Journal of Theoretical and Applied Information Technology
15st June 2026. Vol.104. No.11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PERSONAL DATA PROCESSING IN STATE INFORMATION SYSTEMS: ADMINISTRATIVE, LEGAL, AND TECHNOLOGICAL REGULATION

OLEH PREDMESTNIKOV[1], VLADYSLAV VEKLYCH[2], IVANNA HORBACH-KUDRIA[3], IVAN SHUMEIKO[4], VIKTORIIA KORETSKA[5]

[1]Doctor of Legal Sciences, Professor, Head of the Department of Law, Faculty of Natural Sciences and Geography of Bogdan Khmelnitsky Melitopol State Pedagogical University, Zaporizhzhia, Ukraine
[2]Doctor of Law, Professor of the Department of Theory of State and Law and Constitutional Law, Prince Volodymyr the Great Educational and Scientific Institute of Law, Interregional Academy of Personnel Management, Kyiv, Ukraine
[3]PhD in Law, Associate Professor, The Department of Police Activities, The National Academy of Internal Affairs, Kyiv, Ukraine
[4]PhD in Law, Senior Lecturer, Department of Management and Public Administration, Faculty of Economics and Business of Dmytro Motornyi Tavria State Agrotechnological University, Zaporizhzhia, Ukraine
[5]PhD in Law, Associate Professor, Department of Law, Lutsk National Technical University, Lutsk, Ukraine

E-mail: [1]olehpredmestnikov.melitopol@gmail.com, [2]vladveklych173@gmail.com, [3]ivannakudria117@gmail.com, [4]ishumeiko222@gmail.com, [5]vikoretska18@gmail.com

ABSTRACT

The administrative and legal regulation of personal data processing in state information systems (SIS) is becoming increasingly important because of the development of e-government and digital identification systems. The aim of the study is to establish how legal instruments ensure lawful, transparent, and secure data processing. The methodology includes comparative legal analysis, documentary review, and case studies, with a focus on jurisdictions with developed e-government.
Significant discrepancies between norms and practice were identified, especially in the areas of accountability, data minimization, and cross-border exchange. In Germany, the BundID system provides legal certainty thanks to clear obligations enshrined in federal law. Legal transformation is ongoing in Ukraine (the Diia platform). Most systems lack effective oversight and are not adapted to technological changes. The user access to the X-Road-based platform complies with Articles 5 and 6 of the General Data Protection Regulation (GDPR) regarding the lawfulness of processing and identification. The Delphi procedure revealed only 12% agreement on the criteria of minimization and user autonomy.
It is necessary to update the legal framework, implement risk-based control, unify standards with international norms. Research into automated tools and adaptive management models using artificial intelligence (AI) and biometrics is promising.
Keywords: *Administrative Regulation, Legal Framework, Personal Data, Data Processing, Government Systems, Information Systems, Public Administration, Data Protection*

1. INTRODUCTION

The rapid digitalization of public administration has led to significant changes in the collection, processing, and storage of personal data in public information systems [1]. The administrative and legal regulation of these processes is becoming crucial for ensuring national security, public trust, democratic accountability, and institutional transparency [2]. SIS, in particular population registries, e-government platforms, and digital health services, contain confidential information of citizens. Their functioning requires clear legal regulation, which guarantees compliance with constitutional rights and international obligations in the field of personal data protection [3].

In this context, the effectiveness of administrative regulation increasingly depends on the ability of public institutions to manage complex digital infrastructures. This includes integrated platforms and intelligent systems that operate as socio-technical environments rather than merely legal constructs [4].

The relevance of the study is determined by the global trend of digitalization of public services and the simultaneous expansion of state control [5]. However, many countries, including jurisdictions with developed legal systems, have problems of fragmented regulation, weak implementation of laws, and inconsistent law enforcement practices [6]. Recent studies in the field of information technology show that the latest digital tools not only increase the efficiency of operations, but also transform the ways of decision-making and regulatory control. This, in turn, affects how administrative norms are implemented in the digital environment [7].

In post-Soviet states, these challenges are exacerbated by regulatory inertia, outdated regulations, and unclear administrative mandates. This negatively affects the state's interaction with vulnerable groups in the areas of social security, migration, and personal data management [8].

