ISSN 2617-4162
E-ISSN 2617-4170

UDC 346.9:342.738:004.056:005.7
DOI: 10.32518/sals2.2026.43

Соціально-правові студії. 2026. Т. 9, № 2
Social & Legal Studios. 2026. Vol. 9, No. 2

The responsibility of business entities for breaches of data protection legislation in process management

Mykola Sakaly*
PhD in Law, Senior Lecturer
Izmail State University of Humanities
68601, 12 Repina Str., Izmail, Ukraine
https://orcid.org/0009-0007-9263-3962

Abstract. The aim of this study was to offer a comprehensive theoretical analysis of the development of the system of liability of business entities for violations of the legislation on personal data protection at the stages of collection, storage and processing. The methodology was based on the use of the systemic approach and the comparative legal method to the regulatory frameworks of Ukraine, the United States of America and the Federal Republic of Germany. Research showed that the legal responsibility of business has moved from a strategy of formal compliance to a concept of comprehensive accountability. Under this new paradigm, entities had to demonstrate the practical effectiveness of the protection algorithms they have implemented. In the Ukrainian legal field, it was found that the most critical offences arise at the stages of obtaining consent, inconsistency between the purpose of further use of information and the original purpose, and disregard for the duty to distinguish between business and personal data in personnel processes. Neglecting to identify roles in writing when engaging information processors was found to create conditions for the uncontrolled transfer of data, leading to joint and several liability for counterparties. The study revealed a fundamental difference between the German vertical system of sanctions, which prioritises technical system integrity, and the American sectoral decentralisation model, which is characterised by a strong punitive enforcement approach. It was found that European case law permits compensation for non-material damage in cases of breach of personal data protection legislation, provided an individual has experienced psychological distress or fear of unlawful data use. It was determined that institutional fragmentation in Ukraine, coupled with the absence of an autonomous supervisory authority, reduces the level of legal protection for processing operations, compared to the German model. The study confirmed the necessity of integrating the three-part public interest test into all internal regulations governing access to confidential information, with the aim of preventing mass offences in the municipal sector. The practical significance of the results lies in their potential application by legal departments and enterprise management to implement the concept of data protection by design and conduct security audits to minimise legal risks in the context of digital transformation

Keywords: personal information; data holder; processor; information leaks; institutional fragmentation; confidentiality assurance

Introduction

The relevance of studying the responsibility of business entities for breaches of data protection legislation in process management is determined by the complete digitalisation of business operations, in which information has become both a vital asset and a source of legal risks. When process management requires the continuous collection and processing of large volumes of personal data relating to clients and employees, technical failures or unauthorised access can result in financial sanctions and the destruction of the business's reputation. This issue is also relevant for Ukraine in the context of its European integration obligations, as well as the need to adapt the national legal framework to the standards set out in Regulation (EU) No. 2016/679 of the European Parliament and of the Council "On the Protection of Natural Persons with Regard to the Processing of Personal Data and On the Free Movement of Such Data (General Data Protection Regulation)" (2016). The development of clear theoretical foundations of responsibility in business processes is necessary to form a transparent and safe digital market, ensuring legal certainty that guarantees investment attractiveness and social stability.

G.I. Chanysheva (2026) considered the problem of protection of personal data of employees in terms of international standards, the compliance of Ukrainian legislation with the standards of the International Labour Organisation (ILO). The researcher has found that the current Ukrainian legislation on employees' personal data does not consider the specific requirements of data protection in la-

Suggested Citation **Article's History**: Received: 12.01.2026 Revised: 17.04.2026 Accepted: 27.05.2026 Published: 01.06.2026

Sakaly, M. (2026). The responsibility of business entities for breaches of data protection legislation in process management. *Social & Legal Studios*, 9(2), 43-55. doi: 10.32518/sals2.2026.43.

*Corresponding author (myksakalyyy@outlook.com)

bour relations. This has highlighted the need for a separate chapter on the confidentiality of professional and business qualities in the Draft Labour Code of Ukraine (2026). D. Karpyn *et al.* (2026) researched the rise of digital culture and the collective responsibility for cybersecurity in organisations. They concluded that security should be an integral part of the organisation's activity, with clear responsibility distribution among all roles, starting with risk awareness at the employee level. O.R. Balatska & I.M. Kushnir (2026) analysed the implementation of the European right to be forgotten into the Ukrainian legal field. Their research has confirmed the fragmented nature of the national regulation and the need for a comprehensive legislative reform to protect human dignity and reputation in digital space.

O.V. Klymchuk & O.I. Yaremenko (2026) studied the theoretical and conceptual foundations for harmonising Ukrainian legislation with European cybersecurity standards, focusing on the challenges facing public authorities. They proved that this process cannot be merely formal, but rather requires the transformation of the entire public administration system to strike a balance between state security interests and human rights. O.M. Bykov & V.V. Savchenko (2024), meanwhile, examined the challenges of personal data protection caused by the rapid development of information technologies and growing cyber threats, such as social engineering and large-scale information leaks. They found that national legislation cannot adapt to the pace of digitalisation, resulting in the emergence of "grey areas", while organisational management shortcomings and a lack of regular business entity audits undermine public trust in information-operating institutions. M. Surzhynskyi (2025) studied the challenges of adapting legislation to data protection standards in the field of artificial intelligence (AI), examining the provisions of the Regulation (EU) No. 2024/1689 of the European Parliament and of the Council "Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)" (2024). The author identified the need to introduce regulatory "sandboxes" and ethical codes to ensure algorithmic transparency and protection against biased automated decisions.

V. Strelnyk & I.E. Brazhnichenko (2022) studied the general theoretical aspects of legal regulation and the hierarchy of concepts in the field of information protection. The researchers analysed the criteria for classifying information as personal data and proposed a classification system based on the form of expression and the medium. They also examined the controversial issue of the legal consequences of a data subject's refusal to consent to processing during the conclusion of legal transactions. The study emphasised the importance of developing effective mechanisms to hold data controllers accountable for data becoming publicly accessible on the internet and substantiated the need to align employment and civil law contracts used by Ukrainian companies with international standards.

C. Smith & R. Hawkins (2026) proposed a methodology for demonstrating compliance with data protection principles, developing a framework for business entities and supervisory authorities. The authors demonstrated how structured compliance claims could improve consistency in the way certification bodies assess the lawfulness of data processing. A. Hennig *et al.* (2026) studied the impact of regulatory acts on software development processes by analysing discussions in open-source projects on GitHub. They found that the introduction of the European Parliament and of the Council Regulation (EU) No. 2016/679 (2016) led to a substantial rise in the number of requests to improve the privacy of the code. This indicated the success of legislative incentives to open dialogue within the professional developer community. L. Belli (2026) discussed the evolution of digital architectures and trends towards "legal interoperability" in the BRICS countries with a focus on new regulatory agencies in Brazil, India and China. The author noted that these countries were looking to coordinate policies to push for a global data governance framework, which was indicative of their desire for innovation but with more state control. P. Singh *et al.* (2026) considered the privacy threats in the field of mental health with the application of AI, discussing the ethical limits of automated psychological assessment. They found that the absence of reliable data governance in this realm could lead to patients being re-traumatised and their personal information being used to create profiles. M. Faccioli (2026) analysed civil liability for unlawful processing of data under Article 82 of Regulation (EU) No. 2016/679 of the European Parliament and of the Council, in particular, the criteria for compensation of damage. The author stressed the importance of the Court of Justice of the European Union's (CJEU) case law in the evolution of the concept of compensable damage, particularly non-material damage, which has become a point of reference for Italian and German law. L. Thomas *et al.* (2022) looked at information breach notification systems and intrusion prevention measures, considering the interaction between privacy and cybersecurity laws. The researchers found that, in cases where data owners were unable to prove that adequate technical protection measures had been implemented, case law tended towards full liability.

