Position paper on implementation of EU legislation in Ukraine within Digital Single Market

1. Introduction

Ukraine is dedicated to becoming a part of the European Union, which remains a key objective in its foreign policy. This is especially important given the ongoing war with Russia. Joining the EU is expected to expand Ukraine's diplomatic and economic prospects, as well as significantly improve the living standards of its citizens by adopting European legal frameworks and best practices. It's essential to recognize that the EU is primarily an economic and political union that aims to promote cooperation and strengthen ties between European nations. To maximize its potential and align with the EU's regulatory framework, Ukraine must fulfill certain membership requirements, including the continuous integration of EU laws and the transformation of its digital sector to reflect the best European models.

Ukraine is on the path to become a member of the European Union, with the objective of integrating into the EU Digital Single Market. To achieve this, Ukraine needs to align its national laws and standards with those of the EU. This includes developing institutional and technical capabilities, ensuring the compatibility of digital systems, and investing in high-speed broadband communication and e-government infrastructure. For businesses, this transition will introduce regulations based on European guidelines, primarily aimed at improving consumer protection, which will include provisions for personal data processing. As a result of this change, there is likely to be more competition with European digital market players.

These adaptations are crucial for Ukraine's goal of forging a unified economic sphere with the EU, especially considering the growing impact of digital technologies on global trade and economic landscapes. Without these changes, the EU's rapid advancement in digital market regulation could result in further regulatory obstacles and discrepancies in the digital domain, which could adversely impact bilateral digital trade and the overall progression of economic integration and cooperation between Ukraine and EU member states. The alignment with EU laws such as the General Data Protection Regulation, Digital Services Act, and AI regulations, is not just about compliance. It represents a strategic alignment with a broader vision for a digital economy that is innovative, competitive, and secure.

The most crucial objective for decision-makers is to ensure a smooth transition towards a regulatory environment similar to the EU's strong digital framework. This will help Ukraine become a digitally advanced and economically prosperous nation seamlessly integrated with the European digital economy. In order to achieve a successful transformation of the digital

sector, it is crucial for all major stakeholders, including political leaders, lawmakers, and government officials, to participate actively in the process. This participation is necessary to tailor the transformation efforts to align with the country's legal framework and the unique characteristics of its administrative culture. Leaders must understand the far-reaching impact of digitalization, which requires a fundamental review and restructuring of governance systems.

2. The process of adaptation of Ukrainian legislation to the European Union

The process of bringing Ukrainian legal standards in line with those of the European Union began with the Partnership and Cooperation Agreement (PCA) in 1998, signed by the European Communities and Ukraine[1]. As a result, Ukraine has committed to consistently adapting its legislation, particularly in the digital domain, to ensure compliance with European law. The process of aligning Ukrainian legislation with EU standards fully started in 1999 when the Ukrainian Cabinet of Ministers introduced the Concept of Adaptation of Ukrainian Laws to EU Legislation. This document established the official framework for the adaptation process. The Strategy of Integration outlined the overarching goals and extent of this alignment, emphasizing the harmonization of national laws with modern European legal systems for the benefit of Ukrainian citizens. The strategy aimed to promote political, business, social, and cultural engagement, stimulate Ukraine's economic growth within the EU context, and progressively elevate the living standards of Ukrainians to match those in the EU. Ukraine's adaptation process focused on fulfilling the PCA, forming sector-specific agreements with the EU, and revising and formulating Ukrainian laws to be in closer accord with EU legislation.

The relationship between Ukraine and the European Union underwent a significant change after the EU's expansion in 2004 when Ukraine became EU priority partner within the European Neighbourhood Policy[2]. As they became direct neighbors, the EU and Ukraine declared their intention to strengthen their political and economic ties. To make this possible, the EU-Ukraine Action Plan was introduced on February 12, 2005. The goal of this plan was to align Ukrainian laws with those of the EU, particularly in the digital sector.

In March 2006, Ukraine held parliamentary elections. Following this, the European Union started discussions with Ukraine to create a new and improved agreement. These negotiations started in March 2007 and by March 2012, a preliminary draft of the Association Agreement was ready. However, the then Ukrainian President's decision not to sign the Association

[1] https://ec.europa.eu/commission/presscorner/detail/en/IP_98_198

[2] https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-06/Ukraine%20Opinion%20and%20Annex.pdf

Agreement/Deep and Comprehensive Free Trade Area (AA/DCFTA) sparked the 2014 Revolution of Dignity[3].

After the Revolution of Dignity, Ukraine's newly established government signed the political segment of the Association Agreement (AA) in March 2014. Later, the economic component of the AA, known as the Deep and Comprehensive Free Trade Area (DCFTA), was ratified following the presidential elections in May 2014. Parts of the agreement have been temporarily in effect since 2014, and in September 2017, the AA/DCFTA was fully implemented. This agreement sets the foundation for political association, economic and legislative integration between Ukraine and the European Union, specifically within the Digital Single Market.

3. Ukraine legislative within the framework of Digital Single Market

Since then, the discussions between Ukraine and the EU have been centered around the digital economy, which is a crucial element for further integration between the two. Therefore, a greater focus has been placed on a crucial aspect - Ukraine's integration into the EU's Digital Single Market (DSM). The DSM is a strategic initiative designed to unify and enhance digital markets across the EU by implementing shared methods and standards in the digital realm. The EU's DSM provides economic benefits in two main ways. Firstly, it aligns regulations and eliminates obstacles among Member States in the digital domain. This simplifies digital trade across borders within the EU. Secondly, it encourages digitalization in EU Member States. This includes promoting the use of digital technologies within the EU and advancing digital public services and e-government[4].

