https://doi.org/10.15407/econlaw.2025.03.064
УДК 342.7

Daria BULGAKOVA, PhD in International Law, Associate professor, Department of Law and Public Administration, Zaporizhzhia Institute of Economics and Information Technologies, Kryvyi Rih, Ukraine
orcid.org/0000-0002-8640-3622

THE PROTECTION OF PERSONAL DATA PROCESSED IN CLOUD SERVICES

Keywords: business-to-government data sharing, data protection, service provider, security protocols, confidential information.

The research on the regulation of cloud services aims to address the issue of cloud technologies law, as well as the issue of the responsibility of business and government agencies for the processing and use of business-to-government (B2G) data in the digital environment.

In particular, the entry into force of the Law of Ukraine "On Cloud Services" on September 16, 2022 and the adoption by the Cabinet of Ministers of Ukraine on February 11, 2025 of the Resolution "Some Issues of the Provision and Use of Cloud Services and/or Data Center Services" significantly affect legal practice, especially those related to the exchange B2G data. These innovations create new legal requirements and obligations that must be taken into account when providing and using cloud services and data center services. In the context of Ukraine's integration into the European legal environment, it is important to consider these issues through the prism of European Union law, such as the GDPR.

This paper analyzes the Azure (2021) and FisconetPlus (2020) cases to highlight key data protection challenges in public sector cloud adoption. It reveals issues such as a lack of transparency, excessive data processing, insufficient safeguards, and unclear responsibilities between authorities and cloud providers. The cases underscore the importance of applying GDPR principles like data minimization and privacy by design at all stages, including testing. Lessons from these cases inform recommendations for secure and compliant cloud implementation in Ukraine's public administration.

Given that many enterprises and government agencies are now actively implementing cloud services, law practitioners must be prepared to provide legal assistance in matters of data protection, compliance with regulatory requirements, and safeguards of clients' rights and interests in the context of new technological challenges. Thus, the proposed outcome of the research is necessary for professionals so that they can effectively respond to legal challenges arising in the process of integrating new technologies within the framework of national and European legislation, and provide proper legal support to businesses and government agencies working with cloud technologies.

Introduction. It is believed that the public sector could execute a more secure and efficient digitalization by using cloud services.[1] It is tempting for the public sector to use cloud services because, among other things, the services can lead to more efficient information oversight at a reasonable

[1] **A cloud service consists of** a service model and a delivery model. These models can be integrated in different ways depending on the desired division of responsibility between the cloud service user and the provider. To adapt a cloud service to a user, the services can be separated into three different service models. These are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Servi-

Цитування: Bulgakova D. The protection of personal data processed in cloud services. *Економіка та право.* 2025. № 3. С. 64—76. https://doi.org/10.15407/econlaw.2025.03.064

cost.[2] When it comes to the public sector's use of cloud service providers, there are many aspects to consider, including data transfer. Thus, the research focuses on one of the legal problems, namely, transferring confidential data to a cloud service provider. It is worth emphasizing at the outset that the public sector's use of cloud services is not a simple subject to understand, as the area requires some knowledge of both law and technology. When an authority uses a cloud service, the confidentiality issue is, among other things, whether and how it is possible to transfer sensitive information to the cloud service without disclosure to the cloud service provider in violation of confidentiality legislation. That said, there is reason to clarify the meaning of the term disclosure.

Methods. Among methods are law libraries, regulatory research on GDPR [5], and Ukrainian law on data and cloud processing matters, also notable rulings such as the Norwegian DPA vs NIF of 2021 [6; 7] and the FisconetPlus decision in Belgium of 2020 [8; 9] demonstrate the real-world implications

ce (IaaS). The main difference between the service models is that they offer the user different degrees of control over the cloud service.

A delivery norm depicts how the cloud service is to be made open, and there are four different models. The choice of delivery model can be of importance for the success of the public sector's use of cloud services.

Private cloud services are given to an individual user. The infrastructure is both administered and supplied by the user or by an external party on behalf of the user. The disadvantage of private clouds is that it is costly for the user to maintain the necessary expertise. To establish a more holistic approach and fill regulatory gaps, private actors may need to develop standards that cover aspects other than mere safety [1, p. 84].

Public cloud services are the most common delivery model. The cloud service provider of public cloud services then makes resources such as storage or programs available to the public over the internet. The fact that the service is delivered via the Internet means that the cloud service provider and its computing resources take an external position towards the user. This differs significantly from private cloud services, which instead have an internally simulated resource set with the user.

Shared cloud services or partner cloud services are similar to public services but offer cloud services across organizational boundaries. Several organizations then come together and create a cloud service. This assumes that there are common interests among the organizations, such as similar goals or requirements regarding certification. Digital certificates are distributed in such a way that they can be associated with the servers at the original and the destination sites that are participating in the transfer of information [2, p. 123]. The subsequent processes can be implemented in a technically satisfactory and logically acceptable way via the public key infrastructure (PKI) [ibid]. Besides, each level of certification has an associated compliance mark, which the organisation must use in relevant customer-facing documentation, accompanied by the verification ID assigned to the service by the monitoring body [3]. The cloud service in this scenario can either be operated by the organizations themselves or by an external party. On the other side, there is no stable cybersecurity model since even a high level of cybersecurity certification cannot guarantee that the sharing process is entirely secure [4, p. 28].

Finally, there are **hybrids**, which are combinations of two or all of the above delivery models. When different delivery models are combined, each cloud service nevertheless continues to be a separate entity. What happens is that the delivery models are tied together through technology that opens up the possibility of transferring data or computer programs between the cloud services. For example, the organization may choose to manage some tasks in a private cloud service and some tasks in a public service. The hybrid prototype thus benefits from the various advantages of the other models.

[2] For a better understanding of the subject, the **characteristics of the cloud service** are proposed. The first characteristic is that the cloud service is available on demand through self-service. The cloud service user can choose to activate or deactivate the cloud service and make available the exact desired amount of computing resources without direct personal interaction with the cloud service provider. The limited contact with the cloud service provider means that the possibilities for contractual negotiation for the cloud service are limited.