Despite the thoroughness of existing studies, certain gaps remain that require further investigation. In particular, the specific responsibilities of business entities within process management models are not well understood, since the responsibilities of processors and data holders often overlap. Additionally, there is a lack of systematic, comparative analysis of sanctioning mechanisms that considers the challenges of martial law and digital hypermobility.

This study aimed to provide a theoretical basis and analysis of the legal system for non-compliance with regulatory requirements concerning the protection of personal data within operational business models. To this end, the following tasks were undertaken: analysing the legal regulation of personal data protection in Ukraine, examining the mechanisms of legal responsibility and enforcement practices in the United States, Germany and Ukraine, and formulating strategic recommendations for aligning the system of business entity responsibility in Ukraine with international standards.

Materials and methods

The research methodology was based on a systemic approach, enabling the responsibility of business entities to be considered as a system encompassing the interrelationship between regulatory provisions, the composition of the parties involved (data holders and processors), types of legal responsibility and the stages of the operational data processing cycle (collection, storage and processing) within process management. The analysis covered three jurisdictions: Ukraine, the Federal Republic of Germany, and the

United States of America. The choice of these jurisdictions was determined by the need to compare a transitional legal system undergoing European integration harmonisation (Ukraine), a codified model with the highest protection standards (Germany), and a sectoral, decentralised model with active state-level law-making (the United States). The study's chronological scope covers the period from 1992, when Ukraine's fundamental information legislation – the Law of Ukraine No. 2657-XII "On Information" (1992) – was adopted, to March 2026. This enabled the retrospective development of legal norms to be analysed, as well as their adaptation to the challenges of global digitalisation.

A variety of methods were employed to analyse offences relating to personal data protection, categorised according to the type of material examined. The formal legal method was applied to regulatory legal acts in Ukraine, the United States, Germany and the European Union. These included the Criminal Code of Ukraine (2001), the Federal Trade Commission Act (2006), the Law of Ukraine No. 2297-VI "On Personal Data Protection" (2010), the Code of Ukraine on Administrative Offences (2017), the Federal Data Protection Act (2017), and EU acts in the field of data protection. This method aimed to establish the legal basis for liability, the elements that constitute offences, the conditions for liability, the authority of supervisory bodies, and the types of sanctions. Content analysis was applied to the acts and materials of supervisory authorities, analytical reports and statements. Particular focus was given to the materials of the United States FTC, the California Privacy Protection Agency (CPPA) (The 2025 privacy…, 2025; Q2 2025 privacy…, 2025), the annual report of the Commissioner for Human Rights of the Verkhovna Rada of Ukraine (n.d.), and the reports of the Federal Commissioner for Data Protection and Freedom of Information (2025). This method enabled typical violations to be identified, such as unlawful or excessive data processing, inadequate information provided to data subjects, information leaks, digital monitoring, the use of AI and shortcomings in consent to personal data processing. Statistical analysis was applied to quantitative data on fines, complaints, personal data leaks, inspections, investigations and sanctions. For this purpose, statistical and monitoring data from the DLA Piper GDPR Fines and Data Breach Survey: January 2026 (2026) were used. The aim of the statistical analysis was to compare the intensity of enforcement in Ukraine, the United States, Germany and the European Union. The case study method was applied to individual court decisions, regulatory decisions and examples of law enforcement. This category included acts of the Constitutional Court of Ukraine, in particular Decision of the Constitutional Court of Ukraine No. v002p710-12 (2012) "In the Case on the Constitutional Submission of the Zhashkiv District Council of Cherkasy Region on the Official Interpretation of the Provisions of Parts One, Two of Article 32, Parts Two, Three of Article 34 of the Constitution of Ukraine", as well as decisions of the FTC (Federal Trade Commission), CPPA, European data protection authorities and other regulators in cases concerning violations of personal data processing rules (The 2025 privacy..., 2025; Q2 2025 privacy..., 2025). This method made it possible to establish how courts and regulators qualify violations, assess the lawfulness of data processing and determine the proportionality of sanctions.

The logical legal method was applied when drafting laws such as the Resolution of the Verkhovna Rada of Ukraine No. 4065-IX "On Adopting as a Basis the Draft Law of Ukraine on Personal Data Protection" (2024), and the American Data Privacy and Protection Act (ADPPA) (2022). It was also applied to strategic documents, particularly the Commission Staff Working Document: Ukraine 2025 Report (2025), and reports on the activities of the Federal Commissioner for Data Protection and Freedom of Information (2025). This method was used to reveal the legal content of new institutional instruments that define the obligations of data holders and processors, ensuring responsibility for offences is inevitable. The final stage involved applying the comparative legal method to the Constitution of Ukraine (1996), which is an act of the highest legal force, as well as to foundational regulations and laws: Regulation (EU) No. 2016/679 of the European Parliament and of the Council (2016); the Federal Data Protection Act (2017); and the Colorado Privacy Act (CPA) (2021). The comparison was carried out according to unified criteria, including the composition of those responsible – data holders, controllers, and processors – the legal grounds for imposing sanctions, and the scope of legal responsibility for violations of personal data processing regimes. This method aimed to identify common patterns and specific differences in the legal regulation of personal data protection across different legal systems. Taken together, these methods ensured a comprehensive analysis of the responsibility of business entities by March 2026. The limitations of this study are determined by the absence of uniform case law on compensation for non-material damage in Ukraine.

Results

Legal regulation of the responsibility of business entities for breaches of personal data protection legislation in Ukraine. The constitutional and legislative basis for the protection of personal data in Ukraine is a system of regulatory guarantees for informational privacy. According to Article 32, Part Two of the Constitution of Ukraine (1996), the collection, storage, use and dissemination of confidential information about a person is strictly prohibited without their free consent, except in cases clearly defined by law for the purposes of national security, economic well-being or the protection of human rights. For business entities, this creates a basic obligation to ensure the legality of every operation, including at the business model planning stage. Breaching this principle is considered non-compliance with the general requirement of lawful processing. This constitutional provision was given an expanded interpretation in the Constitutional Court of Ukraine's Decision No. v002p710-12 (2012), which emphasises the inadmissibility of any arbitrary handling of information about individuals. Additionally, Article 31 of the Constitution of Ukraine guarantees the secrecy of correspondence, obliging businesses to provide technical protection for communication channels when transmitting data to third parties. For legal entities implementing process management, these provisions are the main regulatory restriction, since any business operation involving the processing of information of clients or employees must comply with the established criteria of legality and lawfulness at the highest legislative level. The primary legal instrument regulating the processing activities is Law of Ukraine No. 2297-VI (2010), which delineates the scope of application and the main categories of legal relations in the digital era. The law requires the controller to obtain the voluntary and informed consent of the data subject at the data collection stage.

Article 1 of the Law states that the regulations apply to any data processing activity carried out in whole or in part by automated means, and to structured paper filing systems. In the course of their activities business entities usually act as controllers or processors of personal data. Article 2 defines the controller as a person who decides the purpose of processing data and the way to process data. The processor acts on behalf of the controller under a written agreement. In the absence of such a document, or in the event of an ambiguous distribution of obligations, there may be civil liability and it may be difficult to establish the responsibilities of the parties. The determination of the roles is important in the field of process management because both entities are responsible for the protection regime under Article 24 of the Law within the limits of their powers. The controller must ensure the protection of data against unlawful processing and accidental loss, and must designate a person or unit responsible for the organisation of this work. A business entity shall respect the principle of proportionality when storing personal information; The purpose of processing shall be clearly defined and, according to Article 6 of the Law, it shall be lawful, transparent and open. Processing data beyond the necessary scope or for purposes that are incompatible with those originally stated is considered a violation. If a company continues to use information for marketing purposes after archiving or deleting it without additional consent, administrative liability arises. Another obligation is to ensure that employees have proper access to the database. The controller must appoint a responsible person and develop instructions to prevent unauthorised viewing of information by personnel without the relevant authority.