The integration of Ukraine into the DSM brings several key benefits, including improved access to cutting-edge digital technologies and EU innovations, streamlined organization and automation of production and business operations, and enhanced digital capabilities that lead to increased efficiency in Ukraine's economy. Moreover, the adoption of paperless systems will lower operational costs for businesses and public services. This will also lead to decreased costs in cross-border digital trade between Ukraine and the EU as regulatory, informational, and organizational barriers will be reduced, and logistics will be optimized. Furthermore, the integration will have a positive impact on anti-corruption efforts by improving the quality, transparency, and efficiency of digital public services and e-government, such as e-customs and e-transit systems, influenced by the adoption of European best practices.

Yet, in order for Ukraine to become part of the DSM, it is necessary to align its domestic laws and regulations with those of the EU. This requires both institutional and technical proficiency, as well as compatible digital systems. To achieve this, Ukraine needs to develop high-speed

[3] Ibidem

[4] https://www.europarl.europa.eu/RegData/etudes/STUD/2019/631044/IPOL_STU(2019)631044_EN.pdf

broadband communication networks, increase public spending on e-government infrastructure, and undertake other necessary measures. For businesses, complying with European standards is essential for ensuring consumer protection, such as secure handling of personal data. This also means that they have to face more competition from EU companies in the digital marketplace. These changes are crucial for Ukraine to establish a common economic area with the EU.

The Ukraine-UE cooperation within DSM was based on the terms of the Association Agreement and joint commitments made during the Ukraine-EU Summit and other bilateral association meetings. Since then, Ukraine has been actively working with the EU to update the list of EU legislative acts that need to be implemented in Ukraine, as stated in Appendix XVII-3 of the AA between Ukraine and the EU. In August 2018, Ukraine presented a Roadmap for its integration into the EU Digital Single Market to the European Commission, marking the beginning of structured cooperation that unfolded in several stages:

- During the years 2018 to 2019, the European Commission's DG CONNECT analyzed the proposed Roadmap;
- Following this, a thorough on-site evaluation was conducted by experts between 2019 and 2020. This evaluation aimed to examine how the Ukraine-EU Association Agreement was being applied in telecommunications and to craft suggestions for closer legal alignment;
- From 2020 through 2024, the focus shifted to implementing EU technical assistance projects. These projects were designed to support Ukraine's digital transformation and further legally align it[5].

The Ukraine-EU Summit that took place on October 6, 2020, emphasized the importance of the digital sector in promoting economic integration and regulatory alignment between Ukraine and the EU, as per the EU-Ukraine AA. By implementing the terms of this agreement, especially the revised Annex XVII-3, Ukraine intended to comply with the EU's latest standards in electronic communications. Furthermore, Ukraine was gradually aligning its regulations with various aspects of the EU DSM, including electronic identification, electronic payments and e-payment systems, e-commerce, internet-based intellectual property rights protection, cybersecurity, personal data protection, e-government, postal services, and more. These initiatives aided in the gradual integration of Ukraine into the EU's Digital Single Market, which was aimed to promote digital advancements within the country and open new doors of opportunity for individuals and businesses.

On February 11, 2020, Ukraine and the European Union signed a deal worth €25 million, aimed at boosting e-governance and the digital economy in Ukraine in line with the EU legislative

[5] https://ukraine-eu.mfa.gov.ua/en/2633-relations/galuzeve-spivrobitnictvo/yedinij-cifrovij-rinok-yes

standards. This program was designed to enhance the "Diia" system and various e-services. The initiative was focused on improving interoperability, refining register systems, and developing areas such as cybersecurity, broadband, mobile internet, and electronic identification technologies.

The war initiated by Russia in Ukraine in 2022 has had a significant impact on Ukraine's efforts to join the European Digital Single Market. The conflict has caused extensive damage to Ukraine's digital infrastructure, affecting immediate connectivity and compliance with DSM standards. Moreover, the war has redirected resources from digital development to defense and humanitarian needs, which has impacted Ukraine's ability to make necessary investments for DSM integration. Due to the crisis, the Ukrainian government has shifted its focus to crisis management, causing delays in regulatory and legislative efforts needed for DSM integration.

The situation has also raised cybersecurity concerns, complicating the integration process and potentially influencing DSM's cybersecurity strategies. However, there are some positive aspects to consider. The war could accelerate the adoption of digital services and reforms in Ukraine, aligning with some DSM objectives like e-governance and digital literacy. Additionally, the conflict has the potential to strengthen collaboration between Ukraine and the EU. The EU could offer support to Ukraine in rebuilding its digital infrastructure and conforming to DSM standards.

On the other hand the war presents significant obstacles to Ukraine's integration into DSM, but it also provides opportunities for rapid digital transformation and increased EU collaboration. On December 14, 2023, European Union leaders reached a consensus to initiate accession talks with Ukraine, reaffirming their dedication to providing sustained support to the nation and its citizens for as long as necessary. Remarkably, Ukraine has worked hard on its EU initiated accession talks. Key findings of the 2023 Report on Ukraine issued by the European Commission in the beginning of February last year, showed the tremendous development that was made by Ukraine despite the ongoing war in order to open negotiations successfully but also strengthen the Digital Single Market.

The report on the *acquis* alignment of Ukraine highlights the important progress made by Ukraine in the digital sector.