The second element is that the cloud service has expansive availability through networks. The service should be available through a large network, such as the Internet. In spare, the service is accessed through standardized agencies that glorify the use of different platforms by the user, such as mobile phones, tablets, and laptops.

The third characteristic is that the cloud service provider consolidates resources such as storage, processing, and memory. By pooling computing resources, the cloud service provider can serve multiple users simultaneously and redistribute the physical and virtual resources dynamically depending on user demand. The user is normally unaware of the system's infrastructure, but the cloud service appears as a single system. From a purely technical perspective, the user does not need to know where the servers are located or how many there are. However, this uncertainty can cause problems from a legal perspective with requirements from data protection regulations and the like.

The fourth trait is that the cloud service has an immediate elasticity that depends on the exact use. The capacity of the cloud service can be provided and released according to the current use, in some cases even automatically. From a user's stance, the change occurs largely imperceptibly, and the available capacity often appears unlimited and can be allocated in the desired amount at any time.

of inadequate data protection measures. Both decisions stress insufficient testing and lack of data diminishment and risk assessment as core failures under the General Data Protection Regulation (GDPR) [5] obligations (Articles 5, 6, 25, 32, 35). Thus, case law illustrates GDPR [5] enforcement for the best protection of personal data in cloud services.

Analysis of the latest research. Most studies offer an encyclopedic look at the contractual arrangements between cloud service providers and their customers for the best data sharing traditions. It provides guidelines emphasizing issues like data protection, service continuity, and compliance with privacy laws. Recent scholarship and regulatory developments underscore the critical need for robust personal data governance and user-centric safeguards in digital environments. Likewise, Calder [3] provides practical insights into the EU Code of Conduct for Cloud Service Providers, accentuating the matter of contractual obligations, transparency, and accountability to align with GDPR [5]. This is especially pertinent as cloud adoption grows across both public and private sectors. Therefore, the main focus of the author is cloud compliance and data control.

Cloud service legal frameworks, as well as Millard's [10] edited volume on cloud computing law, explore how standardized contractual models can be adapted to promote better legal certainty and protection for data subjects in cross-border cloud services.

Johan David Michels, Christopher Millard, and Felicity Turton [11] analyze the use of standard contracts in cloud services. They highlight the imbalance in bargaining power between cloud providers and users, noting that providers often impose non-negotiable terms. The authors confer key contractual issues such as service levels, liability, data protection, and jurisdiction. They argue for greater transparency and fairness, especially for SMEs and public sector users, and emphasize the need for regulatory and market-driven gains to standard terms in cloud contracts. The analysis by Michels, Millard, and Turton on definitive contracts for cloud services is particularly proper in light of Ukraine's evolving legal landscape.

Georgiopoulou et al. [12] suggest a set of technical and organizational measures specifically tailored to cloud providers. These include encryption, anonymization, and continuous risk assessment strategies that are indispensable for maintaining GDPR [5] obedience and data integrity. Therefore, the work focuses on technical safeguards for GDPR [5] compliance.

Authors Fosch-Villaronga & Millard [1] critique the blurred legal lines in cloud robotics, suggesting that future regulation must address machine autonomy and user consent more clearly to avoid systemic vulnerabilities.

The Laws of Ukraine on personal data protection and cloud services perform as an important regional framework. However, harmonization with EU standards remains essential, especially in transborder data flows and public-private data sharing models under the conclusion of the work by Bulgakova & Stupnik [4].

The public sector's increasing reliance on cloud services for managing sensitive and confidential data introduces legal, ethical, and technological challenges. Among them risk of unauthorized access, disclosure, and processing of personal and confidential information, especially when stored across borders; lack of clarity and consistency in how data protection obligations (Articles 5, 6, 25, 32, and 35 GDPR) are implemented in practice; insufficient technical safeguards in cloud environments, particularly during development, testing, and migration phases; ambiguity in Ukrainian legislation where only limited legal norms (Articles 13–14 of the Law "On Cloud Services") refer to data protection, relying largely on cross-references to the Law "On Personal Data Protection". The challenge of ensuring user agency, transparency, and data sovereignty in cloud ecosystems governed by both national and foreign laws hasn't been explored recently, and this article gonna focus on it, particularly with respect to public sector adoption of cloud services and data sovereignty.

Statement of the problem. The public sector's use of cloud services for the information regime may lead to confidential data being transferred to the cloud service. Consequently, confidential data may be made available to the cloud service provider. At this stage, the cloud service providers should pass to the business cycle modeling engine all the events as a log file [13, p. 219]. Study focuses on an important and growing concern regarding the public sector's use of cloud services, especially when it comes to managing confidential data.

The Azure case [6; 7] and the FisconetPlus case [8; 9] highlight critical challenges in ensuring compliance with data protection regulations when public authorities migrate to cloud-based services. Both cases reveal issues related to the inadequate enactment of data confidentiality measures, insufficient transparency about personal data processing, lack

of proper risk assessment, and unclear delineation of responsibilities between public entities and cloud service providers: mandatory authentication requirements, improper handling of personal data including the use of real instead of anonymized data in testing climates and insufficient consent mechanisms have exposed sensitive data to unauthorized access. These problems underscore the difficulty of offsetting digital modernization and cloud adoption with strict adherence to data preservation principles such as data minimization, privacy by design, and accountability. The cases indicate a pressing need for clearer legal frameworks, robust operational procedures, and stronger technical security to protect individuals' rights and guarantee public trust in cloud service enactments within the public sector.

The adoption of the Law "On Cloud Services" No. 2075-IX [14] and the Cabinet of Ministers' Resolution No. 154 of 11 February 2025 [15] marks a turning point in cloud governance. These instruments now permit state authorities to store registers and sensitive data abroad, a shift necessitated by wartime conditions. However, the rapid regulatory changes pose challenges echoed in the article: a lack of negotiated, fair standard contracts, especially in the public sector, where newly approved model agreements must now align with security, interoperability, and compliance needs. The Ukrainian practical implementation of proposed updates is in the urgency of addressing the contractual imbalance and legal uncertainties identified by the authors, particularly in cross-border and high-risk contexts.