The Standard Procedure for Personal Data Processing, which was approved by the Commissioner for Human Rights of the Verkhovna Rada of Ukraine (n.d.), provides further details on these requirements by specifying that the collection method and storage period must be proportionate to the defined purpose (Ombudsman of Ukraine, 2014). Controllers must document the granting of consent by the data subject, who must give their consent voluntarily and be fully informed. In e-commerce, consent can be given by selecting a box on an information system, provided processing does not begin before activation (Law of Ukraine No. 2297-VI, 2010). Any deviation from these procedures in internal business processes may result in legal action being taken. The general principles of business entities' information activities are also regulated by Law of Ukraine No. 2657-XII (1992). Article 2 of this law sets out the principles for lawfully obtaining, using, disseminating, storing and protecting information.

The analysis provided grounds to assert the need for a clear distinction between open information and personal data with restricted access. According to Law of Ukraine No. 2657-XII (1992), confidential information is information about a person to which access is restricted by that person or by law, and its dissemination without consent is only possible in the interests of national security or economic well-being. Business entities that handle such information within the framework of process management bear disciplinary, civil, administrative or criminal liability for breaches of the established regime. In addition, the processing stages within HR processes required analysis. Article 11 of Law of Ukraine No. 2657-XII establishes that business entities must not use information about an employee's private life to assess their professional qualities. Breaching this rule during recruitment or internal evaluation is classified as the unlawful collection and use of confidential information. In such cases, the business entity is obliged to compensate for the caused moral damage in accordance with Article 31 of the above-mentioned Law. In this respect the significance of Law of Ukraine No. 80/94-VR "On Information Protection in Information and Communication Systems" (1994) is obvious for digitised management. The standard establishes the requirements for the development of complex information protection systems (CIPS), which are binding for state resources and also serve as the benchmark for the private sector. The owner or administrator of a system shall be directly liable for ensuring the integrity, confidentiality and availability of the data of the system, in accordance with Article 9 of the Law. If information is blocked, leaked or destroyed as a result of unauthorised actions, this indicates the failure of the business entity to meet its obligations. Article 11 states that individuals who violate requirements concerning technical or cryptographic protection are liable under the law.

Electronic document management is covered by Law of Ukraine No. 851-IV "On Electronic Documents and Electronic Document Management" (2003). Article 8 of this Act obliges businesses to ensure that electronic documents can be restored in their original format. Breaching file storage or integrity procedures at this stage of the business process renders the document legally invalid, and criminal liability for falsification of information may arise where intentional manipulation is detected. Additionally, under Articles 8 and 9 of Law of Ukraine No. 80/94-VR (1994), as amended in 2025, the system owner is responsible for ensuring the confidentiality and integrity of data during processing in information and communication systems. Failure to implement technical protection measures that results in the blocking or destruction of information constitutes a criminal offence under Articles 361–363-1 of the Criminal Code of Ukraine (2001).

Breaching procedures for storing electronic documents to the extent that they cannot be restored in their original format is also regarded as an offence. Telecommunications companies are subject to the additional provisions of the Law of Ukraine No. 1089-IX "On Electronic Communications" (2020), which are based on the principles of transparency and regulatory predictability. Network providers must protect user data and ensure the electromagnetic compatibility of equipment. They are liable under Article 12 of Law of Ukraine No. 2163-VIII "On the Basic Principles of Cybersecurity in Ukraine" (2017) for breaches of legislation in the field of information protection in cyberspace. Business entities' activities are also subject to rules on access to public information. While personal data usually has restricted access, information on the receipt of budget funds or property by legal entities under public law cannot always be classified. According to Article 6 of Law of Ukraine No. 2939-VI "On Access to Public Information" (2011), the "three-part test" must be applied to restrict access. This process involves assessing the public interest against potential harm. The unjustified classification of open information as confidential constitutes an administrative offence under Article 212-3 of the Code of Ukraine on Administrative Offences (2017). An analysis of enforcement practices and human rights observance in 2024 revealed systemic problems in data protection (Commissioner for Human Rights of the Verkhovna Rada of Ukraine, n.d.).

The most common violations among business entities were the processing of data unlawfully, without proper legal grounds; the insufficient informing of data subjects about their rights; and the absence of administrative documents regulating processing operations. These violations indicate a widespread breach of the duty of lawfulness and transparency at the stage of data collection and initial processing. There were also cases of passport data and addresses being published on websites without the consent of the individuals concerned (Commissioner for Human Rights of the Verkhovna Rada of Ukraine, n.d.). This led to criminal proceedings being opened under Article 182 of the Criminal Code of Ukraine (2001). Another case involved the unlawful use of data by water supply enterprises, who published information about 24,000 debtors, including debt amounts and personal account numbers. This was stopped by order of the Ombudsman (Commissioner for Human Rights of the Verkhovna Rada of Ukraine, n.d.). This case demonstrated a disregard for the principles of proportionality and purpose in the operational cycle of the enterprise; using data for public pressure instead of debt recovery through judicial proceedings can result in joint and several civil liability for non-material damage under Article 31 of the Law of Ukraine No. 2657-XII (1992). The Council of Europe (n.d.) project "Supporting the Implementation of European Human Rights Standards in Ukraine: Phase II" emphasised responsibility for the disclosure of data during video recording and the use of mobile applications in official activities. Commission Staff Working Document: Ukraine 2025 Report (2025), stated that despite certain progress, Ukraine still needs to adopt new draft laws (Draft Law No. 6177, 2021; Resolution of the Verkhovna Rada of Ukraine No. 4065-IX, 2024) in order to fully harmonise with Regulation (EU) No. 2016/679 of the European Parliament and of the Council (2016). As of March 2026, business entities in Ukraine will be subject to multi-level responsibility. Administrative liability under Article 188-39 of the Code of Ukraine on Administrative Offences (2017) for failing to comply with data protection procedures may result in civil claims for compensation for non-material damage under Article 31 of the Law of Ukraine No. 2657-XII. Criminal liability for violating privacy may arise where substantial harm is caused. To effectively manage processes, enterprises are advised to provide professional development courses for employees and conduct regular information audits in accordance with the Ministry of Digital Transformation's recommendations (Commissioner for Human Rights of the Verkhovna Rada of Ukraine, n.d.). Table 1 provides a comprehensive description of regulatory requirements and types of legal response to breaches of information processing regimes, depending on the stage of the enterprise's operational cycle.

Table 1. Matrix of the responsibility of business entities for breaches of personal data processing regulations by business process

Stage of the business process	Regulatory basis	Key obligation of the business entity	Type of legal liability for breach
Collection and initial processing	Articles 2, 6 of Law of Ukraine No. 2297-VI (2010)	Recording voluntary and informed consent; clear definition of the purpose	Administrative liability under Article 188-39 of the Code of Ukraine on Administrative Offences (2017)
Storage and archiving	Article 2 of Law of Ukraine No. 2657-XII (1992); Article 6 of Law of Ukraine No. 2297-VI (2010)	Compliance with the principle of proportionality and processing periods	Administrative liability, civil liability, including compensation for damage
Internal access and HR processes	Article 11 of Law of Ukraine No. 2657-XII; Article 24 of Law of Ukraine No. 2297-VI (2010)	Distinguishing between professional characteristics and confidential information	Disciplinary liability; civil liability under Article 31 of Law of Ukraine No. 2657-XII (1992)
Electronic document management	Articles 12, 13 of Law of Ukraine No. 851-IV (2003)	Ensuring integrity and the possibility of restoration in the original format	Criminal liability for falsification/ forgery of information
Operation of information and communication systems	Articles 8, 9 of Law of Ukraine No. 80/94-VR (1994)	Implementation of CIPS and cryptographic protection of information	Criminal liability under Articles 361–363-1 of the Criminal Code of Ukraine (2001)
Publication and disclosure	Article 29 of Law of Ukraine No. 2657-XII; Article 6 of Law of Ukraine No. 2939-VI (2011)	Conducting the "three-part test" before disclosing data	Administrative liability under Article 212-3 of the Code of Ukraine on Administrative Offences (2017); criminal liability under Article 182 of the Criminal Code of Ukraine (2001)
Use of contractors	Article 4 of Law of Ukraine No. 2297-VI (2010)	Written identification of roles and control over information processors	Civil liability, including joint and several liability of counterparties