From a legal perspective, personal data protection in SIS is closely linked to more general guarantees of citizens' rights and freedoms. This, in turn, depends on the effectiveness of administrative practices and mechanisms of institutional accountability [9].

From a technological perspective, the risks faced by SIS are becoming increasingly complex. Key threats include ransomware attacks, unauthorized access, and large-scale data leaks that challenge the resilience of the state's digital infrastructure [10].

An additional problem is the lack of interoperability between legacy platforms and modern digital solutions. This complicates the secure and timely exchange of data between government agencies. In parallel, the integration of advanced technologies, in particular AI and blockchain, creates new regulatory challenges related to algorithmic accountability, ethical use, and ensuring transparency. The increasing complexity of cyberattacks combined with the accelerated implementation of innovative technologies emphasizes the need to create legal mechanisms that are adaptive, technologically sound, and aligned with international cybersecurity standards [11].

Despite the growing attention to the issues of personal data protection and cybersecurity, key issues remain unexplored. These include the demarcation of administrative powers between government agencies, the role of public authorities in preventing the misuse of data, and the effectiveness of administrative liability mechanisms for security breaches.

Research hypothesis: the level of personal data protection in SIS depends on the quality of the legal regulation, administrative accountability, and transparency of institutions.

The academic novelty of the study lies in the development of an interdisciplinary comparative framework that combines legal compliance assessment, administrative accountability analysis, and technological governance evaluation for state information systems. Unlike prior studies focused primarily on isolated legal or technical aspects, this research integrates Legal Compliance Scores (LCS), Administrative Efficiency Index (AEI), Digital Legal-Twin Modelling (DLTM), and Delphi-based validation into a unified model for evaluating the practical effectiveness of personal data governance.

Digital Legal-Twin Modelling refers to the creation of a virtual legal-administrative representation of regulatory procedures, data flows, and institutional control mechanisms within digital state systems.

Algorithmic Audit Matrix refers to a structured multi-criteria compliance assessment model used to evaluate the alignment of technological systems with legal and administrative standards.

The aim is to critically evaluate the current model of administrative and legal regulation of personal data processing in SIS and offer recommendations for its modernization, taking into account international experience and modern technological challenges.

Research objectives:

1. Analyse the regulatory and legal background and institutional frameworks for the regulation of personal data in state administration;

2. Study the legal mechanisms of control, supervision, and liability for data security violations;

3. Identify gaps and contradictions in regulation and develop proposals for its improvement.

2. LITERATURE REVIEW

The literature review was conducted using a structured comparative approach aimed at identifying the current state of research on administrative and legal regulation of personal data processing in state information systems. The literature sample included peer-reviewed journal articles, international regulatory reports, and legal-technical studies indexed in Scopus, Web of Science, IEEE Xplore, and official European Union databases published primarily between 2020 and 2025. The selection criteria included: (1) direct relevance to personal data regulation in digital public administration; (2) analysis of legal or technological safeguards in state information systems; (3) empirical or comparative methodological design; and (4) applicability to GDPR-oriented governance models. Sources focused exclusively on private-sector data ecosystems without relevance to public administration were excluded. This approach ensured the representativeness, relevance, and methodological adequacy of the literature sample for identifying current research gaps and unresolved regulatory challenges.

This review analyses the current literature on various legal systems, focusing on conceptual development and comparative analysis of regulatory frameworks. Consent mechanisms and data protection guarantees in public administration are separately considered. The main research gaps and directions for further research are also covered.

The authors [12] proposed a DICON consent management model that is independent of the application area. This system has built-in legal compliance mechanisms and creates a basis for further discussions on the implementation of consent in public systems. However, the implementation of such technical solutions in public administration is still poorly studied. The study [13] conducted a comparative analysis of approaches to de-identification of personal data in the EU, the US, Japan, and South Korea. They found significant differences in anonymization and pseudonymization standards. However, the study does not cover the implications of these differences for cross-border interoperability of public systems and regulatory harmonization. Besides, it does not address the issue of mutual legal assistance in cases of data security breaches. The author [14] analyses the issue of information security within the framework of Ukrainian legislation, focusing on legislative gaps and shortcomings in national cybersecurity. The author points to the lack of clear standards for processing biometric and confidential data in state electronic platforms. However, her study is descriptive and does not contain a comparative analysis with European models. The researchers [15] consider the legal regulation of biometric data and facial recognition technologies based on a comparative law approach. They note significant differences in control and supervision mechanisms in different countries. Despite the relevance of the criticism of security models, the study does not examine the specifics of biometric data processing in large SIS.