- ➔ The legislation in Ukraine regarding electronic communications and information technologies is being brought in line with EU practices. This is primarily done through two key laws: the Law on Electronic Communications and the Law on the National Commission for State Regulation of Communications, Radio Frequency Spectrum, and Postal Services. These laws are modeled after the EU's Directive 2018/1972, which established the European Electronic Communications Code. The laws aim to ensure that the regulatory body's legal status aligns with European standards.

- ➔ A new regulatory authority has been established in Ukraine that is legally and functionally independent, with exclusive regulatory responsibilities and decision-making powers. However, full implementation of these laws requires adopting many secondary regulations, many of which have been enacted, focusing on EU principles like transparency and general authorization. Despite these efforts, the regulator faces financial constraints, limiting its capacity to fully perform its functions.
- ➔ Security challenges caused by the Russian aggression have delayed the implementation of acts related to radio spectrum policy, including reallocating the 700 MHz band for mobile communications. However, Ukraine's e-government system has progressed well, particularly with the 'State in a Smartphone' initiative launched in 2019, demonstrating resilience and adaptability during the war.
- ➔ Ukraine is working towards aligning its legislation with EU roaming policies, potentially joining the EU's 'Roam like at home' scheme. In electronic identification and trust services, Ukraine shows significant alignment with EU standards, particularly after adopting legislation for mutual recognition of electronic trust services. Ukraine's open data policy aligns well with the EU Open Data Directive, ranking high in the EU Open Data Maturity Report 2022. Additionally, Ukraine is implementing a national cybersecurity strategy, seeking alignment with EU standards, though it currently lacks a 5G network and plans for EU-aligned 5G security.
- ➔ In audiovisual policy, Ukrainian legislation is broadly in line with the EU's Audiovisual Media Services Directive, with recent laws ensuring media regulator independence and content transparency. However, stricter rules are in place for retransmitting EU content, particularly aimed at preventing Russian TV channels from broadcasting in Ukraine, a measure necessary for the current security climate.

In summary, the government is actively aligning its electronic communications and information technology laws with EU standards. While financial constraints and security challenges due to the Russian conflict pose hurdles, progress in e-government, cybersecurity, and audiovisual policies indicate a strong commitment to EU integration.

4. Data Protected Ukraine

GDPR implementation in Ukraine is essential for integration into the EU Digital Single Market. For Ukrainian organizations and businesses that process EU residents' data, it is not just a legal obligation but also a sign of their commitment to data protection and privacy standards to ensure compliance with their rights. Implementing mechanisms and procedures to respect these rights requires significant adjustments in data handling practices, IT systems, and customer service protocols. Moreover, raising awareness and understanding of these rights among Ukrainian data subjects, when applicable, improves transparency and builds trust, aligning Ukraine's digital market practices with European norms and expectations.

Ukraine's primary legislation for data protection is the 2010 Law on Personal Data Protection ("PDP"), which sets out the basic rules and responsibilities regarding the collection, processing, and use of personal data by both private entities and the Ukrainian government[6].

Apart from the PDP, the main sources of Personal Data protection in Ukraine are among others:

- ➔ The Constitution of Ukraine
- ➔ The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and Additional Protocol to it, ratified by Ukraine in 2010
- ➔ The Civil Code of Ukraine
- ➔ A number of regulations approved by the Ukrainian Parliament Commissioner for Human Rights
- ➔ Model Rules on Personal Data Processing
- ➔ The Law of Ukraine "On Information"
- ➔ The Law of Ukraine "On Electronic Commerce"
- ➔ The Law of Ukraine "On Electronic Communications," and
- ➔ The Law of Ukraine "On Protection of Information in the Information and Telecommunication Systems"[7].

In June 2014, Ukraine signed an Association Agreement with the European Union. The General Data Protection Regulation (GDPR) was not yet established at that time, so it could not be incorporated into the agreement. Despite this, Article 15 of the Agreement committed Ukraine and the EU to work together to achieve high levels of personal data protection that would align with top European and international standards.

Ukraine, not being a member of the European Union, is not directly subject to the EU's General Data Protection Regulation (GDPR). However, Ukraine is making efforts to align with the EU-Ukraine Association Agreement, which includes amending its data protection laws to be in line with the GDPR. The Ukrainian Cabinet of Ministers committed to these amendments by October 25, 2017, and in October 2017, announced plans to adopt the GDPR into its national laws by May 25, 2018, the date when the GDPR would come into effect across the EU[8].

[6] https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf
[7]https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook/emea/ukraine/topics/key-data-privacy-and-cybersecurity-laws
[8]https://www.connectontech.com/2018-3-21-ukraine-may-bring-its-data-privacy-legislation-into-correspondence-with-the-gdpr-as-early-as-25-may-2018/

In response to major developments in global and especially European personal data protection standards, the Ukrainian legislature has crafted two proposed legislations. These are focused on integrating the General Data Protection Regulation (EU) 2016/679 (GDPR) and the updated Convention 108+ for the Protection of Individuals with Respect to Automatic Processing of Personal Data into Ukrainian law.

To achieve compliance, a proposed Law on Personal Data Protection was submitted to the Ukrainian Parliament in June 2021. Unfortunately, this initial draft law was rejected on August 16, 2022. Following this setback, a revised version of the law, called the Second Draft Law, was introduced to Parliament on October 25, 2022[9]. The Second Draft Law aims to revise Ukraine's data protection framework to align with GDPR standards. The revisions address aspects such as terminology, the rights of data subjects, and the responsibilities of data controllers and processors.