Source: compiled by the author

A comprehensive approach combining legal literacy, technical protection and ethical responsibility is key to minimising risks for business entities operating under martial law and in the context of active European integration. In summary, the current regulatory framework in Ukraine for data protection legislation breaches is extensive but requires further codification and alignment with European Union legislation (Regulation (EU) No. 2016/679 of the European Parliament and of the Council, 2016). The key challenges are the severity and inevitability of punishment for

information leaks from state and corporate registers. This issue has become particularly relevant following the large-scale cyberattacks of December 2024 (Commissioner for Human Rights of the Verkhovna Rada of Ukraine, n.d.). Business entities must understand that personal information is not only a resource for process optimisation, but also a matter of heightened responsibility. An error can result not only in a fine, but also in reputational damage and a loss of trust in the global digital space.

Enforcement practice and mechanisms of legal responsibility of business entities in the United States, Germany and Ukraine: Comparative analysis. The institutional architecture of responsibility for breaches of personal data protection legislation in countries with developed legal systems, such as Germany and the United States, has demonstrated two distinct approaches to the normative determination of process management. The German model is based on codification and unified European Union standards (Regulation (EU) No 2016/679…, 2016), whereas the American system is characterised by sector-specific legislation and active regional and state-level lawmaking (Children's Online Privacy Protection Rule, 2013; Colorado Privacy Act, 2021). Unlike the sectoral model of the United States and the codified model of Germany, Ukraine demonstrates a transitional type of regulation. While responsibility is dispersed among the states in the United States and unified by Regulation (EU) No. 2016/679 of the European Parliament and of the Council in Germany, institutional fragmentation is observed in Ukraine as of March 2026 (Commissioner for Human Rights of the Verkhovna Rada of Ukraine, n.d.). The actual number of penalties imposed is limited by the absence of an autonomous supervisory authority.

In process management, where the collection and processing of information are integrated stages in creating added value, business entities need to implement the concept of Privacy by Design. This is not only a technological requirement, but also a legal safeguard against substantial sanctions. As of 2026, Germany's legal regime will be determined by the synergy between Regulation (EU) No. 2016/679 of the European Parliament and of the Council (2016) and the Federal Data Protection Act (2017). In German process management doctrine, attention is paid to the transparency principle enshrined in Recital 39 of Regulation (EU) No 2016/679. Natural persons must be fully informed about the scope and purposes of processing, and any deviation from the defined purpose is treated as an offence. Article 24 of Regulation (EU) No 2016/679 imposes an obligation on business entities, as controllers, to take technical and organisational measures to demonstrate compliance with the law. For German businesses, this means the need to update security policies regularly, as confirmed by the provisions of Section 38 of the Federal Data Protection Act, which establishes a mandatory requirement to appoint a data protection officer where an enterprise permanently employs more than 20 persons involved in automated processing. By comparison, in Ukraine the obligation to appoint a responsible person, or DPO, does not yet have such a clear quantitative determination, which leads to the absence of administrative documents in business processes. It was precisely this organisational deficiency that caused the unlawful publication of information about 24,000 debtors in Ukraine (Commissioner for Human Rights of the Verkhovna Rada of Ukraine, n.d.), whereas in Germany similar gaps in contractor management are punishable by fines of EUR 15 million (DLA Piper GDPR..., 2026).

An analysis of the statistical indicators presented in the DLA Piper GDPR Fines and Data Breach Survey: January 2026 (2026) revealed a high level of supervisory activity in Germany. As of January 2026, the total amount of fines imposed in this jurisdiction from the beginning of the application of Regulation (EU) No 2016/679 of the European Parliament and of the Council was €137,415,121. The figure illustrates the methodical approach of the German regulators. For instance, in 2025 the Federal Commissioner for Data Protection and Freedom of Information fined a telecommunications provider EUR 30 million for violating Article 32(1) of Regulation (EU) No 2016/679 after identifying weaknesses in the authentication of customer accounts via the hotline and online portal. It also fined the company €15 million for violating Article 28(1) because of deficiencies in its agreements with data processors that created fraud risks. Such examples highlight that process management accountability goes beyond that of the entity itself to control over the involvement of counterparties. Moreover, German legislation establishes strict administrative and criminal liability in case of particular violations. Under Section 43 of the Federal Data Protection Act (2017), a person who intentionally or negligently fails to comply with a data subject's request or gives incomplete information may be liable to a fine of up to EUR 50,000. In addition, criminal sanctions may be imposed under Section 42 of the Federal Data Protection Act: transferring data to third parties for commercial purposes without authorisation may result in imprisonment for up to three years. One of the milestones in 2025 was the decision of the CJEU (DLA Piper GDPR..., 2026) based on the request of the German Federal Court of Justice (BGH), which recognised that non-material damage under Article 82(1) of Regulation (EU) No 2016/679 of the European Parliament and of the Council may include negative emotions such as fear or irritation, if evidence of their existence is submitted. This expands the scope of civil liability of business entities to their customers for cases of leakage of information.

In contrast to the centralised solution in Europe, the legal status of data protection in the United States is based on a multi-layered system. The FTC takes a central role. Section 5 of the Federal Trade Commission Act (2006) prohibits "unfair or deceptive acts or practices". This provision puts the FTC in charge of how companies maintain their public promises of confidentiality. In Q2 2025, the regulator reached a settlement with HoYoverse for USD 20 million for violations of the 2013 Children's Online Privacy Protection Rule, misleading users regarding in-game purchases and improper data collection from minors. In Ukraine, on the contrary, the practice of enforcement has only started moving towards compensation for non-material damage in 2025. The main tools available in Ukraine are an order from the Ombudsman or a criminal case initiated under Article 182 of the Criminal Code of Ukraine (2001) (rather than sanctions, as in the US and Germany for failure to verify customer identity) (Commissioner for Human Rights of the Verkhovna Rada of Ukraine, n.d.). The development of process management is driven by the dynamic adoption of personal data protection laws at the state level in the United States.

One of the most notable examples is the Colorado Privacy Act (2021), which came into effect in July 2023. This act grants consumers the rights of access, correction, deletion

and data portability, as well as the right to opt out of targeted advertising and profiling. Businesses are required to conduct data protection impact assessments for any activity posing an elevated risk to consumer rights. Breaches of the CPA are punishable by fines of up to USD 20,000 for each individual violation. In 2026, Indiana, Kentucky and Rhode Island joined the group of states with comprehensive data privacy regulation (Understanding data privacy..., 2026). This creates a "patchwork" of legislation, meaning that companies operating nationally must harmonise their business processes according to the strictest standards, as set out in the California Consumer Privacy Act (CCPA) (2024)/California Privacy Rights Act of 2020 (2020) (Colorado Privacy Act, 2021). In 2025, the CPPA showed a strong commitment to ensuring compliance with consumer rights. A landmark settlement was reached with Honda in the amount of USD 632,500 for violations relating to connected vehicle data. The regulator found that the company had required excessive verification for the exercise of opt-out rights, and had used asymmetric choice architecture in cookie consent forms (Q2 2025 privacy..., 2025). This case showed that responsibility for process management arises not only for data leaks, but also for creating obstacles to data subjects exercising their rights. California also introduced the "Delete Act", which, from August 2026, will require data brokers to use a centralised system for processing user deletion requests (Tolson, 2026). A notable feature of the American market is the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In January 2025, the largest settlement was recorded with Solara Medical Supplies in the amount of USD 3 million following a phishing attack that compromised electronic protected health information (ePHI) (Q2 2025 privacy..., 2025). The main reason for the sanction was the absence of a comprehensive risk analysis in the organisation's business processes, which is a direct HIPAA requirement. This underlines the theoretical proposition that a business entity's responsibility is preventive in nature: punishment is not merely for the fact of an attack, but for negligence in building a protected management model.