Research results. The Law "On Cloud Services" that came into force on 17th of February 2022, No. 2075-IX [14] allowed the transfer of registers abroad and the storage of data in the cloud. The next step forward for the cloud service regulation was remarkable when the Cabinet of Ministers of Ukraine on 11th of February 2025 acquiesced the rules for the use of cloud services by state controls in its resolution "Some issues of the provision and use of cloud services and/or data center services" No. 154 [15] initially proposed by the Ministry of Digital Affairs on the regulation of cloud services in state institutions. The taught rules primarily interest the permission to transfer registers abroad and store data in the cloud. From now on, state authorities will be able to leave them in data centers abroad and not transfer them to Ukraine after the end of hostilities. It also assented the system for the requirement of cloud services and/or data center services related to the processing of state information resources or information with limited access, requirements for providers of cloud services and/or data center services, procedure for the figure and use of electronic catalogs of cloud services and/or data center services, model deal on the need of cloud services and/or data center services to a public user of cloud services and a critical infrastructure operator regarding a critical information infrastructure facility. It is designed to sustain a cybersecurity plan and the effect of a national cloud model.

The situation materializes where the cloud service provider is subject to foreign legislation that may require the disclosure of information from the provider to a foreign government. The explanation is the chance that encryption of a certain strength could potentially prevent classified details from being divulged to the cloud service provider, which would enable cloud service use by the public sector.

The delay regarding the privacy decree has led to authorities handling the outsourcing of confidential information to private cloud service providers in widely different ways. Some are refraining from using external providers for information management for the time being. Others are running confidential transmission through manual routines and have other information handled digitally by a provider. Some authorities interpret the privacy legislation in a way that opens up the use of cloud services. However, there is generally a reluctance among authorities to engage cloud service providers to handle confidential information unless it is clear that the introduced law does not prevent such use. At the same time, it is not appropriate for transfers where the report in question is not covered by an applicable confidentiality provision. Information that is not cocooned by pertinent confidentiality requirements can never be encircled by confidentiality.

However, authorities handle confidential information to a large extent. If an authority chooses to use a cloud service, confidential information may consequently be transferred to the service. It follows that confidential information may be made available to a cloud service provider.

Case study on the Azure Cloud Services. Documents cannot be subject to secrecy, but data in documents can be. In this context, it is critical to point out that the data perception regulation always applies. In this regard, it is proposed to view the case study on the Azure Cloud Services [6; 7]. The Norwegian Sports Federation and the Olympic and Paralympic Committees (NIF) decided to transition from local IT infrastructure to Microsoft Azure

cloud services. On December 20, 2019, the Norwegian Data Protection Authority (Datatilsynet) received a non-conformance report from NIF. The report stated that on December 18, 2019, NIF received a request from the National Cyber Security Centre of Norway (NCSC-NO) regarding a data leak affecting athletes' information through a specific publicly accessible IP address. It is calculated that around 3.2 million individuals were affected, including 486,447 minors aged 3 to 17. This was discovered during a routine scan of Irish IP addresses conducted by the Irish National Cyber Security Centre (CSIRT-IE), which reported the finding to NCSC-NO, which in turn informed NIF. NIF found that the access had been open for 87 days and immediately took action to shut it down.

The issue arose during the transition of resources from a local solution to Azure and was linked to the testing of a cloud service called Elasticsearch. Elasticsearch was used in testing a potential solution for third-party membership system providers in Norwegian sports, allowing identity verification against the central sports database. During testing of this new Elasticsearch service aimed at improving participant management, NIF used actual personal data instead of anonymized or limited datasets. At the same time, Elasticsearch formed a product called Kibana, which operated on an IP port that was not open within NIF's network but was accessible via the internet.

Due to the need for up-to-date personal information and the limited time to test the solution, a decision was made based on the assessments at the time to use real data from the central sports database. This ensured the integrity of the information and maintained a realistic test scenario.

At the time, there were no established operational procedures or technical security measures for the new cloud environment, as it was still under development. Because of the lack of an authentication mechanism in the software and an error that led to the use of a publicly available IP address, the Elasticsearch and Kibana services became openly accessible. It's worth noting that while Elasticsearch did not initially allow bulk data downloads, it permitted individual searches. Kibana also allowed fuzzy (broad) search capabilities.

Besides, these services were not indexed for open access, so one had to know the IP address or execute a more targeted query. This is why the organization was unaware that confidential facts remained publicly attainable. Once the issue was discovered, the services were disabled, and NIF switched to another service. However, the question of whether the data disseminated in the test environment should be deleted remained unresolved.

The categories of personal data revealed included: name, date of birth, gender, address, email, phone number, and club affiliation. At the same time, individuals with strictly confidential or unassailable homilies were not part of the data breach. Although NIF had no reason to accept that anyone other than the Irish and Norwegian security agencies accessed the data, Elasticsearch and Kibana did not induce access logs (as only a trace version was used), making it impossible to fully rule out a data breach. Therefore, NIF deems it far-fetched that anything other than these instruments processed the data. NIF also emphasized that the test environment where the data leak occurred was never intended for use in the cloud and was therefore not covered by a security assessment.

NIF acknowledged that its risk assessment was flawed and that the central sports database had been pulled into a cache without implementing safeguards such as using de-identified data or restricting the dataset. As a result, NIF failed to consider the option of using anonymized data and did not implement adequate security measures during testing.

This highlights a significant lapse in data security during the testing phase of a cloud-based service. The key mistakes made by NIF were:

(1) instead of using anonymized data or a subset of the data, NIF exposed sensitive information, which could have been avoided;

(2) there was no comprehensive risk evaluation before using live data in a testing environment, which is critical to safeguarding personal information;

(3) proper security protocols were not in place to ensure data was protected during the test phase, leading to the breach;

(4) limited data could have been used, significantly reducing the risk of exposing personal information.

To address the data leak, Orange Cyberdefense was engaged to investigate whether personal data had been misapplied for criminal goals. The investigation had its limitations, focusing only on personal information that was accessible online. The Orange Cyberdefense report pointed out that various tools exist for tracking database leaks, including cases involving Azure (Elasticsearch and Kibana). However, this does not mean that all disclosed databases are found and exploited. Furthermore, a leaked data-

base can be accessed without any malicious intent (no clear evidence of criminal activity was found).