The proposed Draft Law on Personal Data Protection (PDP) introduces several important changes, including new definitions for terms like biometric data, data breaches, genetic data, health data, overall annual turnover, pseudo-anonymization, profiling, and large-scale data processing. The law also establishes new principles for data processing, such as legality, fairness, transparency, data minimization, purpose limitation, accuracy, storage limitation, integrity, confidentiality, and accountability.

The grounds for data processing have also been revised, with the introduction of the concept of "legitimate interest." The Draft Law on PPD ("On Personal Data Protection") also enhances the consent framework by specifying how consent should be acquired, situations where consent is not considered given, and limitations on using consent as a processing basis when other grounds are applicable. The law also provides a refined definition of sensitive data, along with a broader range of processing conditions. Additionally, it requires non-Ukrainian controllers and processors to appoint representatives within Ukraine. Controllers (or their representatives) must maintain detailed records of their processing activities, and mandatory regular data protection impact assessments (DPIA) are required, with obligatory prior consultations with the data protection authority in cases of high-risk processing.

The Draft Law on PPD also introduces specific circumstances under which controllers and processors are required to appoint data protection officers (DPOs), and outlines the qualifications for these officers. Furthermore, the law introduces a new scale of administrative fines for violations of data protection laws. The fines vary based on the severity of the breach, with the most serious infringements subject to fines up to 5% of a company's annual turnover, with a minimum of UAH 300,000 (around USD 10,100) per violation. The second legislative

[9] https://www.dataguidance.com/notes/ukraine-data-protection-overview

proposal, the Draft Law on the Data Protection Authority (DPA), aims to create an independent governmental body responsible for policy formulation (through mandatory regulations) and enforcement (via prosecuting violations) in data privacy and public information access. The National Commission for Personal Data Protection and Access to Public Information would have semi-investigative powers and the capability to probe into violations with the assistance of technology experts and professionals from various fields.

The DPA would have the authority to gather necessary information, including confidential and restricted access data, from any individual, company, or organization. It would be granted access to information and telecommunication systems, databases, and registers, even those with limited access, managed by state bodies or local authorities. This includes the use of state and government communication means, special communication networks, and other technical resources.

The DPA would be allowed access to personal data handled by the controller and/or processor, as required for fulfilling its duties. It would have the capacity to investigate potential breaches of Ukraine's "On Personal Data Protection" and "On Access to Public Information" laws, either based on complaints or on its own initiative. The authority could request written explanations from government and private entities, organizations, employees, and individuals regarding situations that might indicate legal violations.

The DPA could obtain information from foreign countries' databases and registers, including paid information, if needed for accessing information. It would have the power to impose fines on entities processing personal data. The authority could appeal to courts for the enforcement of relevant laws. Additionally, the Draft Law introduces new fines for non-compliance with the DPA's decisions or requests, or for denying access to the DPA for investigational purposes:

- ➔ Individuals could face fines ranging from UAH 20,000 to UAH 100,000 (approximately USD 678 to USD 3,390), and legal entities could be fined from 0.5% to 1% of their total annual turnover from the previous year, but not less than 3,000 tax-free minimum incomes (around USD 1,729). Repeat non-compliance would result in a fine doubled from the previous amount[10].

The Ukrainian Parliament is anticipated to pass these drafts and other necessary regulations to advance data privacy reform. This move is part of Ukraine's integration into the EU Digital Single Market, fulfilling obligations under the EU-Ukraine Association Agreement, and supporting the broader government digital agenda.

The Draft Law on Personal Data Protection in Ukraine aims to enhance the business landscape by introducing several key amendments. Firstly, the law introduces unified and expanded

[10] https://www.dataguidance.com/opinion/ukraine-draft-data-protection-bill-what-you-need

terminology, such as definitions for biometric data and data breaches, providing businesses with a clearer understanding of their data handling responsibilities. This enhanced clarity aligns company operations more closely with legal standards.

Secondly, new data processing principles such as lawfulness, fairness, and transparency are being established. These principles aim to make companies more responsible in their data processing, aiding in compliance and building trust with customers and partners. Moreover, the law updates the grounds for data processing and refines the consent concept. This revision aids companies in ethically and lawfully obtaining and using personal data, thereby reducing legal risks and boosting customer trust. Additionally, the handling of sensitive data is enhanced with an expanded list of processing grounds. This broadened framework allows businesses to better protect individual rights while effectively utilizing sensitive data.

For foreign companies, the requirement to appoint local representatives simplifies compliance with Ukrainian regulations and facilitates easier operation within the country. The law also mandates companies to maintain records of their processing activities and conduct regular Data Protection Impact Assessments (DPIAs). This ensures ongoing compliance and effective risk management, protecting companies from potential legal issues and data breaches. The appointment of qualified Data Protection Officers (DPOs) is another requirement. This ensures companies have dedicated personnel for managing data protection, enhancing their ability to respond effectively to regulatory changes.

A new scale of administrative fines is introduced, varying according to the severity of violations. This clarity in potential financial consequences encourages businesses to prioritize data protection. Lastly, the establishment of an independent Data Protection Authority, the National Commission for Personal Data Protection, promises a more structured regulatory environment. This body will enforce regulations and provide guidance to companies, facilitating smoother business operations.

In essence, these proposed changes are aimed at fostering a more transparent, responsible, and legally compliant data processing environment in Ukraine. This is likely to lead to increased consumer trust, reduced legal risks for businesses, and an overall more favorable business climate.