From 2026 onwards, the Data Privacy Framework Program (n.d.) will regulate the global integration of data exchange processes between the United States and the European Union. While this mechanism provides legal certainty for the transfer of personal information, it requires American organisations to self-certify and publicly commit to complying with the DPF principles. Breaches of these principles are subject to review by both the FTC and European supervisory authorities. The European Data Protection Board's (2026) report emphasises the need to strengthen international cooperation in enforcing decisions. The main obstacle is the absence of cross-border enforcement mechanisms for fines, forcing governments to seek ways of recognising each other's regulatory acts. The US case has become an example of the influence of geopolitics on business responsibility. In the context of process management theory, the issue of harmonising US federal law arises. The draft American Data Privacy and Protection Act (ADPPA) (2022) is seen as an attempt to create a uniform standard to replace state legislation. Under the ADPPA, large data holders with revenue exceeding USD 250 million would be held to a higher standard of security. However, as of 2026, the law is still under discussion, leaving businesses in a state of regulatory uncertainty. Comparing Germany and the United States reveals a common trend: the increased personal accountability of management for systemic data protection failures. In the United States, this approach is implemented through orders of the New York State Department of Financial Services (NYDFS), which will require the mandatory implementation of multi-factor authentication for all financial institutions from November 2025 (New York Privacy Act, 2022; The 2025 privacy..., 2025).

In summary, the comparative analysis of the responsibility of business entities in Germany, the United States and Ukraine reveals that, by 2026, the global legal field had definitively shifted from a strategy of formal compliance with procedures, or a "compliance checklist", to the concept of demonstrating actual protection effectiveness, or accountability. In all three of the studied jurisdictions, data processing is now considered a potential threat to human rights and requires specific accountability mechanisms. In Germany, this has been implemented through a system of administrative fines of up to 4% of a company's annual turnover (Regulation (EU) No. 2016/679…, 2016), as well as the criminalisation of the commercial misuse of data (Federal Data Protection Act, 2017). In the United States, diversification is observed through judicial settlements and the expansion of the powers of state attorneys general, with the main emphasis placed on preventive risk analysis and combatting asymmetric choice interfaces (Colorado Privacy Act, 2021; Q2 2025 privacy..., 2025). Ukraine, being in a state of active transformation towards European integration, demonstrates a transitional type of responsibility. For Ukrainian businesses, this means integrating legal risks into the technical architecture of every operation at the design stage. Based on the study conducted and taking into account the Commission Staff Working Document: Ukraine 2025 Report (2025), a list of strategic recommendations for harmonising the domestic institutional framework has been developed (Table 2).

Table 2. Strategic recommendations for improving the system of responsibility of business entities in Ukraine

Area of reform	Essence of the measure and regulatory basis	Expected legal effect
Institutional autonomy	Establishment of a National Data Protection Commission as an independent regulator in accordance with the requirements of the General Data Protection Regulation (GDPR) (Commission Staff Working Document…, 2025).	Increased inevitability of punishment for cross-border information leaks.
Regulatory harmonisation	Adoption of new versions of laws to replace the outdated Act No. 2297-VI in order to ensure full compliance with EU standards (Draft Law No. 6177, 2021).	Reduction of barriers to the participation of Ukrainian companies in Europe's single digital market.
Process security	Introduction of mandatory CIPS audits for business entities providing public services online (Law of Ukraine No. 80/94-VR, 1994).	Minimisation of risks of unauthorised access to clients' passport and financial data.

Table 2, Continued

Area of reform	Essence of the measure and regulatory basis	Expected legal effect
Corporate responsibility	Introduction of the institution of certified DPOs for enterprises with more than 20 employees (Regulation (EU) No. 2016/679 of the European Parliament and of the Council, 2016).	Transition from reactive error correction to systematic risk management.

Source: compiled by the author

Unlike the American sectoral model, Ukrainian law is oriented towards the German model of comprehensive codification, but with the specific challenges of martial law. Whereas in Germany multi-million-euro sanctions are imposed for authentication breaches (DLA Piper GDPR..., 2026), in Ukraine the main problem remains institutional fragmentation: with 857 official complaints in one year (Commissioner for Human Rights of the Verkhovna Rada of Ukraine, n.d.), the actual number of penalties imposed is limited by the absence of an autonomous supervisory authority comparable to Germany's Federal Commissioner for Data Protection and Freedom of Information (2025) or the American FTC. At the same time, the Ukrainian experience of counteracting leaks from corporate registers, as illustrated by the case of water utilities, indicates the need to introduce the "three-part test" not only for state bodies but also for private business entities that operate with significant data sets (Commissioner for Human Rights of the Verkhovna Rada of Ukraine, n.d.). A common challenge for Ukraine, Germany and the United States remains adaptation to AI technologies, where European Regulation (EU) No. 2024/1689 of the European Parliament and of the Council (2024) and American regulations form new contours of responsibility. Effective process management as of March 2026 requires business entities in Ukraine not merely to provide technical protection for servers, but to deeply embed ethical standards for handling information. On the basis of the comparative analysis, it was recommended that Ukrainian legislation eliminate procedural discrimination against data subjects and introduce mandatory audits of comprehensive information protection systems for businesses providing public services. It is advisable to implement the German experience of appointing DPOs for large enterprises and the American practice of preventive risk analysis at the stage of designing business operations. This will ensure the real accountability of Ukrainian companies and their compatibility with the digital space of the European Union.

Discussion

The results of this study showed that by 2026, business entities' responsibility for breaches of data protection legislation had definitively transformed from formal compliance with procedures into a comprehensive accountability system, the key element of which was demonstrating the actual effectiveness of protective measures. The tendency identified in this study towards increased administrative and criminal pressure on businesses in Germany, the United States and Ukraine is consistent with D. Banisar's (2026) conclusions regarding the global unification of privacy standards, covering 85% of the world's population. This confirmed the thesis of the present study, namely that a strategy of documentary protection is no longer relevant for Ukrainian businesses, since international practice requires controllers to continuously assess the effectiveness of security algorithms. S. Gatti (2026) analysed the importance of the accountability principle in detail, which became the basis of the German model under the GDPR. The author determined that the key element in implementing Article 5(2) of Regulation (EU) No. 2016/679 of the European Parliament and of the Council (2016) was the controller's ongoing risk evaluation, with a direct impact on liability rules and fault criteria. The results of the present study concerning strict sanctions against German telecommunications providers for deficiencies in customer authentication were consistent with a case examined by A.Y. Şakar & D.H.A. Bağce (2026). The scholars assessed a data breach involving an airline and found that failing to implement administrative measures resulted in serious sanctions, thus confirming the theoretical thesis of the present study regarding the preventive nature of legal responsibility. This approach was supplemented by M. Cura *et al.*'s (2026) proposal for forensic photography. The researchers developed a smartphone framework that ensured compliance with the four pillars of the GDPR. This demonstrates that technological innovations can be both a source of risk and a tool for compliance. This shows that technical insecurity in business processes can automatically result in legal offences, where technological solutions must act as both a source of risk and an instrument of compliance.