Following the incident, NIF began reviewing and improving its operational procedures and implemented new security protocols. It strengthened the requirements for risk assessments and their documentation. The case also highlighted the need to improve procedures for handling test data, prompting NIF to rely more heavily on synthetic test data. NIF noted that it was difficult to change long-standing local solutions, particularly due to the significant amount of business logic embedded in the database.

Datatilsynet issued a preliminary notice (under Section 16 of the Public Administration Act) of its intention to impose the following decision: under Article 58(2)(i) of the GDPR [5], the Norwegian Sports Confederation and the Olympic and Paralympic Committee would be fined for transgressing Articles 5(1) (a, c, f), 6, and 32 of the GDPR [5], for EUR 250,000. While NIF did not dispute the description of the event provided by the Data Protection Authority, it did object to the amount of the fine. After reconsidering new information regarding NIF's community and finances, the Data Protection Authority decided to reduce the fine to EUR 125,000. To coordinate with the abovementioned, cloud providers must harbor full documentation of biased data kept, where it came from, and with whom they are shared, including the rationale for processing [12, p. 667]. NIF is also instructed to conduct thorough testing of a large importance of participant data from sports crews in all Norwegian municipalities and cities.

The lesson for the Ukrainian data protection law under the case study on the Azure Cloud Service. According to Article 13 of the Law of Ukraine "On Cloud Services" [14], the protection of personal data when using cloud computing technology for their processing and providing cloud services and/or data center services is carried out per the requirements of the Law of Ukraine "On Protection of Personal Data" [16]. Article 14 also establishes that the provider of cloud services and/or data center services ensures and creates appropriate conditions for data protection in the cloud computing system in the manner named by the legislation of Ukraine and the pact between the parties. At the request of the user of cloud services and/or in the manner stipulated by the agreement, the provider of cloud services and/or data center services provides information on the protection of information in the cloud computing system from internal and external threats, including cyberattacks. These are the only two articles that are devoted to data protection and, as it seems, have a reference norm to another law.

Following Article 5 of the Law of Ukraine "On Personal Data Protection" [16], personal data may be classified as confidential information about a person by law or by the relevant person. Personal data relating to the exercise by a person authorized to perform state or local self-government functions, official or service powers, is not confidential information. Article 6 also stipulates that the processing of data about an individual that constitutes confidential information shall not be permitted without his or her consent, except in cases specified by law, and only in the interests of national security, economic well-being, and human rights.

The information that is to be kept secret by a confidentiality provision is called the subject of confidentiality. The starting point is not to achieve more confidentiality than is necessary to protect the subject of the confidentiality provision. In order to limit the scope of confidentiality to an appropriate limit, most confidentiality provisions include what is called a damage requirement. Confidentiality thus has a legal definition, but the concept of disclosure is not defined in law. To understand the definition of confidentiality, the meaning of disclosure must therefore be ascertained. Furthermore, it is useful to be aware of two additional concepts defined, namely, classified information and information subject to confidentiality. Classified information refers to information for which there is a provision on confidentiality. For information that is classified, however, confidentiality applies in the individual case.

The case study on Fisconetplus. It is a proposed case study on FisconetPlus, when the Federal Public Service (FPS) Finance of Belgium did not successfully apply FisconetPlus in its operations [8; 9].

In 2018, as part of digital modernization, FisconetPlus was moved to the SharePoint cloud environment. Access to the cloud repository was free, but the changes introduced required users to log in to the portal via a Microsoft user account. This shift was reanalyzed by Belgium's Data Protection Authority (DPA) following a series of fusses. The study has shown that FPS Finance offers access to FisconetPlus in a way that does not require a Microsoft user account (anonymous or not), specifically through the basic search system. Therefore, even if users have a choice between an option with fewer functionalities (where personal data is either not processed or processed to a minimal extent)

and a more user-friendly option (which involves the collection and processing of personal data), this does not mean that the more convenient option necessarily offers a lower level of protection in accordance with GDPR [5].

The mere fact that access to information is possible without a Microsoft account does not rule out the possibility that authentication via a third-party service provider could violate Article 6 of the GDPR [5], as there are no warrants that the personal data processing of the data subjects is done properly.

As such, FPS Finance did not offer the most privacy-friendly choice (direct access without authentication) in a clear and default manner. This constitutes a violation of Article 25 of the GDPR [5] regarding privacy by design and by default data protection.

Furthermore, there are clear data flows to and from Microsoft. FPS Finance did not sufficiently inform potential data subjects about how their personal data would be used by Microsoft. The fact that access could be made via an anonymous Microsoft account also proves, by its nature, that allowing access through a new or existing Microsoft account involves the processing of more personal data than strictly necessary under Article 5(1)(c) of the GDPR [5].

Therefore, FPS Finance did not relent with the data minimization code. It is influential to note that no authentication agents or identification requirements, whether controlled by the government or other entities, should be mandatory for accessing public information that is intended to be made available to the public. Furthermore, personalized services, such as saving favored sources or automatic notifications, should not require systematic unique identification of users. Thus, the proportionality principle is also violated in this case.

Given the conceivable risks to data subjects' rights and freedoms, particularly regarding the security of the cloud platform, FPS Finance should have conducted a data protection impact assessment (DPIA) before implementing this system.

In order to create an account, users must accept Microsoft's privacy policy and cookie settings, which by default trigger certain tracking and advertising features. Using a Microsoft account involves placing non-essential cookies without obtaining reasonable clearance, as the cookie banner on the website contained consent through "further browsing." It indicated that by continuing to browse, users agreed to the use of cookies. However, there should be a report or vibrant actions by the user to provide free, specific, clear, and unambiguous consent under GDPR [5].

Therefore, given the combination of the "further browsing" course and cookie policy, there is a mismatch between the cookies listed in the cookie policy and the cookies packed upon opening the website. This mismatch constitutes a violation of the GDPR's [5] transparency principle, which requires that users be notified about the scope and nature of data processing and provide informed consent. If the cookies loaded are not listed in the policy, it may indicate hidden data processing, violating users' rights and the principles of lawful data processing.