The study [16] analyses the transformation of approaches to personal data protection in the context of Industrial Revolution 4.0. Although the study focuses on consumer data, its findings have indirect implications for public systems, especially due to the convergence of commercial and administrative data sources. However, the legal mechanisms for distinguishing these processes remain outside the author's attention. The authors [17] analyse the regulation of public e-services, revealing fragmentation of legislation, lack of standardized procedures and legal inconsistency. However, aspects of technical implementation and the burden on authorities to comply with the requirements are hardly addressed. The study [18] examines Data Protection Impact Assessments (DPIAs) under the GDPR through a feminist legal approach. The work brings an interdisciplinary ethical perspective, emphasizing the importance of contextualizing risks. However, the practical relevance for public administration is limited by the lack of recommendations for integrating DPIA into public processes.

The technical and methodological aspects of data anonymization have attracted considerable attention in the academic community. The authors [19] reveal the insecurity of current practices of biometric data anonymization, pointing out the risk of creating a "false sense of privacy". This issue is further emphasized the researchers [20], who presented the SwipeFormer model for mobile biometric authentication. Their study demonstrates both the potential of using biometrics in public services and the associated privacy threats. The authors [21] reached similar conclusions, analysing the use of electronic health records based on fingerprint sensors. They emphasize the need for strict legal controls in areas where sensitive personal data are processed, in particular in healthcare.

At the same time, there are certain significant gaps in the academic literature. First, there is a lack of comprehensive studies of administrative data

processing procedures in SIS, as most studies focus either on private sector practices or on general principles of data protection. Second, there are conceptual contradictions among researchers: some emphasize the need for strict regulation to ensure the protection of individual rights [18; 19]. At the same time, others emphasize the functional need for flexible regulation to improve the efficiency of public services [17]. Third, although biometric technologies are actively studied, the issues of accountability of government agencies implementing these tools have not been sufficiently investigated. This is especially true for oversight mechanisms and legal remedies in cases of violations. Finally, cross-national comparative studies are reduced mainly to de-identification policies [13]. At the same time, insufficient attention has been paid to the administrative and legal principles of regulating state information systems in Eastern European, African, and Middle Eastern countries.

The analysis of prior literature demonstrates that existing studies predominantly examine either technical cybersecurity mechanisms or general legal principles of personal data protection separately. However, insufficient attention has been devoted to integrated administrative-legal and technological assessment models capable of evaluating the practical effectiveness of state information systems under conditions of digital transformation. In particular, previous studies rarely combine legal compliance indicators, institutional accountability mechanisms, technological interoperability, and user autonomy within a unified analytical framework. Therefore, this study contributes to the literature by developing a comparative interdisciplinary model based on Legal Compliance Scores (LCS), the Administrative Efficiency Index (AEI), Digital Legal-Twin Modelling (DLTM), and Delphi-based expert validation for assessing the effectiveness of personal data governance in state information systems.

3. METHODS

3.1. Research design

The study was conducted as a structured assessment of the administrative and legal mechanisms for regulating the processing of personal data in SIS. The analysis was conducted on the example of selected jurisdictions in four stages (Figure 1).

The comparative multi-stage research design was selected because it enables simultaneous assessment of legal, institutional, and technological dimensions of personal data governance across different administrative systems. The selected design is appropriate for answering the research objectives because it allows identification of regulatory inconsistencies, institutional implementation gaps, and differences in technological compliance mechanisms within comparable digital governance environments.

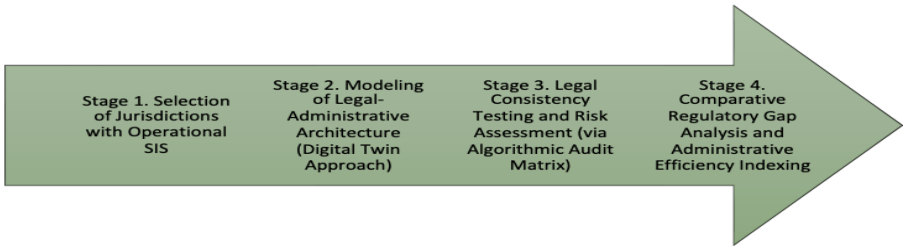


Figure 1: General research design

Source: developed by the authors based on MiniTAB [22]

3.2. Sampling

The empirical background of the study is formed by five national SIS, one in each of these countries (Table 1).