This study's comparative analysis of the legal frameworks of the United States and Germany highlighted the "transatlantic divide", a concept that has been the subject of philosophical and legal reflection by R. Poscher & E. Orrù (2026). The authors stressed that the concept of privacy was complex and ambiguous: in the United States it was often understood as the right to be left alone, in Germany it was based on informational self-determination . These differences have a direct impact on the organisation of process management of business entities of both jurisdictions. In addition, S. Singal & N. Chorev (2026) examined the relationship between data collection practices and neoliberalism. They concluded that data protection policy was still largely compatible with neoliberal market rationalities. Deepanshu & A. Kumar (2026) have analysed the need for Ukraine to create an autonomous supervisory authority, as found in this study in India. The authors concluded that the success of India's new Data Protection and Data Security Act (DPDP Act) of 2023 depended on regulatory clarity and institutional independence. T. Alok & A. Ram (2026) compared the Indian law to the GDPR and concluded that the Indian setup is still in nascent stages of development. This led to the need for more detailed guidance for businesses, that is similar to the conclusions of the present study regarding the transitional period in Ukraine. A. Siddiqui (2026) further noted that the Indian approach needed better institutional safeguards and clear rules for cross-border transfers to meet global standards. The present study focused on the financial services sector, where the risk of data leaks has led to fictitious debtors being created. This was consistent with the findings of A.R. Kristanto & S.R. Slamet (2026), who investigated the liability of Indonesian banks. The scholars proved that corporations were

liable under the principles of "strict liability" and "vicarious liability", even when violations were committed by internal staff. A. Suciara *et al.* (2026) compared the approaches in Indonesia and Japan, emphasising the advantages of objective liability without proof of fault for protecting the rights of bank clients in the context of modern digital transformation. This fully supports the present study's proposals for reforming Ukrainian legislation on offences.

Process management in the public sector also entails high risks of offences, particularly with regard to the sale of civil servant data, as studied by E.S. Darmayanti & A.E. Subiyanto (2026). They found that the complexity of data classification made it difficult to prove the element of "unlawfulness" in the use of information, highlighting the need to strengthen governance within state agencies. This study also found that implementing AI in business processes requires new frameworks of responsibility, which is consistent with the work of U. Joshi *et al.* (2026). The authors identified difficulties in assessing causation in cases of AI errors in medicine, calling for integrated liability legislation that would not stifle innovation. N.U. Qinvi *et al.* (2026) studied the problem of biometric data protection in AI-based photo marketplaces. They identified that indirect consent mechanisms and the complexity of algorithms created a gap between legal norms and practice, requiring greater accountability from platforms. G. Anbarasi & D. Sankar (2026), in the context of criminal justice and AI, pointed out significant discrepancies in the regulation of personal data collection between the EU and India. Discrepancies such as these pose a privacy risk in the use of algorithms for investigative purposes or to monitor people convicted of crimes. These results supported the current study's conclusions regarding the need for ethical supervision of sensitive information processing. The present study's findings concerning the importance of the right to be forgotten in the digital space were consistent with K. Faisal's (2026) work. The author examined the tension between freedom of expression and the protection of data on criminal convictions, demonstrating that the principle of proportionality is key to balancing public access to information with individual privacy. The new Albanian law analysed by I.S. Berisha *et al.* (2026) successfully approximated national law to the GDPR by prioritising the principles of lawfulness and data minimisation. This serves as an example of the harmonisation described in the present study for Ukraine. The present study found that the legal responsibility of business entities in Ukraine must be clearly defined according to the stages of the management process, from obtaining consent to the final destruction of information. The systemic absence of certified personal data protection officers was found to create gaps in the organisational structure of national enterprises, causing mass offences in the municipal and agricultural sectors. The necessity of integrating the "three-part test" procedure directly into managerial decision-making algorithms to distinguish between public interest and restricted access was proven. Theoretically, it was substantiated that enforcement practice should shift towards recognising non-material damage as an objective consequence of information leakage. Implementing these results in practice will enable Ukrainian businesses to enforce data protection and prepare their internal operations for full regulatory integration into the European digital space.

In summary, the study proved that, by 2026, responsibility for privacy violations had definitively acquired the character of an "accountability-driven" model. The results of the present study coincided with the work of international scholars on the merits of transitioning to strict liability in the financial sector, the importance of the independence of regulatory institutions, and the challenges associated with implementing AI. The importance of the results lies in confirming that, to ensure effective process management, business entities in Ukraine, the United States and Germany must integrate legal safeguards into the technical architecture of every business operation.

Conclusions

The scientific study provided theoretical substantiation for the transformation of business entities' responsibility as of spring 2026. This confirmed the definitive transition from a strategy of formal compliance with procedures to the concept of real accountability, demonstrating the effectiveness of protective measures. The study revealed that, in the context of modern process management, information processing has evolved from a technical operation to a legal risk factor, with business responsibility emerging as the primary regulator of the digital market. The study also confirmed that Ukraine has an extensive but institutionally fragmented mechanism for imposing liability that requires modernisation.

Within the Ukrainian legal framework, it was determined that the liability of business entities hinges on the precise identification of their roles as either data controllers or processors. The analysis revealed that offences most frequently occur during the consent collection stage, where businesses often fail to fulfil their duty to provide clients with comprehensive information. At the storage stage, it was found that the critical issue is inconsistency between the processing purpose and initial arrangements, leading to administrative sanctions. Within internal HR processes, a systemic breach of the duty to distinguish between an employee's business characteristics and information about their private life was identified, creating grounds for civil claims. At the stage of electronic document management, it was found that the obligation to ensure the authenticity and integrity of documents is often ignored, which jeopardises the legal validity of business operations. It was found that using information processors without detailed written agreements in place constitutes widespread non-compliance and leads to the uncontrolled transfer of information to third parties. Analysis of enforcement practices revealed that state and municipal enterprises frequently fail to comply with the proportionality procedure when publishing debtor lists, which constitutes gross interference with private life. The absence of certified personal data protection officers within organisations' internal structures was found to create systemic preconditions for cyber incidents. Despite a significant number of complaints from citizens, it was found that real legal responsibility remains low due to the absence of an independent regulator capable of imposing effective sanctions.

Analysing the models revealed a fundamental difference between the European and American systems. Germany has a strict vertical system of responsibility, where the total sanctions amounting to EUR 137 million reflects the priority given to protecting data integrity, even in cases of minor technical vulnerabilities. In contrast, the United States has confirmed the dominance of sectoral decentralisation, or a "patchwork" system, where settlements of USD 20 million for violations of children's privacy demonstrate a punitive

approach to regulation. A common trend across all jurisdictions is the increased personal responsibility of management for systemic information leaks, making data protection an integral part of corporate governance. For Ukraine, this means overcoming the stage of merely completing formal documents and moving towards the real integration of technical and legal security tools into every business process. The results obtained mean that effective process management in Ukraine is impossible without full harmonisation with European Union regulations and the establishment of an independent supervisory authority. The study's practical value lies in identifying algorithms for minimising legal risks through implementing the concept of "protection by design". Further research should focus on developing legal mechanisms for holding those responsible for algorithmic discrimination and automated decision-making in global digital networks to account.

Acknowledgements

None.

Funding

None.

Conflict of interest

None.

References

[1] Alok, T., & Ram, A. (2026). Balancing privacy and practicality in the age of technology: A comparative analysis of the EU general data protection regulation and India's digital personal data protection act. In A. Sharma, A. Sehrawat & T.K. Chandola (Eds.), *Humanities and social sciences: A multidisciplinary approach* (pp. 135-143). London: Routledge.

[2] American Data Privacy and Protection Act (ADPPA). (2022). Retrieved from https://www.consumerprivacyact.com/american-data-privacy-and-protection-act-adppa/.

[3] Anbarasi, G., & Sankar, D. (2026). Data protection challenges in AI-driven criminal justice in the EU and India. *International Journal of Computational Intelligence Systems,* 19, article number 20. doi: 10.1007/s44196-025-01037-6.

[4] Balatska, O.R., & Kushnir, I.M. (2026). Right to be forgotten in digital space: Implementation of European standards into Ukrainian legislation. *Analytical and Comparative Jurisprudence*, 1(1), 11-15. doi: 10.24144/2788-6018.2026.01.1.1.