5. Ukrainian Digital Content Policy

Last year, the European Union rolled out the Digital Services Act (DSA) with the aim of standardizing content regulation across all EU member states. This is crucial legislation for the Digital Single Market, and it is important for Ukraine further DSM integration. Providers of digital services have until 24 February 2024 to implement the requirements. The DSA primarily provides for information and transparency requirements that online intermediaries and platforms must comply with to varying degrees if they offer services in the EU. These include,

for example, online marketplaces, social networks, content sharing platforms, app stores and search engines[11].

In early 2023, the European Union released an evaluation of Ukraine's progress towards EU membership. The report stated that Ukraine has made moderate progress in digital transformation and media. Notably, the country has excelled in delivering digital services to its citizens and businesses, and in using technology to increase the transparency and efficiency of its public administration. Ukraine's legislative infrastructure largely conforms to EU standards, particularly with the European Electronic Communications Code.

Ukraine has been actively aligning its legal framework with European Union directives in the fields of electronic commerce and digital services. The country has fully implemented Directive on electronic commerce and Directive concerning digital content and services, by revising Ukrainian consumer protection and digital content laws[12]. In addition, Ukraine is considering incorporating EU regulations like the Digital Services Act and the regulation on fairness and transparency for online intermediation services into a proposed Ukrainian law on digital services. Consultations with the EU have already begun in this regard.

The Ukrainian Law "On Digital Content and Digital Services" was enacted on August 10, 2023, to align Ukraine's digital sector regulations with the standards set by the European Union scheduled to take effect on March 2024[13]. This law is a crucial part of Ukraine's legal landscape. It establishes a legal framework for providing digital content and services under contractual agreements and focuses on protecting consumer rights in the digital realm.

Ukraine has already implemented various laws, including the Consumers Protection Law, Cloud Services Law, Virtual Assets Law, and E-Commerce Law. However, the Digital Content Law holds unique significance. It harmonizes Ukrainian legislation with EU norms and strengthens consumer protections specifically in the digital content and services sector. This law is particularly geared towards business-to-consumer (B2C) relations, unlike the Cloud Services Law, which focuses more on business-to-government (B2G) interactions.

The Digital Content Law safeguards consumer rights in the digital sector more structurally than the Consumers Protection Law. It provides clear guidelines on warranties, refunds, and dispute resolution. Additionally, it complements the Cloud Services Law by covering cloud services in B2C relations. It also distinguishes between digital content and virtual assets, which are regulated under the Virtual Assets Law.

[11] https://kpmg-law.de/en/these-legislative-changes-will-affect-companies-in-2024/

[12] https://eu-ua.kmu.gov.ua/wp-content/uploads/Zvit_EN.pdf

[13]https://insightplus.bakermckenzie.com/bm/intellectual-property/ukraine-aligning-consumer-protection-law-with-european-union-standards

This law works in tandem with the E-Commerce Law by treating traders as e-commerce actors. It defines digital content as data in digital form, including a variety of formats such as computer programs, mobile apps, videos, audio files, digital games, and e-books. It also includes services that enable consumers to create, process, store, or access digital data, like cloud computing and social media services. Notably, the law's scope extends to digital content and services delivered through physical means, such as DVDs or USBs, when their primary function is to carry digital content. It also applies to digital content or services made to a consumer's specifications.

Additionally, the upcoming Consumer Rights Protection Law in Ukraine is set to be enacted on July 7, 2024. The aim is to bring the country's consumer protection standards in line with European Union norms, with a particular focus on e-commerce.

- **Broader Protection Scope:** This Law broadens consumer protection to include marketplaces, classifieds, and price aggregators. It also expands its coverage to food products. However, it excludes certain categories like medical services and gambling.
- **Digital Content and Withdrawal Rights:** The Law introduces specific regulations for digital content and services. It establishes a new right of withdrawal for contracts involving digital content.
- **Warranty Periods:** The Law mandates a two-year warranty for new items, one year for used items, and ten years for real estate. However, it limits warranty periods to the product's lifespan if it is less than two years.
- **E-Commerce Registration and Portal:** E-commerce businesses must register on the E-Consumer Portal by July 7, 2026, to be recognized as "verified sellers." This portal facilitates communication between businesses, consumers, and the consumer protection authority. It also allows for consumer complaint filing. Unregistered e-commerce sites may face access restrictions by ISPs, as enforced by the consumer protection authority.
- **Enhanced Information Requirements:** Both online and offline sellers must meet revised precontractual information requirements. There is a comprehensive list of details needed for distance contracts. Information can be provided through various methods, including online platforms[14].

Implementing the EU acquis in Ukraine poses several challenges. These include the lack of official Ukrainian translations of EU legal acts, the need for greater technical assistance and expert support to align legislation and improve the capacity of public authorities, and

[14]https://insightplus.bakermckenzie.com/bm/intellectual-property/ukraine-aligning-consumer-protection-law-with-european-union-standards

insufficient financial resources to establish new public authorities as required by reforms such as the Digital Services Coordinator (under the Digital Services Act).

However, recent legal reforms in Ukraine are bringing the country's digital services in line with EU standards. This will improve access to the European market and make it easier for local and EU-based businesses to comply with regulations. The Digital Content Law and the upcoming Consumer Rights Protection Law are key to these changes. They aim to boost consumer trust by promoting transaction transparency and fairness, which could lead to stronger customer loyalty and better business reputations.

The Digital Content Law provides a clear framework for digital services, helping businesses to plan, develop, and market their digital offerings effectively. The Consumer Rights Protection Law establishes clearer guidelines for consumer rights, including extended warranties and withdrawal rights, which encourages more consumer-friendly business practices. The extension of consumer protection to new areas such as marketplaces and classifieds expands market opportunities for businesses. The introduction of out-of-court dispute resolution mechanisms streamlines consumer complaint and dispute handling, which could reduce legal costs and speed up resolutions.