Table 1: National information systems involved in the empirical analysis

Country	Information system	Selection criteria (generalized)
Germany	BundID	High level of functional maturity; legal regulation of personal data under GDPR; accessible documentation
Estonia	X-Road	The most developed digital infrastructure; full integration with GDPR; openness of documentation
Poland	ePUAP	Developed e-administration; harmonized with GDPR; accessibility of regulatory framework
Croatia	eGrađani	Medium level of maturity; legislation adapted to GDPR; availability of public documentation
Ukraine	Diia (portal and application)	Hybrid model (post-Soviet + GDPR elements); rapid development; limited open documentation

Source: developed by the authors

The justification for the sample size (n=5 systems) is based on the richness of the data and the application of a comparative legal approach. Each system underwent a unified procedural review, which guaranteed the homogeneity of the analysis and the possibility of comparison. Given the high level of complexity of administrative and legal architectures, as well as the focus of the study on national-level practices, the sample is sufficient to achieve the set objectives.

3.3. Methods

- Digital Legal-Twin Modelling (DLTM). Each information security system (ISS) was reconstructed as a digital legal twin. This twin covers regulatory layers, which include regulations, administrative rules and data protocols, as well as control mechanisms such as authorization logs and consent registers. Procedural workflows were also integrated into the model.

The models were implemented using BPMN 2.0 diagrams in the Camunda Modeler environment. This enables efficient tracking and reproduction of administrative sequences. The approach used provides a structured representation of legal obligations and administrative functions in visual and machine-readable formats.

- Algorithmic Audit Matrix (AAM). A multi-criteria audit matrix was used to assess compliance with the legislation, covering six key dimensions (lawfulness of data collection; limitation of processing purposes; data minimization; transparency and accountability; implementation data subject rights; data processing security).

Each of the above dimensions was rated on a scale from 0 to 10, where 0 meant complete non-compliance and 10 meant complete compliance. The rating was based on an analysis of regulatory acts, implementation instructions and relevant platform documentation. The following formula was used:

$$Legal\ Compliance\ Score\ (LCS) = \frac{\sum_{i=1}^{n} d_i}{n}$$

Where: d_i – score per dimension; n – number of dimensions (here, 6).

-Development of the Administrative Efficiency Index (AEI). To quantify administrative efficiency in legal data management, the AEI was formulated as follows:

$$AEI = \frac{C_l + T_p + U_a}{3}$$

Where: C_l – Clarity of legal norms (measured by the number of unambiguous obligations per 1,000 words); T_p – Technology Policy Integration Index (based on compatibility between legal powers and IT protocols); U_a – User Autonomy Index (degree of end-user control over personal data settings based on direct testing).

- Delphi method for peer review. To reduce subjective bias, each AAM result was reviewed by a panel of 9 experts (lawyers, IT auditors, public sector regulators) over two Delphi rounds. Mean values were used where the difference in scores exceeded ±2 points.

To reduce unnecessary methodological variation and increase reliability, all evaluated systems were assessed using identical analytical dimensions, standardized scoring criteria, and unified procedural workflows. Control measures included Delphi-based expert verification, normalization of evaluation indicators, cross-validation of legal sources, and repeated comparative assessment of regulatory documentation. These mechanisms

minimized subjective interpretation and ensured consistency of comparative results across jurisdictions.

3.4. Tools

All software used was open source or licensed by institutions, including Camunda BPMN Modeler, LibreOffice Calc, and QGIS 3.28 (used to visualize administrative jurisdiction boundaries in mapping SIS regulations).

4. RESULTS

The conclusions regarding the effectiveness of administrative and legal regulation were reached through a comparative assessment of Legal Compliance Scores (LCS), Administrative Efficiency Index (AEI), Digital Legal-Twin Modelling outputs, and Delphi-based expert validation. Systems demonstrating consistently high scores across legal clarity, technological integration, user autonomy, transparency, and security dimensions were interpreted as administratively effective and legally sustainable. Conversely, lower scores and high expert disagreement indicated fragmentation of regulation, insufficient institutional accountability, and limited implementation maturity.