In February 2019, the DPA's appraisal service determined that the modernization updates were a breach of the GDPR [5]. It was selected that there was no lawful basis for FPS Finance to force citizens to assign their data to a private establishment as a prerequisite for accessing public sector information.

As a result, the Belgian DPA ruled that disclosing personal data cannot be a condition for accessing public information.

In June 2020, the DPA's inspection benefit allocated a temporary measure, the first of its kind in data protection history, ordering FPS Finance to temporarily discontinue FisconetPlus, including the permit to the repository via the Microsoft SharePoint portal.

Subsequently, FPS Finance deactivated access to its FisconetPlus portal via Microsoft accounts, though access remained available through other means. FPS Finance decided to resolve the dispute by re-releasing FisconetPlus and transitioning from Microsoft tools to a platform developed in-house and fully hosted on its infrastructure. However, due to budget and human resource constraints, temporary solutions were implemented, including simple chats through MyMinfin without authentication and consultations via the creation of an anonymous Microsoft user account.

The case was also under review by the DPA's judicial chamber, which, in its decision of December 23, 2020, confirmed the next GDPR violation: (1) FPS Finance did offer an alternative method of accessing FisconetPlus without requiring authorization via a basic search system. Thus, users could choose between a minimal personal data processing option and a more serviceable rendition that involved data collection. However, this choice between options was neither obvious nor set by default, which constitutes a violation of Article 25 of the GDPR "data protection by design and by de-

fault"; (2) there were violations of the principles of personal data processing, particularly due to insufficient information provided. FPS Finance failed to explain to users clearly how Microsoft processes their data. There was also an infringement of the principle of data minimization under Article 5(1)(c) of the GDPR, since even the use of an anonymous Microsoft account involved processing more personal data than necessary. Mandatory authentication for accessing publicly available information violates the principle of proportionality, as personalized functions (such as saving sources or receiving notifications) should not require user identification; (3) topics with cookies and consent were identified. The inspection report showed that Microsoft places up to 54 cookies on the end user's widget, including non-essential cookies. This is particularly the case when authenticating with a Microsoft account, whether anonymous or regular. Notably, cookies such as ANON and NAP are used to collect additional information about users and were subject to a separate technical analysis during the investigation.

Also, when devising an account, users were required to accept Microsoft's privacy policy and cookie policy, which by default included marketing trackers. The use of a banner with the wording "further browsing means consent" does not meet the GDPR requirements for valid authorization, which must be informed, specific, unambiguous, and freely given. Therefore, the mismatch between the cookies itemized in the policy and those loaded signifies hidden data processing, which constitutes a violation of the principle of transparency.

In December 2020, the DPA's Litigation Chamber ratified the violations and issued an official warning to FPS Finance.

The measures taken by FPS Finance following the proceedings involved deactivating access via Microsoft accounts, while retaining alternative access approaches. It was also decided to develop an internal platform that would not rely on external providers. Due to budget and staffing constraints, temporary access solutions were used through MyMinfin without authentication or via an anonymous Microsoft account.

The Litigation Chamber of the Belgian Data Protection Authority concluded that requiring mandatory authentication via a Microsoft account to access FisconetPlus posed a high risk to the rights and freedoms of individuals, falling under the scope of Article 35 of the GDPR. In support of this conclusion, the Inspection Service pointed to several risk-enhancing factors:

1. The FisconetPlus platform is hosted in the federal G-Cloud, which operates on Microsoft technologies;

2. The domain *gcloudbelgium.sharepoint.com* is registered to Microsoft Corporation;

3. The infrastructure is based on a hybrid cloud controlled by a third party located outside the EU, adding risks related to jurisdiction and data transfers.

Therefore, the Inspection Service emphasized the lack of additional technical safeguards from FPS Finance, such as the application of international standards, which are instructed when working with cloud technologies.

The lesson for the Ukrainian data protection law under the case study on FisconetPlus. The FisconetPlus case supplies influential insights for Ukraine, especially as it moves toward broader integration of cloud services in public administration and critical infrastructure. The case shows that confidentiality is twofold: (1) confidentiality of actions, confirming technical safeguards and secure environments, and (2) the duty of confidentiality, which is a legal obligation that may arise from national laws on cloud services or personal data protection, as well as contractual commitments.

In Ukraine, the Model Agreement on Cloud Services [15] incorporates such a duty for cloud service providers and data center operators. However, FisconetPlus teaches that such duties must be strictly enforceable, especially where contractors perform roles akin to public authorities. A duty of confidentiality can follow from both "On cloud services" [14] and "On personal data protection" [16]. There are principally two types of burden of confidentiality. The first is the sanctioned duty of confidentiality described above. The latter duty of confidentiality can be imposed through like-mindedness. Accordingly, a model agreement on the provision of cloud services and/or data center services to a public user of cloud services and a critical infrastructure operator regarding a critical information infrastructure facility, endorsed by the resolution of the Cabinet of Ministers of Ukraine of February 11, 2025.

Contractors of such a congruence are covered by confidentiality to the extent that they are considered to have such a connection to the authority that the contractor is considered to experience in the authority's activities. What the authority's actual activities are is stated in the authority's instructions or sub-agreement. If it is stated in regu-

lations that a contractor shall hold a certain class, it heeds that confidentiality shrouds the contractor. Otherwise, it is mandated that the task that falls to the contractor is otherwise handled by a civil servant or that it is reasonable that such a civil servant could have that task. A person who is employed by a private service provider is generally not covered by the provisions, but there are exceptions. The oddities are circumstances where the employee is placed at the disposal of the authority and participates in the activities in a manner that can be compared to an assignment situation. If the employee is not covered by the confidentiality provisions, any inconveniences can usually be resolved, for example, with an agreement between the company and the employee on confidentiality.