Overall, these legal updates in Ukraine provide businesses with an opportunity to improve their operations, legal compliance, and consumer engagement. This aligns them with European standards and market expectations, making them more competitive in both domestic and European markets.

6. Roadmap for the Regulation of AI in Ukraine

The pace of AI development in Ukraine is noteworthy, particularly in the context of the ongoing conflict with Russia. Experts have observed that Ukraine's approach to AI is more bottom-up and antifragile compared to other countries, making it small, scalable, and effective. Ukrainian AI is being used for a range of applications, including collecting evidence of war crimes, controlling drones, detecting disinformation, demining, and reconstruction planning.

The artificial intelligence sector in Ukraine is advancing rapidly. The country is home to over 2,000 companies that focus on software development within the AI field. In recent years, Ukraine has taken significant strides in making open data publicly available. This effort has led to Ukraine achieving the 31st rank globally in the Global Open Data Index, reflecting its commitment to open data initiatives[15].

Ukraine is set to introduce its artificial intelligence (AI) regulations in 2024, with plans to unveil them after the adoption of the European Union's AI Act. This is to ensure that Ukraine's

[15] https://data.europa.eu/en/news-events/news/open-data-ukraine

national regulations align with the broader regional law. The Ukrainian Ministry of Digital Transformation has developed a roadmap for AI, emphasizing its crucial role in various sectors, including military technology. AI has been instrumental in Ukraine for tasks such as tracking enemy personnel and equipment and shooting down missiles.

However, Ukraine has taken the first steps towards establishing legal frameworks for artificial intelligence (AI). The "Concept of the Development of Artificial Intelligence in Ukraine," formulated in December 2020, is a significant milestone in this initiative[16]. This document explicitly defines AI within the Ukrainian context, outlining its objectives, foundational principles, and specific goals for the advancement of AI technologies. Additionally, 2020 marked the commencement of a detailed AI development strategy in Ukraine. The Institute of Artificial Intelligence Problems (IAIP) of the National Academy of Sciences (NASU), along with the Ministry of Education and Science of Ukraine (MESU), spearheaded the IAIP-project titled "Creating Strategy for the Development of AI in Ukraine"[17]. This project brought together Ukrainian scientists with expertise and practical experience in AI to collaboratively develop, discuss, and promote the AI Strategy for Ukraine.

According to the concept, AI is a comprehensive array of information technologies that are capable of executing complex tasks using scientific research methodologies and sophisticated information processing algorithms. This includes the ability to autonomously generate or source data, develop and utilize proprietary knowledge bases, and create models for decision-making. Additionally, it encompasses algorithms for data handling and strategies to fulfill predefined objectives.

For the successful execution of the AI Development Strategy in Ukraine, it is crucial to handle the research and practical aspects of AI technology efficiently. A key aspect of this process is formulating a legal structure that adheres to EU and standards while harmonizing with the legislative frameworks of countries that are at the forefront of AI. This necessitates the Ukrainian government's initiative to create specific laws, including resolutions, regulations, and guidelines, tailored to the realm of artificial intelligence. The national executive body overseeing AI should base its regulations on ethical norms, with a focus on:

- **Enhancing well-being:** Prioritizing the development and use of AI that benefits human well-being.
- **Limiting harmful AI behavior**: Restricting AI systems designed to cause intentional harm.
- **Maintaining human control:** Ensuring AI systems are supervised by humans as much as possible.

[16] http://pgp-journal.kiev.ua/archive/2022/12/7.pdf
[17] https://ceur-ws.org/Vol-3513/paper09.pdf

- **Upholding legality:** Ensuring AI usage complies with existing laws[18].

In order for the strategy to be effective, it is important to support both foundational and practical AI research, as well as integrate these findings into various goods and services. To achieve this, a specialized AI Development and Implementation Committee should be created and placed under the supervision of Ukraine's Cabinet of Ministers. This Committee will be responsible for overseeing the implementation of the strategy, while scientific oversight and input will be provided by the Scientific Center for Artificial Intelligence and the Institute of Artificial Intelligence Problems. The main objective is to establish a comprehensive and dynamic AI regulatory structure by 2030, focusing on ensuring safety and promoting the growth and development of AI technologies and systems.

Moreover, the AI Development Expert Committee collaborated with the Ministry of Digital Transformation in Ukraine to create a strategic framework for regulating AI in the country. This framework, called "A Roadmap for the Regulation of Artificial Intelligence in Ukraine," was developed in October 2023 after extensive discussions with representatives from various sectors, including business, academia, science, non-governmental organizations, and government entities. The roadmap aims to guide the regulation of AI in Ukraine, taking inspiration from international trends and the expected European Union AI Act. This approach emphasizes a community-driven model, encouraging both private and public entities to take the lead in self-regulation initiatives.

According to the Ministry of Digital Transformation the strategy adopts a bottom-up approach, empowering business and public sector leaders to spearhead self-regulatory practices. This approach is poised to enhance the competitiveness of Ukrainian firms specializing in AI technology and expand their reach into international markets. Key principles of the AI regulatory roadmap include:

- **Service function:** The plan is to equip businesses with the necessary tools for compliance with forthcoming Ukrainian laws and integration into the EU market, prior to enforcing any legal regulations.
- **Balance:** The intention is not to be a frontrunner in imposing regulations but to observe and learn from the outcomes of similar endeavors in other nations.
- **Collaborative and Self-Governance:** Emphasizing a joint effort between the government and the private sector to cultivate a culture of self-regulation.
- **International perspective:** In formulating the law, a global viewpoint is adopted, considering factors like the EU AI Act's extraterritorial impact and the Brussels Effect, alongside national interests.