4.1. Legal Compliance Scores (LCS) – results of an algorithmic audit matrix

All systems were assessed against six legal dimensions reflecting key principles of the GDPR or administrative law. Table 2 shows the scores for each dimension and the aggregated LCS indices for national SIS. The scores were based on a scale of 0 to 10, with 10 indicating full compliance with the law and implementation of best practices, and 0 indicating full non-compliance or lack of appropriate legal mechanisms.

Table 2: Legal Compliance Scores (LCS) for SIS and legal dimension (max. score per dimension = 10)

Country	SIS	Lawfulness	Purpose Limitation	Minimization	Transparency	Rights Implementation	Security	LCS (Avg)
Germany	BundID	9.5	9.2	8.9	9.4	9.0	9.1	**9.18**
Estonia	X-Road	9.0	8.7	8.5	9.0	8.8	8.9	**8.82**
Poland	ePUAP	8.3	8.0	7.5	7.8	7.2	7.5	**7.72**
Croatia	eGrađani	7.5	7.8	7.0	7.2	6.8	6.9	**7.20**
Ukraine	Diia	6.8	6.5	6.3	6.9	6.0	6.4	**6.48**

Source: developed by the authors based on European Commission, Directorate-General for Justice and Consumers [23], European Data Protection Board [24], European Data Protection Board [25]

The legal compliance of digital personal data processing systems were assessed according to six key dimensions for the purpose of a comprehensive analysis of compliance with the law, in particular with European standards. *The first criterion* is the lawfulness of data collection based on clear legal grounds (consent, legal obligation, public interest). Germany (9.5) and Estonia (9.0) received the highest scores due to a strong regulatory framework. Ukraine (6.8) has a lower score due to insufficient harmonisation of legislation. *The second dimension* is purpose limitation: collecting data for specific and legitimate purposes. Germany (9.2) and Estonia (8.7) adhere to this strictly, Ukraine (6.5) is weaker due to general formulations of the purposes. *The third criterion* is data minimisation, i.e. limiting the collection to only necessary personal data. Germany (8.9) and Estonia (8.5) are effective, while Croatia (7.0) and Ukraine (6.3) collect excessive data. *Fourth* — transparency: availability of information about data processing. Germany (9.4) has multi-level notifications and interactive tools, Ukraine (6.9) is improving the Diia mobile application, but lacks transparency at the server level. *Fifth* — implementation of subjects' rights: access, correction, deletion. Germany (9.0) and Estonia (8.8) use automated tools, Ukraine (6.0) — mainly manual requests. *Sixth* — security: technical and legal protection (encryption, logging, protocols). Germany (9.1) and Estonia (8.9) comply with the GDPR and cyber policies, while Ukraine (6.4) has a weaker infrastructure. Overall, the average legal compliance score (LCS) is highest in Germany (9.18), followed by Estonia (8.82), Poland (7.72), Croatia (7.20), Ukraine (6.48), which reflects the level of legal maturity of digital systems and the implementation of digital rights.

4.2. The AEI Results

The AEI calculations included legal clarity (CL), technology policy integration (TP), and user autonomy (UA). These components were quantified by a formula and normalized for comparison. Table 3 provides a summary index of the effectiveness of personal data processing regulation.

Table 3: The AEI values for SIS

Country	SIS	Clarity of Legal Norms (CL)	Tech-Policy Integration (TP)	User Autonomy (UA)	AEI (Avg)
Germany	BundID	87.2	92.5	85.7	88.47
Estonia	X-Road	85.0	88.0	83.2	85.40
Poland	ePUAP	75.3	77.0	70.5	74.27
Croatia	eGrađani	70.1	72.5	68.0	70.20
Ukraine	Diia	65.8	67.2	60.4	64.47