[5] Banisar, D. (2026). National comprehensive data protection/Privacy laws and bills 2026. *SSRN*. doi: 10.2139/ssrn.1951416.

[6] Belli, L. (2026). Understanding the Brics countries, their digital cooperation, and their emerging data protection architectures. In L. Belli & W.B. Gaspar (Eds.), *Personal data architectures in the BRICS countries* (pp. 1-32). Oxford: Oxford University Press. doi: 10.1093/9780198974468.003.0001.

[7] Berisha, I.S., Kerka, E.P., & Andersons, A. (2026). Personal data protection and privacy. *European Journal of Economics, Law and Social Sciences*, 10(1), 84-94. doi: 10.2478/ejels-2026-0009.

[8] Bykov, O.M., & Savchenko, V.V. (2024). Personal data protection in modern legislation. *Legal Bulletin*, 14(4), 67-72. doi: 10.31732/2708-339X-2024-14-A9.

[9] California Consumer Privacy Act (CCPA). (2024, March). Retrieved from https://oag.ca.gov/privacy/ccpa#sectiona.

[10] California Privacy Rights Act of 2020. (2020, November). Retrieved from https://thecpra.org/.

[11] Chanysheva, G.I. (2026). The right of an employee to the protection of personal data: ILO standards and the legislation of Ukraine. *Academic Visions*, 51.

[12] Children's Online Privacy Protection Rule. (2013, July). Retrieved from https://www.ftc.gov/system/files/2012-31341.pdf.

[13] Code of Ukraine on Administrative Offences. (2017, June). Retrieved from https://zakon.rada.gov.ua/laws/show/8073-10#Text.

[14] Colorado Privacy Act. (2021, July). Retrieved from https://www.consumerprivacyact.com/colorado-privacy-act-cpa/.

[15] Commission Staff Working Document: Ukraine 2025 Report. Accompanying the Document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2025 Communication on EU enlargement policy. (2025, November). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025SC0759.

[16] Commissioner for Human Rights of the Verkhovna Rada of Ukraine. (n.d.). *Annual report of the Commissioner for Human Rights of the Verkhovna Rada of Ukraine on the state of observance and protection of human and civil rights and freedoms in Ukraine in 2024*. Retrieved from https://www.ombudsman.gov.ua/storage/app/media/uploaded-files.

[17] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/en/254%D0%BA/96-%D0%B2%D1%80#Text.

[18] Council of Europe. (n.d.). *Supporting the implementation of European human rights standards in Ukraine: Phase II*. Retrieved from https://www.coe.int/uk/web/kyiv/supporting-implementation-of-the-european-human-rights-standards-in-ukraine/.

[19] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.

[20] Cura, M., Loureiro, R., Marcelino, P., Rodrigues, V., & Andrade, J.P. (2026). General data protection regulation: An algorithmic proposal for forensic photography. *International Journal of Legal Medicine*, 140, 1689-1697. doi: 10.1007/s00414-025-03640-w.

[21] Darmayanti, E.S., & Subiyanto, A.E. (2026). Criminal liability for the sale of civil servant data based on the personal data protection law. *Interdisciplinary Social Studies*, 5(2), 884-894. doi: 10.55324/iss.v5i2.1011.

[22] Data Privacy Framework Program. (n.d.). *Data Privacy Framework (DPF) overview*. Retrieved from https://www.dataprivacyframework.gov/Program-Overview.

[23] Decision of the Constitutional Court of Ukraine No. v002p710-12 "In the Case on the Constitutional Submission of the Zhashkiv District Council of Cherkasy Region on the Official Interpretation of the Provisions of Parts One, Two of Article 32, Parts Two, Three of Article 34 of the Constitution of Ukraine". (2012, January). Retrieved from https://zakon.rada.gov.ua/laws/show/v002p710-12#Text.

[24] Deepanshu, & Kumar, A. (2026). Corporate liability for data breaches under the Digital Personal Data Protection Act, 2023: Legal challenges and regulatory responses. *Vistas: International Journal of Multidisciplinary Studies*, 1(1), 103-121. doi: 10.5281/zenodo.18385783.
[25] DLA Piper GDPR Fines and Data Breach Survey: January 2026. (2026). Retrieved from https://www.dlapiper.com/en/insights/publications/2026/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2026.
[26] Draft Labour Code of Ukraine. (2026, January). Retrieved from https://itd.rada.gov.ua/billinfo/Bills/Card/69516.
[27] Draft Law No. 6177 "On the National Commission for Personal Data Protection and Access to Public Information". (2021, October). Retrieved from https://itd.rada.gov.ua/billinfo/Bills/Card/27996.
[28] European Data Protection Board. (2026). *Report on international data protection enforcement cooperation*. Retrieved from https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/report-international-data-protection_en.
[29] Faccioli, M. (2026). Liability for unlawful personal data processing. In R. Bocchini (Ed.), *Digital platforms-from technical foundations to legal and economic implications: Volume 1* (pp. 745-763). Cham: Springer. doi: 10.1007/978-3-032-07978-7_34.
[30] Faisal, K. (2026). Navigating the fine line: The complex reconciliation of data protection and freedom of expression in criminal conviction and offences data. *Digital Policy, Regulation and Governance*, 28(1), 17-34. doi: 10.1108/DPRG-10-2024-0260.
[31] Federal Commissioner for Data Protection and Freedom of Information. (2025). *Activity report 2024: 33rd activity report on data protection and freedom of information*. Retrieved from https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Taetigkeitsberichte/33TB_24.pdf?__blob=publicationFile&v=2.
[32] Federal Data Protection Act. (2017, June). Retrieved from https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html.
[33] Federal Trade Commission Act. (2006, December). Retrieved from https://www.ftc.gov/sites/default/files/documents/statutes/federal-trade-commission-act/ftc_act_incorporatingus_safe_web_act.pdf.
[34] Gatti, S. (2026). Accountability principle and its implementation in the general data protection regulation. In R. Bocchini (Ed.), *Digital platforms-from technical foundations to legal and economic implications* (pp. 709-729). Cham: Springer. doi: 10.1007/978-3-032-07978-7_32.
[35] Health Insurance Portability and Accountability Act of 1996. (1996, August). Retrieved from https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996.
[36] Hennig, A., Schulte, L., Herbold, S., Kulyk, O., & Mayer, P. (2026). The whos, whats, and whys of issues related to personal data and data protection in open-source projects on GitHub. *Empirical Software Engineering*, 31(1), article number 9. doi: 10.1007/s10664-025-10742-x.
[37] Joshi, U., Baisil, S., Kini B, S., Mehta, M., & Datta, S. (2026). AI ethics in Indian healthcare: A scoping review of national and international guidelines on privacy, data protection, and security. *BMC Medical Ethics*, 27(1), article number 86. doi: 10.1186/s12910-026-01435-1.
[38] Karpyn, D., Leshko, R., Karpyn, A., Leshko, O., Voytovych, K.H., & Hoyvanovych, N. (2026). *Cybersecurity. Protection of personal data, digital devices and access to resources*. Drohobych: Drohobych Ivan Franko State Pedagogical University.
[39] Klymchuk, O.V., & Yaremenko, O.I. (2026). Harmonization of domestic legislation to European standards of cybersecurity and personal data protection: Challenges for public authorities. *Current Issues in Modern Science*, 44(2), 410-423.
[40] Kristanto, A.R., & Slamet, S.R. (2026). Legal liability of financial services institutions for personal data leakage under the Personal Data Protection Act. *Golden Ratio of Data in Summary*, 6(1), 83-90. doi: 10.52970/grdis.v6i1.1981.
[41] Law of Ukraine No. 1089-IX "On Electronic Communications". (2020, December). Retrieved from https://zakon.rada.gov.ua/laws/show/1089-IX#Text.
[42] Law of Ukraine No. 2163-VIII "On the Basic Principles of Cybersecurity in Ukraine". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2163-19#Text.
[43] Law of Ukraine No. 2297-VI "On Personal Data Protection". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text.
[44] Law of Ukraine No. 2657-XII "On Information". (1992, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12#Text.
[45] Law of Ukraine No. 2939-VI "On Access to Public Information". (2011, January). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2939-17#Text.
[46] Law of Ukraine No. 80/94-VR "On Information Protection in Information and Communication Systems". (1994, July). Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
[47] Law of Ukraine No. 851-IV "On Electronic Documents and Electronic Document Management". (2003, May). Retrieved from https://zakon.rada.gov.ua/laws/show/851-15#Text.
[48] New York Privacy Act. (2022, February). Retrieved from https://www.consumerprivacyact.com/new-york-privacy-act/.
[49] Ombudsman of Ukraine. (2014). *Typical procedure for processing personal data*. Retrieved from https://ombudsman.gov.ua/uk/rekomendaciyi-ta-rozyasnennya/tipovij-poryadok-obrobki-personalnih-danih.
[50] Poscher, R., & Orrù, E. (2026). Data protection and privacy: Digitalisation, power, and the transatlantic divide. In *Conceptions of data protection and privacy: Legal and philosophical perspectives* (pp. 1-12). Oxford: Hart Publishing. doi: 10.5040/9781509983759.0005.
[51] Q2 2025 privacy & data protection regulatory enforcement report. (2025). Retrieved from https://compliancehub.wiki/q2-2025-privacy-data-protection-regulatory-enforcement-report.
[52] Qinvi, N.U., Ahmad, R.S., & Wahyunisa, H. (2026). Personal data protection in an artificial intelligence – based photo marketplace on the FotoYu Platform. *Journal of Cyber Law and Technology Regulation*, 1(1), 1-11.