[18]https://www.researchgate.net/publication/362902569_Regarding_the_Draft_Strategy_Development_of_Artificial_Intelligence_in_Ukraine_2022_-_2030

➔ **Product approach:** Assisting businesses in preparing to venture into global markets.

Moreover, Ukraine has taken active steps in aligning with the implementation of the AI Act, as evidenced by the Ukrainian government's establishment of a regulatory sandbox tailored for AI developers. This initiative, highlighted by Gordiy Rumyantsev, a state expert in the Directorate of European and Euro-Atlantic Integration at the Ministry of Digital Transformation of Ukraine, offers a controlled setting[19]. In this environment, development companies can nurture their products from the earliest design stages, ensuring compliance with the anticipated requirements of the forthcoming European Union Act.

7. Cybersecurity and Cloud – key components of the Ukraine resilience

Currently, cybersecurity emerged as a paramount concern for Ukraine, given the escalating cyber threats and the critical role of secure digital infrastructure in national security and economic stability. Ukraine has implemented various laws and regulations to strengthen cybersecurity measures, protect critical information infrastructure, and mitigate cyber risks. As a candidate country for the EU Membership, Ukraine must transpose into national law all the Acquis Communautaire; Chapter 10 of the acquis is about Information Society and Media, and it includes cybersecurity legislation[20]. By aligning its cybersecurity legislation with EU directives and best practices, Ukraine aims to enhance cyber resilience, bolster trust in digital services, and foster a secure and resilient digital ecosystem.

The Ukrainian cybersecurity landscape has evolved significantly over the years, with the establishment of a formal framework and various bodies to address cyber threats. Challenges in the cybersecurity domain in Ukraine include the need for more explicit legislative definitions, particularly concerning cyberterrorism, and the requirement for specialized investigative units and training for personnel dealing with cybercrimes. Moreover, there's an acknowledged need for more robust scientific research and development in the field to keep pace with rapidly evolving cyber threats. The 2017 Law "On the Basic Principles of Cyber Security of Ukraine" marked a significant step in formalizing the country's approach to cybersecurity, though the formation of related bodies began much earlier[21]. In 2007, the State Special Communications and Information Protection Service was established, leading to the creation of the Computer Emergency Response Team (CERT-UA) and the State Cyber Protection Centre.

The development of these bodies has been accompanied by efforts to align with international standards and practices, such as gaining accreditation from international cybersecurity organizations. Additionally, the restructuring and expansion of tasks within these bodies have

[19] https://www.kmu.gov.ua/en/yevropejska-integraciya/coordination/cifrova-transformaciya
[20] https://ecs-org.eu/ecso-uploads/2024/01/Collaboration-between-ECSO-and-Ukraine-Dec-2023.pdf
[21] https://www.redalyc.org/journal/4762/476273700003/html/

been a continuous process, reflecting the dynamic nature of cyber threats. One of the critical aspects of Ukraine's cybersecurity strategy has been the emphasis on a coordinated approach at various levels - national, regional, and international. This strategy involves not only government entities but also the private sector and civil society, underlining the comprehensive nature of cybersecurity.

In 2019, the Ukrainian government and president enacted several key resolutions and decrees to enhance the security and defense sectors' preparedness. These included establishing standardized procedures and criteria for reviews in public security, defense industry, and intelligence agencies. Notably, the reviews in cyber defense and critical information infrastructure were not conducted due to the absence of government-approved procedures. These reviews have been instrumental in forming a suite of long-term national security documents, such as the National Security Strategy, Military Security Strategy, and Strategies for Public Security, Civil Protection, Defence Industry, and Cyber Security of Ukraine. These strategies form the foundation for state programs and other planning documents in national security and defense[22].

However, the absence of a formal review process for cyber defense of state information resources and critical infrastructure is a significant gap. To address this, it's necessary to develop and approve procedures for such reviews, drawing from international and national experiences. This includes establishing methods for conducting reviews by law enforcement, organizing public-private partnerships for cyber security, and ensuring the security of state and municipal resources managed through cloud computing.

The President of Ukraine's decree "On some measures to improve access of individuals and legal entities in electronic services" aims to strengthen the security of national electronic resources and systems. Cybersecurity is a crucial aspect of national security and defense, as outlined in Ukraine's Constitution and the Law on National Security.

Ukraine is committed to following international standards in cybersecurity. This commitment involves adhering to the Budapest Convention, also known as the Convention on Cybercrime of the Council of Europe, which Ukraine ratified in 2005. Additionally, Ukraine looks to the European Commission's Directive on security of network and information systems (NIS and NIS 2 Directive) as a significant international framework for enhancing cybersecurity standards within the EU. Although the Directive is not legally binding on Ukraine due to its non-EU status, it provides valuable guidelines and measures to improve Ukraine's national policies and administrative strategies in cybersecurity and cyber protection.

In June 2021, the European Union and Ukraine held their first Cyber Dialogue to strengthen Ukraine's cybersecurity defenses and improve its legal framework. During the dialogue, both

[22] https://ceur-ws.org/Vol-2866/ceur_276_283_pleskach.pdf

parties exchanged updates and progress regarding their respective cyber domains. The main topics discussed were institutional and policy developments, with a focus on the revision of the EU's Network Information Security (NIS) Directive and Ukraine's efforts to align its cyber policies and laws with the EU's standards and regulatory framework.