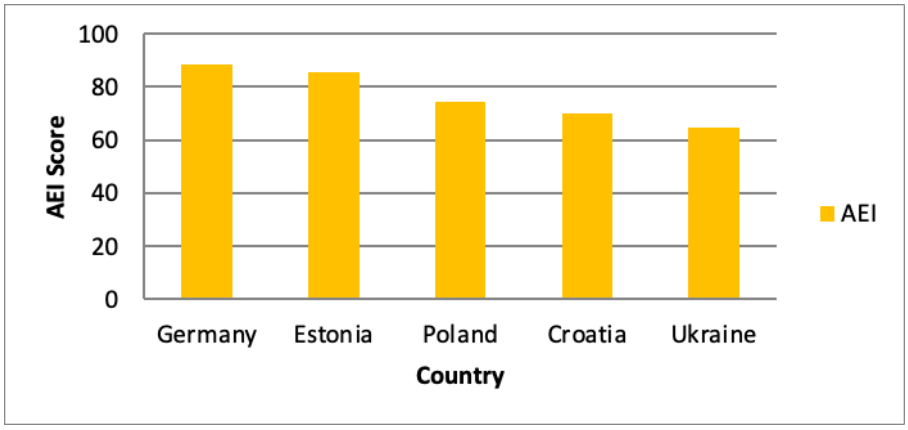
Source: developed by the authors based on Bundesamt für Sicherheit in der Informationstechnik [26], X-Road Project [27], Ministerstwo Cyfryzacji [28], Government of Croatia [29], State Services Online [30], OECD [31]

Germany (BundID) demonstrates a high level of legal clarity (CL = 87.2), driven by detailed provisions of federal data protection law. Technical and legal integration (TP = 92.5) is implemented through the OAuth2 consent tracking protocol. Users have high autonomy (UA = 85.7) thanks to specialized control panels, which provides the highest level of overall efficiency (AEI = 88.47). Estonia (X-Road) has a stable regulatory framework (CL = 85.0), aligned with the Public Information Act and GDPR. Transparent technical architecture, including blockchain logs (TP = 88.0), and decentralized identity management (UA = 83.2) ensure a high level of AEI (85.40).

Poland (ePUAP) is characterized by moderate legal clarity (CL = 75.3), complicated by regulatory fragmentation. Technical integration (TP = 77.0) is limited to functional, but not legally deep solutions. User autonomy is low (UA = 70.5), AEI — 74.27. Croatia (eGrađani) has a concise, but weakly digitalized regulatory framework (CL = 70.1). Partial technical integration (TP = 72.5) and limited user control (UA = 68.0) lead to AEI = 70.20. Ukraine (Diia) is in the transformation stage (CL = 65.8). Despite innovative technologies, legal integration is weak (TP = 67.2), and user autonomy is limited (UA = 60.4), which results in the lowest AEI (64.47).

Figure 2 is a bar chart comparing the (AEIs) for the systems of Germany, Estonia, Poland, Croatia, and Ukraine as a comprehensive assessment of the effectiveness of personal data processing regulations.

Figure 2: Comparative performance of the AEI in five national systems



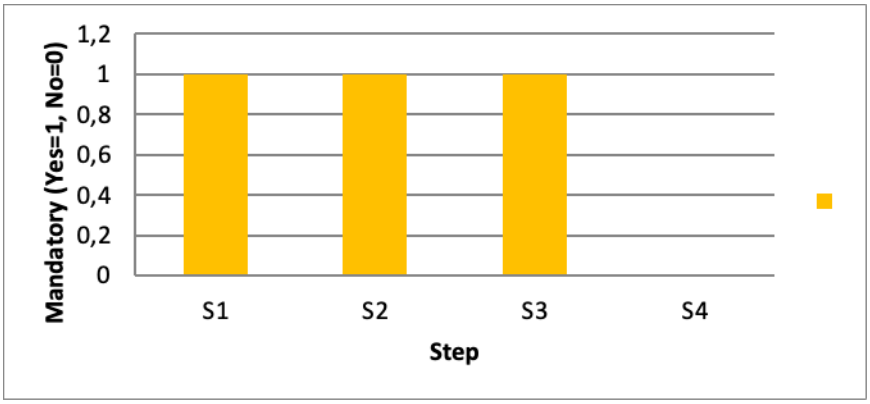
Source: developed by the authors based on European Commission [32], United Nations Development Programme [33]

The visual gradient of the bar heights clearly illustrates the downward trend in administrative efficiency, extending from Western European countries (Germany, Estonia) to Eastern European countries (Croatia, Ukraine). The chart clearly shows the gaps between legal frameworks and technical implementations. This shows that the maturity of a digital system in itself is not a guarantee of a high level of administrative efficiency. The image above confirms the key conclusion of the study: a balanced integration of legal regulation, technological solutions, and user rights protection is crucial for effective personal data management.