[53] Regulation (EU) No. 2016/679 of the European Parliament and of the Council "On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)". (2016, April). Retrieved from https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

[54] Regulation (EU) No. 2024/1689 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) (Text with EEA Relevance)". (2024. June). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

[55] Resolution of the Verkhovna Rada of Ukraine No. 4065-IX "On Adopting as a Basis the draft Law of Ukraine on Personal Data Protection". (2024, November). Retrieved from https://zakon.rada.gov.ua/laws/show/4065-20#Text.

[56] Şakar, A.Y., & Bağce, D.H.A. (2026). Assessment of the personal data protection board's decision on a data breach committed by an airline company. *Journal of Aviation*, 10(1), 71-76. doi: 10.30518/jav.1770648.

[57] Siddiqui, A. (2026). Data protection and privacy in the digital age: Comparative perspectives on India's digital Personal Data Protection Act and the EU General Data Protection Regulation. *SSRN*. doi: 10.2139/ssrn.6050296.

[58] Singal, S., & Chorev, N. (2026). Free markets, high walls: Data protection and the question of post-neoliberalism. *Socio-Economic Review*, 2026, article number mwaf094. doi: 10.1093/ser/mwaf094.

[59] Singh, P., Kumar, S., Singh, S.K., & Singh, H. (2026). Privacy in mental healthcare by data protection: Exploring AI-powered psychological assessment and identity crisis intervention with legal provisions. In L.R. Janjua, K. Edina & B. Singh (Eds.), *Imposter syndrome and AI: Navigating human identity in the age of intelligent machines* (pp. 327-346). Hershey: IGI Global Scientific Publishing. doi: 10.4018/979-8-3373-6618-0.ch017.

[60] Smith, C., & Hawkins, R. (2026). Arguing conformance with data protection principles. *arXiv*. doi: 10.48550/arXiv.2601.15155.

[61] Strelnyk, V., & Brazhnichenko, I.E. (2022). General theoretycal aspects of legal regulation of personal data protecton in legislation of Ukraine. *Legal Scientific Electronic Journal,* 10, 215-217. doi: 10.32782/2524-0374/2022-10/50.

[62] Suciara, A., Idias, B., Siregar, N.J., Siregar, T.A.F., & Prabowo, T.W. (2026). Strict liability vs fault based: Perbandingan Indonesia dengan Jepang terhadap kebocoran data. *Al-Zayn: Journal of Social Sciences & Law*, 4(1), 739-749.

[63] Surzhynskyi, M. (2025). Challenges and opportunities for adapting Ukrainian legislation to European standards for personal data protection in the field of artificial intelligence. *Law of Ukraine*, 4, 26-37. doi: 10.33498/louu-2025-04-026.

[64] The 2025 privacy & compliance "Fines & Follies" awards: A year of record-breaking enforcement. (2025). Retrieved from https://compliancehub.wiki/the-2025-privacy-compliance-fines-follies-awards-a-year-of-record-breaking-enforcement.

[65] Thomas, L., Gondal, I., Oseni, T., & Firmin, S. (2022). A framework for data privacy and security accountability in data breach communications. *Computers & Security*, 116, article number 102657. doi: 10.1016/j.cose.2022.102657.

[66] Tolson, B. (2026). *Compliance U.S. data privacy laws and regulations in 2026*. Retrieved from https://www.smarsh.com/blog/thought-leadership/data-privacy-laws/.

[67] Understanding data privacy laws: A 2026 compliance guide. (2026). Retrieved from https://www.tekclarion.com/cyber-security/data-privacy-laws-2026/.

Відповідальність суб'єктів господарювання за порушення законодавства про захист даних у процесному управлінні

Микола Сакали
Кандидат юридичних наук, старший викладач
Ізмаїльський державний гуманітарний університет
68601, вул. Репіна, 12, м. Ізмаїл, Україна
https://orcid.org/0009-0007-9263-3962

Анотація. Метою дослідження був комплексний теоретичний аналіз трансформації системи відповідальності суб'єктів господарювання за порушення законодавства про захист персональних даних на етапах їх збирання, зберігання та опрацювання. Методологія базувалась на застосуванні системного підходу та порівняльно-правового методу до нормативних масивів України, Сполучених Штатів Америки та Федеративної Республіки Німеччина. У ході роботи встановлено, що юридична відповідальність бізнесу змістилася від стратегії формального дотримання інструкцій до концепції повної підзвітності, де суб'єкти зобов'язані демонструвати реальну результативність впроваджених алгоритмів захисту. Виявлено, що в українському правовому полі найбільш критичні правопорушення виникають на стадіях отримання згоди, невідповідності мети подальшого використання відомостей та ігнорування обов'язку розмежування ділових і особистих даних у кадрових процесах. З'ясовано, що нехтування письмовою ідентифікацією ролей при залученні розпорядників інформації створює умови для неконтрольованої передачі даних, що призводить до солідарної відповідальності контрагентів. Доведено фундаментальну відмінність між німецькою вертикаллю санкцій, де пріоритетом є технічна цілісність систем, та американською секторною децентралізацією з вираженою каральною спрямованістю правозастосовчої практики. Встановлено, що європейська судова практика допускає відшкодування нематеріальної шкоди у справах про порушення законодавства про захист персональних даних, якщо особа зазнала психологічного дискомфорту або страху неправомірного використання її даних. Визначено, що інституційна фрагментарність в Україні та відсутність автономного наглядового органу знижують рівень правової захищеності процесних операцій порівняно з німецькою моделлю. Обґрунтовано необхідність інтеграції трискладового тесту суспільного інтересу в усі внутрішні регламенти доступу до конфіденційної інформації для уникнення масових правопорушень у комунальному секторі. Практична значимість результатів полягає у можливості їх використання юридичними службами та менеджментом підприємств для впровадження концепції захисту за призначенням і проведення аудитів безпеки з метою мінімізації юридичних ризиків в умовах цифрової трансформації

Ключові слова: персональні відомості; володілець; розпорядник; витоки інформації; інституційна фрагментарність; забезпечення конфіденційності