further development.

The aim of this study is to identify the key elements of the EU regulatory framework governing digital business and to determine their implications for Ukrainian enterprises entering the EU digital market.

Based on the analysis of the regulatory framework, the key regulations that Ukrainian businesses need to consider when entering the EU market have been identified (table 1).

Table 1. Key regulations governing digital business in the EU

Name	Descriptions
General Data Protection Regulation	This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. It also protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data [2].
Digital Markets Act	The purpose of this Regulation is to contribute to the proper functioning of the internal market by laying down harmonised rules ensuring for all businesses, contestable and fair markets in the digital sector across the EU where gatekeepers are present, to the benefit of business users and end users. This Regulation applies to core platform services provided or offered by gatekeepers (Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft, Booking) to business users established in the EU or end users established or located in the EU, irrespective of the place of establishment or residence of the gatekeepers and irrespective of the law otherwise applicable to the provision of service [3].
Digital Services Act	The aim of this Regulation is to contribute to the proper functioning of the internal market for intermediary services by setting out harmonised rules for a safe, predictable and trusted online environment that facilitates innovation and effectively protects fundamental rights [4].
Data Act	This Regulation lays down harmonised rules, inter alia, on: - the making available of product data and related service data to the user of the connected product or related service; - the making available of data by data holders to data recipients and to public sector bodies (where there is an exceptional need for those data for the performance of a specific task carried out in the public interest); - facilitating switching between data processing services; - introducing safeguards against unlawful third-party access to non-personal data; - the development of interoperability standards for data to be accessed, transferred and used [5].
Artificial Intelligence Act	The purpose of this Regulation is to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation [6].

Thus, the EU has developed a comprehensive regulatory landscape aimed at fostering fair competition and innovation while ensuring data protection, platform accountability, secure data use, and trustworthy artificial intelligence.

The international development strategy of Ukrainian enterprises in the EU digital market should be based on the proactive implementation of regulatory compliance. This requires a comprehensive set of measures, including preliminary regulatory audits, personal data protection in accordance with European standards, compliance with the regulatory framework governing digital markets, and the assessment of risks and transparency requirements related to artificial intelligence systems. Embedding these requirements into the design and development of digital products can help mitigate regulatory barriers and facilitate their effective scaling across the European Union.

REFERENCES

1. Eurostat. ICT sector – value added, employment and R&D : Statistics Explained. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_sector_-_value_added,_employment_and_R%26D

2. Regulation (EU) 2016/679 (General Data Protection Regulation) : Regulation of the European Union of 27.04.2016 № 2016/679. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

3. Regulation (EU) 2022/1925 (Digital Markets Act) : Regulation of the European Union of 14.09.2022 № 2022/1925. URL: https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng

4. Regulation (EU) 2022/2065 (Digital Services Act) : Regulation of the European Union of 19.10.2022 № 2022/2065. URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

5. Regulation (EU) 2023/2854 (Data Act) : Regulation of the European Union of 13.12.2023 № 2023/2854. URL: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng

6. Regulation (EU) 2024/1689 (Artificial Intelligence Act) : Regulation of the European Union of 13.06.2024 № 2024/1689. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

7. World Bank. GDP (current US$) : World Development Indicators. URL: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=EU-CN-US

Trosteniuk T.M., PhD, Associate Professor
Zhytomyr Polytechnic State University

LEGAL FRAMEWORK FOR ENSURING THE ECONOMIC SECURITY OF THE STATE UNDER CONTEMPORARY CHALLENGES

Against the backdrop of large-scale changes in the global economic environment, the escalation of military threats, instability in international markets, disruptions to supply chains, increasingly intense technological competition, and the proliferation of cyber threats, the importance of national economic security has become increasingly evident. For Ukraine, the consequences of the full-scale war, the need to ensure national economic stability, protect critical infrastructure, maintain investment potential, and establish a legal framework for post-war recovery further exacerbate these challenges.

At the same time, the nature of contemporary threats to economic security is complex and extends far beyond the scope of traditional economic crimes. These threats include dependence on critical resources and technologies, disruptions to supply chains, cyber risks, economic coercion, unlawful influence over strategic enterprises, and the use of economic instruments to pursue geopolitical objectives. Therefore, there is an urgent need to improve the legal and regulatory mechanisms for preventing and responding to such threats.

This issue is particularly important in the context of Ukraine's European integration. The European Union is gradually developing a comprehensive economic security system that combines such elements as the protection of critical supply chains, technological and cybersecurity, the protection of critical infrastructure, and the mitigation of economic dependencies. In this context, aligning Ukrainian