4.3. Summary of the DLTM results

Each SIS was reconstructed as a digital legal twin to visualize regulatory sequences, data checkpoints, and user consent. Figure 3 illustrates the BPMN 2.0 model of the Estonian X-Road platform, one of the most modern public information systems in the European Union (EU).

Figure 3: Digital legal twin of the Estonian BPMN-based X-Road system



Source: developed by the authors Visual Paradigm [34], STP Informationstechnologie GmbH. [35], Digital Twin Consortium [36]

The user's interaction with the state digital service via the X-Road platform begins with an access request, which is recorded as the start of personal data processing in accordance with the law. The first stage is authentication using an ID card or Mobile-ID with multi-factor authentication (MFA), which complies with the principles of lawfulness and identification in accordance with Art. 5 and 6 of the GDPR. In case of unsuccessful authentication, the processing is terminated. Next, the system determines the need for the user's consent. If further data processing, in particular transfer to third parties, requires consent, its presence and validity are checked in accordance with Art. 7 of the GDPR. In the absence of valid consent, the user is redirected to the procedure for providing it. This process is automated using a legal digital twin in accordance with the rules of law.

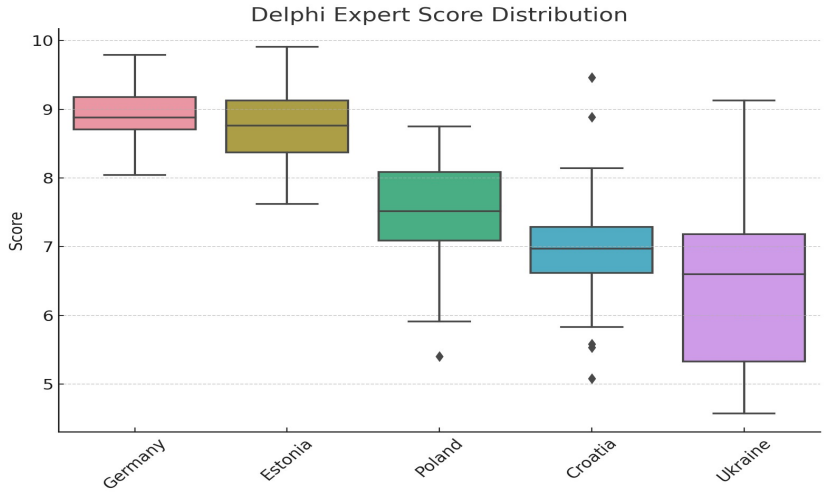
If consent is not required (for example, in tax reporting), the verification stage is bypassed and the request is transmitted through the secure decentralized architecture of X-Road. This ensures the minimization of processing and data integrity in accordance with Art. 5(1)(c) and 32 of the GDPR. All transactions are recorded in a blockchain journal in accordance with Art. 30 of the GDPR and the Estonian Information Society Services Act, which guarantees transparency and immutability of records. The completion of the process may include the provision of a service or the recording of an exceptional event (denial, timeout, access attempt), which ensures legal reliability.

4.4. Delphi Panel Consolidation

The Delphi method showed an average of 12% of the previous scores. The main differences concerned the criteria of "data minimization" and "user autonomy". Figure 4 shows a box plot of the distribution of scores of five national SIS over two rounds. The assessment was carried out on six dimensions of GDPR compliance. The indicators reflect the consolidated position of the nine experts of the interdisciplinary group after eliminating differences in the results.

An assessment of the legal compliance of digital identification systems in five European countries revealed significant differences in the level of expert consensus. In Germany (BundID), the median is 9.2 with a narrow interquartile range (8.8–9.6), indicating high unanimity and confidence among experts. In Estonia (X-Road), the median is 8.8, the IQR is somewhat wider but remains stable (8.3–9.3); the variation is related to the interpretation of the decentralized architecture. In Poland (ePUAP), the median score is 7.5, the IQR is wider (6.9–8.1), indicating differences in the perception of legal clarity and level of implementation.