The second round of Cybersecurity Dialogue in 2022, emphasized the need to enhance cyber resilience amid Russia's ongoing war against Ukraine[23]. In a recent dialogue, the EU showed solidarity with Ukraine against cyber-attacks targeting its infrastructure and discussed the cyber threat landscape. Both sides reviewed their cybersecurity frameworks, including the EU's NIS Directive and Ukraine's alignment efforts. The discussions emphasized international cooperation's importance in cybersecurity and highlighted Ukraine's focus on joint projects with the EU, particularly in light of its EU candidate status. The EU has committed significant financial and material support, amounting to €29 million, to enhance Ukraine's cyber resilience. The dialogue ended with a pledge to further strengthen cybersecurity collaboration.

Moreover in November 2023, The European Union Agency for Cybersecurity (ENISA) has established a Working Arrangement with Ukrainian counterparts, with a focus on several key areas:

- **Cyber Awareness & Capacity Building:** This includes efforts to strengthen cyber resilience, such as participating in EU cybersecurity exercises and trainings, potential secondment arrangements, and sharing cyber awareness tools and programs.
- **Best Practice Exchange:** The aim is to align legislation and implementation approaches, particularly in critical areas like the implementation of key cyber legislation (e.g., NIS2) and sectors like telecommunications and energy.
- **Knowledge and Information Sharing:** This involves a more systematic exchange of knowledge and information about the cybersecurity threat landscape to enhance mutual situational awareness among stakeholders and communities[24].

This arrangement encompasses both immediate structured cooperation actions and the groundwork for long-term alignment in cybersecurity policies and methods.

Cybersecurity policies play a crucial role in the use of cloud solutions. The military aggression of the Russian Federation against Ukraine, which began in 2014, has had a significant impact on the development of cloud technologies in the country. The escalation of the conflict, especially in the eastern regions, forced many commercial, state, and financial entities to move their infrastructure to safer regions in the central and western parts of Ukraine. Unfortunately, several organizations lost their physical servers, which contained critical data,

[23] https://www.eeas.europa.eu/eeas/ukraine-and-eu-held-second-round-ua-eu-cybersecurity-dialogue_en
[24] https://www.enisa.europa.eu/news/enhanced-eu-ukraine-cooperation-in-cybersecurity

during the conflict, or were unable to evacuate them in time. This situation has emphasized the importance of transferring data from local servers to cloud storage, ensuring data preservation in the face of military expansion and reducing organizational relocation costs.

After the escalation of the conflict in Ukraine in February 2022, companies such as Google offered free access to cloud technologies to Ukrainian businesses. This was partly due to the financial constraints faced by businesses in adopting advanced technologies. The conflict accelerated the adoption of cloud services not only by businesses but also by government and local authorities. This transition played a crucial role in maintaining the stability of government electronic services amidst ongoing cyberattacks and physical assaults on infrastructure by the aggressor. The growing reliance on cloud technologies highlights their significant impact on various aspects of life and the economy in Ukraine, emphasizing the need for thorough scientific research into the legal framework supporting the cloud services market in the country.

In February 2022, Ukraine's Verkhovna Rada passed the "Law on Cloud Services," marking a significant legislative step in regulating cloud services[25]. This law delineates the usage of cloud services by various entities, including state authorities and local self-government bodies. It establishes a legal foundation for the cloud services market in Ukraine and empowers state authorities to regulate and formulate policies in this sector. The law also defines private and public cloud service users and introduces the concept of cloud computing technology. It legalizes the operation of data processing centers in Ukraine, which provide services such as data storage, cloud services, and data backup.

The cloud services market in Ukraine is still in its early stages compared to more advanced economies. This is due to financial constraints and the impact of Russia's military actions on the economy. Although the "Law on Cloud Services" has set a legal foundation for cloud services, it requires refinement and additions, particularly in terms of regulating cybersecurity to comply with EU legislative frameworks and data processing centers. Effective market models for cloud services in Ukraine depend on improving regulatory mechanisms for state information resources and better oversight by the State Service for Special Communications and Information Protection. Additionally, legislative improvements are necessary for state control in the cloud sector and managing cloud computing infrastructure affected by military operations.

Ukraine's Cybersecurity and Cloud policy benefits businesses operating within its digital landscape by enhancing security and resilience, aligning with international standards, and collaborating with global partners. It also includes investment in cyber infrastructure, a comprehensive cybersecurity strategy, and legal and regulatory clarity. This policy ensures a

[25] https://kyivindependent.com/zelensky-signs-law-on-cloud-services/

digitally secure and forward-thinking environment for businesses, characterized by enhanced protection, international compliance, collaborative growth opportunities, and a strategic approach to tackling cyber threats.

8. Summary

Ukraine's efforts to integrate into the EU Digital Single Market involve aligning its digital policies and laws with EU standards. This includes adapting its legislation in areas like cybersecurity, electronic communications, data protection, and cloud services. The process began with the Partnership and Cooperation Agreement in 1998 and progressed with the EU-Ukraine Association Agreement. Ukraine's focus is on enhancing digital infrastructure and services, complying with EU laws such as GDPR, and developing a comprehensive digital strategy. The adoption of the "Law on Cloud Services" is a significant step in regulating cloud technologies. Challenges such as financial constraints and the impact of military conflicts are being addressed to ensure a successful transition. Ukraine's commitment to digital transformation is demonstrated through various legislative actions and collaborations with EU bodies, aiming to foster a more competitive and secure digital economy.