Regarding the inclusion of persons on "other similar grounds," this may be the case where the authority has granted an individual staffing company to facilitate work accumulation or staff shortages in the authority's activities. The employees of the individual players can then be said to have been recalled at the disposal of the authority in a manner that corresponds to a direct assignment agreement between the authority and the employee. Under such circumstances, for example, the staffing company's employees are included in the authority's operations, similar to "on other similar grounds," and are thus encircled by the definition. For example, a trader might sign up for a cloud storage service like Dropbox to meet an immediate need to share files with a business partner, but also with a view to using the service to share photographs with friends and family [10, p. 221]. It may not become clear for some months how that individual will use the service [ibid.]. If the test to be applied is the individual's purpose at the time of signing up, and that intent was never properly considered, it is not only hard but extremely artificial to attempt to apply the test [ibid.]. Of course, the individual's purpose might be deduced from the nature of the service and how it was subsequently used [ibid.].

Under EU law, for example, article 3 of the Rome I Regulation [17], a contract shall be governed by the law chosen by the parties. The choice shall be made expressly or revealed by the terms of the contract or the circumstances of the case. To achieve this, a user shall provide a set of private data the access to which is only allowed to the user or only he knows about it [18, p. 10]. Besides, by their choice, the parties can select the law applicable to the whole or part only of the contract. The fact that there are borderline cases regarding persons who are not covered by the law of another country, but where there is nevertheless an interest in maintaining secrecy, does not justify a general rule of secrecy according to the legislator. The article of the mentioned Regulation also states that where all other elements relevant to the situation at the time of the choice are located in a country other than the country whose law has been chosen, the choice of the parties shall not prejudice the application of provisions of the law of that other country which cannot be derogated from by agreement [17]. Hence, other needs for confidentiality were to be satisfied in another law or through agreement structures such as confidentiality agreements that depend on who confidentiality applies to. The main rule is that information that is classified may not be disclosed to individuals or to other authorities. However, the choice of law in business-to-consumer ('B2C') contracts cannot deprive consumers of the protection afforded them under laws that cannot be derogated from by agreement under the consumer's local law [11].

Under the stipulation 7 of the approved by the resolution of the Cabinet of Ministers of Ukraine of February 11, 2025 Procedure, data from the user to the provider may be transferred using physical media or electronic communication networks, means of cryptographic information protection in compliance with the requirements for integrity, confidentiality and availability of tip established by legislation in the areas of information protection in information, electronic communication and information-communication systems and cybersecurity. The methodology and grounds for the transfer of electronic information resources from one provider to another are provided for in the contract. In all cases, such transfer must be carried out in compliance with the requirements for integrity, confidentiality, and availability of information established by legislation in the areas of information protection in information, electronic communication, and information-communication systems and cybersecurity. The provider must also demonstrate internal audits at least once a year to affirm adherence to the internal stakeholder control system under these conditions.

Therefore, a core GDPR [5] concern in the case was the use of Microsoft infrastructure located outside the EU, without satisfactory safeguards. This created risks of unauthorized access, cross-border data transfer topics, and fixed governance by the na-

tional authority. Ukraine should draw from this by prioritizing sovereign cloud plans, ensuring jurisdictional control over data, levying rigid localization powers, or adopting EU-standard contractual precautions.

Conclusions. Thus, the research shows a clear trend toward integrating robust data protection frameworks like the GDPR [5] into national laws such as Ukraine's Personal Data Protection Law [12] and the Law on Cloud Services [14]. The European Data Act [19] and case law, such as the Azure Cloud Service and FisconetPlus cases, demonstrate the growing importance of ensuring that cloud services comply with strict data protection regulations, maintain transparency, and secure data sovereignty. Ukrainian enterprises and cloud providers will need to ensure compliance with both Ukrainian and EU regulations to avoid legal repercussions, especially in cross-border data transfer scenarios.

The idea is that knowledge should not be broadcast further than it is essential. Where data cannot be shared or centralized, model-to-data can still theoretically boost a virtual form of data aggregation through a federated data system (ie, distributed data system) [20, p. 4]. A federated data system is composed of a network of autonomous data repositories or nodes that share a common data structure /schema and governance principles, but the data remains localized [ibid.]. The appraisal of the authority and branch of shifting is meant to be made on a case-by-case basis, for example, based on managerial division and function. With regard to the critical issues related to cloud services, under EU law, the Data Act [19] provides for a strengthened right to portability of cloud computing services, facilitating consumers in switching from one cloud data processing service provider to another, preventing vendor lock-in [21, p. 148].

As follows, the research assesses that a cloud service provider is not covered by the secrecy circle. This is partly because the provider does not have an assignment that otherwise dips to an employee of the authority, and partly because its employees cannot be considered to participate in the authority's activities on other similar grounds. Since a cloud service provider is not covered by the secrecy circle, various secrecy considerations arise when authorities use cloud services.

In combination with the typical risk of damage that exists with the data, there should be sufficient information to make it possible to make a decision on the disclosure.

Taking into consideration the case studies, the research came to the heeding:

1) Azure Cloud Service Case (Norway) highlights the implications of inadequate testing and adherence to GDPR. Cloud service providers must ensure that data handling practices align with GDPR's principles, especially regarding data security and transparency. The Norwegian Data Protection Authority's decision underscores the essence of proactive obedience and regular audits for cloud services operating in multiple jurisdictions, including Ukraine.

2) FisconetPlus (Belgium) examined GDPR violations concerning data protection assessments. It underscores the necessity for cloud providers to conduct Data Protection Impact Assessments (DPIAs) when supervising sensitive personal data. Ukrainian cloud service providers must similarly cling to DPIA requirements if they are processing personal data in line with both Ukrainian and EU laws.

Therefore, it is recommended that Ukrainian companies adopt best practices from this outcome, which could enhance the contract draft and help mitigate legal risks.

Recommendations. There is a need for more in-depth studies on how jurisdictional laws intersect with public sector cloud data, especially as national laws vary regarding data protection, law enforcement access, and foreign surveillance laws. The further examination should also explore how cross-border data transfers can be effectively governed in the context of public sector services. Hence, a more meticulous framework for understanding the legal terrain of cloud data in international contexts, particularly for government use, is essential. This could include an analysis of existing tools like the EU-U.S. Privacy Shield or Standard Contractual Clauses and their effectiveness in ensuring compliance with data sovereignty.

The examined case on the Azure cloud Services highlights the necessity of complying with the GDPR at all stages, including testing. It is recommended to pay attention to the following areas of control when handling personal data in cloud environments [6; 7]: (1) using real data instead of anonymized or limited datasets increases the risk of confidential information leakage; (2) a comprehensive risk assessment must be conducted before the use of personal data, even in a test environment; (3) failure to implement basic cybersecurity measures renders data helpless to conceivable unauthorized access; (4) when processing personal data in the tes-

ting mode of a cloud service, it is advisable to use partial, masked, substituted, or synthetic data.

The ensuing offers are proposed to ensure compliance with the principles of transparency, data minimization, proportionality, and data protection by default based on the case-study on FisconetPlus [8, 9]: (1) when implementing cloud technologies and conducting national data protection impact assessments (DPIAs) in the context of cloud solutions, it is essential to consult the updated ISO/IEC 22123 standards in the field of cloud computing; (2) a DPIA should be piloted even for temporary technical solutions, as well as for final permit models planned for enactment. The absence of such an assessment constitutes a violation of Article 35 of the GDPR; (3) the status of joint controllership with the service provider should be regulated in the context of cookie sequence and the processing of personal data during authentication. The existence of joint responsibility requires transparent delineation of roles and obligations per Articles 5 and 26 of the GDPR; (4) compliance of the cookie banner with the principles of translucence and informed consent under Article 7 of the GDPR can be achieved by distinguishing between essential and non-essential cookies, and by avoiding consent instruments via "additional viewing pages" that penalize access to the service; (5) the creation of new infrastructure must incorporate the principles of privacy by design and by default. During the transition to an internally developed platform, it is advisable to take into account Article 25 of the GDPR, which demands underrating data processing, sidestepping excessive authentication, and confirming anonymous or pseudonymized credentials to public communication.

REFERENCES

1. Fosch-Villaronga E., Millard C. Cloud robotics law and regulation. *Robotics and Autonomous Systems*. 2019. Vol. 119. P. 77-91. https://doi.org/10.1016/j.robot.2019.06.003
2. Sharma P., Sharma M., Elhoseny M. (Eds.). Applications of cloud computing: approaches and practices. 1st Ed. New York: Chapman & Hall/CRC, 2021. https://doi.org/10.1201/9781003025696
3. Calder A. EU Code of Conduct for Cloud Service Providers — A compliance guide. IT Governance Publishing, 2021. 54 p.
4. Bulgakova D., Stupnik V. The Sharing of Business-to-Government Data. *Administratyvne pravo i protses*. 2023. No. 2 (41). P. 18-37. https://doi.org/10.17721/2227-796X.2023.2.02
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). *Official Journal of the European Union*. 4.5.2016. L 119. P. 88-1. URL: http://data.europa.eu/eli/reg/2016/679/oj
6. Bulhakova D. Sprava DATATILSYNET pro vytik personalnykh danykh u norvezkii sportyvnii federatsii pry testuvanni khmarnoho servisu AZURE. *Sotsialna spravedlyvist ta tsyfrova ekonomika. 2025*: Mizhnarodna nauk.-prakt. konf. u ramkakh Kiber tyzhnia Shotlandii. Onlain-konferentsiia. 2025 [in Ukrainian].
7. Case on the Azure Cloud Service: (1) Case number 20/01626; (2) Country: Norway (EU); (3) Dispute body: Datatilsynet vs Norges idrettsforbund og olympiske og paralympiske komitй (NIF), the Norwegian Olympic and Paralympic Committee and Confederation of Sports (NIF), The Norwegian Olympic and Paralympic Committee and Confederation of Sports (NIF); (4) Source of law: Articles 5(1)(a)(c)(f), 6, 32 GDPR; (5) Date of decision: May 05, 2021; (6) URL: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/varsel-om-overtredelsesgebyr-til-norges-idrettsforbund/; https://www.edpb.europa.eu/news/national-news/2021/norwegian-dpa-norwegian-confederation-sport-fined-inadequate-testing_en
8. Bulhakova D.A. Vymohy GDPR dlia intehratsii khmarnykh rishen na prykladi keisu pro FISCONETPLUS. XI *yurydychni mohylianski chytannia*: Vseukr. nauk.-prakt. konf. (24 kvit. 2025 r.). Mykolaiv, 2025. P. 22-26. URL: https://lnk.ua/b1V9dzleg [in Ukrainian].
9. Case on FisconetPlus: (1) Case Number: 82/2020; (2) Country: Belgium (EU); (3) Dispute body: Data Protection Authority (DPA) vs FPS Finance; (4) Source of law: Articles 6(1), 25(1), 35 GDPR; (5) Date of decision: December 23, 2020; (6) URL: https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-82-2020.pdf
10. Cloud computing law / ed. by C.J. Millard. 2nd Ed. Oxford University Press, 2021. 648 p.
11. Michels J.D., Millard C., Turton F. Standard Contracts for Cloud Services. *Cloud Computing Law* / ed. by C.J. Millard. 2nd Ed. Oxford University Press, 2021. P. 61.
12. Georgiopoulou Z., Makri E.-L., Lambrinoudakis C. GDPR compliance: proposed technical and organizational measures for cloud provider. *Information and Computer Security*. 2020. Vol. 28 (5). P. 665-680. https://doi.org/10.1108/ICS-01-2020-0009
13. Casalicchio E., Cardellini V., Interino G., Palmirani M. Research challenges in legal-rule and QoS-aware cloud service brokerage. *Future Generation Computer Systems*. 2018. Vol. 78, pt 1. P. 211-223. https://doi.org/10.1016/j.future.2016.11.025

14. Pro khmarni posluhy: Zakon Ukrainy vid 17.02.2022 No. 2075-IX URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text [in Ukrainian].
15. Deiaki pytannia nadannia ta vykorystannia khmarnykh posluh ta/abo posluh tsentru obrobky danykh: postanova Kabinetu Ministriv Ukrainy vid 11.02.2025 No. 154. URL: https://zakon.rada.gov.ua/laws/show/154-2025-%D0%BF#Text [in Ukrainian].
16. Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 01.06.2010 No. 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text [in Ukrainian].
17. Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I). *Official Journal of the European Union*. 4.7.2008. L 177. P. 6-16. URL: https://eur-lex.europa.eu/eli/reg/2008/593/oj
18. Zandesh Z., Ghazisaeedi M., Devarakonda M.V., Haghighi M.S. Legal framework for health cloud: A systematic review. *International Journal of Medical Informatics (Shannon, Ireland)*. 2019. Vol. 132. P. 103953. https://doi.org/10.1016/j.ijmedinf.2019.103953
19. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance), PE/49/2023/REV/1. *Official Journal of the European Union*. 22.12.2023. L 2023/2854. URL: http://data.europa.eu/eli/reg/2023/2854/oj
20. Suver C., Thorogood A., Doerr M., Wilbanks J., Knoppers B. Bringing Code to Data: Do Not Forget Governance. *Journal of Medical Internet Research*. 2020. Vol. 22. No. 7. e18087. https://doi.org/10.2196/18087
21. Trubiani F. Cloud Computing Services: Towards a Digital Sustainability under EU Digital Law. *European Journal of Privacy Law & Technologies*. 2023. Is. 2. P. 143-154. https://doi.org/10.57230/ejplt232TF

Received 29.04.2025

Дар'я БУЛГАКОВА, д-р філософії з міжнародного права,
доцент кафедри права та публічного управління,
Запорізький інститут економіки та інформаційних технологій,
м. Кривий Ріг, Україна
orcid.org/0000-0002-8640-3622

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ЧАС ЇХ ОПРАЦЮВАННЯ У ХМАРНИХ СЕРВІСАХ

Досліджено проблему оброблення персональних даних користувачів під час застосування хмарних сервісів органами державної влади. Основну увагу приділено недолікам у сфері прозорості, мінімізації, пропорційності й інформованої згоди, а також відсутності оцінювання впливу впровадження технічних рішень на захист даних. В умовах інтеграції України в європейське правове середовище важливо розглядати ці питання крізь призму права Європейського Союзу, а саме Загального регламенту захисту даних *GDPR*. Дослідження показало, що відсутність чітких меж відповідальності та недотримання принципів *GDPR* створює високі ризики для прав і свобод фізичних осіб. Тому розглядається питання запровадження спільної відповідальності державних органів і хмарних провайдерів, зокрема в контексті автентифікації через сторонні акаунти та використання *cookie*-файлів, наголошується на необхідності відповідальності основних гравців обміну даними, а саме бізнесу та державних органів (*B2G*), під час оброблення даних у цифровому середовищі хмарних сервісів.

Набуття чинності Законом України від 16.09.2022 «Про хмарні послуги» та постановою Кабінету Міністрів України від 11.02.2025 «Деякі питання надання та використання хмарних послуг та/або послуг центру обробки даних» істотно впливає на юридичну практику, особливо щодо *B2G* обміну. Нові правові вимоги та зобов'язання, які виникають під час надання та використання хмарних послуг і послуг центрів оброблення даних, потребують практичних роз'яснень.

Розглянуто два актуальних щодо проблематики дослідження кейси, які можна використати для удосконалення вітчизняного законодавства. Перший кейс витоку персональних даних у Норвезькій конфедерації спорту (*NIF*), що стався внаслідок тестування хмарного сервісу *Microsoft Azure* (2021) без належного технічного та організаційного забезпечення, демонструє критичну важливість дотримання вимог захисту персональних даних на прикладі *GDPR*, що є необхідним на всіх етапах упровадження хмарних технологій. Використання реальних персональних даних у тестовому середовищі без оцінювання ризиків і налаштування захисту призводить до відкриття доступу до особистої інформації. Це й сталося у досліджуваному кейсі, де понад 3,2 млн осіб, серед яких майже пів мільйона неповнолітніх, стали об'єктами порушень, захист даних яких не був дотриманий. Для України, яка активно впроваджує цифрову трансформацію та інтеграцію хмарних рішень у публічний і приватний сектори, цей кейс є показовим. Він підкреслює необхідність запровадження обов'язкових практик оцінювання ризиків, використання синтетичних або знеособлених даних під час тестування, а також розроблення чітких стандартів кібербезпеки для хмарних середовищ. У контексті побудови електронного врядування та впровадження концепції "хмара за замовчуванням» (*cloud by default*) дотримання принципів прозорості, мінімізації та відповідальності під час роботи з персональними даними має бути стратегічним пріоритетом.

Дослідження другого кейсу *FisconetPlus* (2020) показує важливість чіткого дотримання принципів конфіденційності і захисту персональних даних під час впровадження хмарних сервісів у публічному секторі. Встановлено, що обов'язок конфіденційності має юридичне та договірне підґрунтя, а також повинен охоплювати всіх учасників, зокрема й підрядників, які виконують функції органів влади. Кейс підкреслює необхідність застосування принципів *privacy by design* і *privacy by default*, мінімізації даних, прозорості і забезпечення контролю над обробленням даних, особливо коли хмарна інфраструктура розміщується за межами країни. Для України цей кейс є важливим уроком зі створення національних правил і стандартів безпеки, які б гарантували захист персональних даних і державний суверенітет під час використання хмарних технологій.

Багато підприємств і державних установ нині активно впроваджують хмарні послуги, тому правники мають бути готовими надавати правову допомогу в питаннях безпеки даних, виконання вимог регуляторів, а також захисту прав й інтересів клієнтів у контексті нових технологічних викликів. У зв'язку з цим запропоновано практичні рекомендації щодо забезпечення відповідності хмарних рішень європейським вимогам, а саме: оцінювання впливу, дотримання принципу захисту даних за замовчуванням (*privacy by design* і *by default*) та впровадження прозорої політики збирання та оброблення даних.

Результати дослідження є актуальними для правників, щоб вони могли ефективно реагувати на правові виклики, які постають у процесі інтеграції новітніх технологій у межах національного та європейського законодавства, та забезпечувати належну правову підтримку бізнесу й органам влади, що працюють із хмарними сервісами.

Ключові слова: обмін даними між бізнесом і державою, захист даних, постачальник послуг, протоколи безпеки, конфіденційна інформація.