Figure 4: Box plot of Delphi-validated expert estimates by legal dimension



Source: calculated by the authors based on European Commission, Directorate-General for Climate Action, Ricardo Energy & Environment, & E4tech [37], Stat59 [38], University of Turku Futures Research Centre (eDelphi) [39]

The eGrađani system in Croatia has a median of 7.0, a wide IQR (6.2–7.8) and possible outliers below 6, indicating criticism of regulatory vagueness and the presence of non-automated procedures. The least agreement is observed in Ukraine (Diia), where the median is 6.5 and the IQR is the widest, with scores up to 5.5 and below. This is caused by the ambiguous perception of Diia's mobile-oriented architecture and the lack of complete regulatory design. Overall, the results demonstrate a high level of consensus in assessing legal compliance for Germany and Estonia. This indicates the structural and procedural maturity of their digital systems. Poland and Croatia are characterized by a moderate divergence of expert opinions, reflecting the ambiguity in legal regulation and implementation of guarantees. In the case of Ukraine, the highest level of uncertainty is observed, indicating the transitional state of the legal system and different approaches to interpreting the regulatory framework for digital identification.

5. DISCUSSION

The aim of the study was to analyse the administrative and legal regulation of personal data processing in SIS. Particular attention was paid to finding a balance between the right to personal privacy and state interests in the field of security and digital transformation.

The results of the study confirmed the initial hypothesis: while legal regulation in Ukraine and a number of comparable jurisdictions formally complies with international standards, administrative implementation mechanisms remain fragmented. This creates risks of both inefficiency and violations of fundamental human rights.

The key conclusion is the identification of significant gaps in state information systems. In particular, centralized solutions such as the Ukrainian platform — Diia, despite facilitating the accessibility of electronic services, demonstrate an insufficient level of protection against large-scale data breaches. In contrast, decentralized architectures, in particular X-Road in Estonia, provide a more stable and legally accountable framework. This emphasizes the need to develop a new performance assessment model that will allow government agencies to verify the compliance of technical measures with established legal obligations.

The findings [19] on the unreliability of anonymization in biometric systems are consistent with our findings. Similarly, we argue that anonymization or pseudonymization without strong enforcement mechanisms is ineffective. However, our focus shifts from technical unreliability to the inadequacy of administrative oversight. The authors [20] reveal the potential of biometrics in the mobile environment. However, our study finds that in the context of massive public platforms such as Action, the lack of proper administrative regulation

significantly increases vulnerabilities. The researchers [12] argue for the weakness of the institutionalization of consent in public systems. We agree with their arguments, but further argue that a key problem is the lack of administrative capacity to enforce the rules across institutions. The authors [13] identify the differences in national de-identification systems. Our results complement these findings, demonstrating that the Ukrainian approach, due to excessive centralization, can be attributed to a "low level of compliance" with international standards.

The study [14] points to the lack of a unified legal approach to information security in Ukraine. Our results confirm this thesis, but also highlight the insufficient development of the administrative machinery, which leads to uneven law enforcement. The researchers [15] showed the risks of biometrics abuse in the face of weak regulation. Our study confirms these results, revealing a particular threat in centralized state databases. The study [16] emphasized the growing importance of personal data protection in the digital economy. We extend this approach by arguing that the protection of user rights should be an integrated element of public administration. The authors [17] found inefficiency of e-government services in Kazakhstan. Our findings show similar problems in Ukraine, indicating the systemic nature of regional challenges. The study [18] emphasizes the importance of using DPIA as part of GDPR. Our analysis proves that in Ukraine this tool is almost not used, which creates a gap between legal harmonization and administrative practice. The authors [21] demonstrate the benefits of biometric systems in the field of healthcare. At the same time, we argue that without proper regulation they can generate additional risks in large public registers.

Theoretical contribution. The study proposes a new model for assessing the administrative effectiveness of regulating state information systems. It is based on the interaction of legal norms, institutional capacity, and technological safeguards and provides a systematic approach to assessing the transformation of regulatory provisions into real data protection.

Practical contribution. The obtained results give grounds to provide recommendations for the governments of Ukraine and other states:

1. Move from centralized platforms (e.g., Diia) to distributed architectures like X-Road;

2. Implement domain-independent consent management systems to strengthen user control;

3. Institutionalize mandatory DPIAs for all state projects involving work with confidential data;

4. Create independent bodies to ensure administrative accountability.

6. LIMITATIONS

1. Limited jurisdictional coverage. The study focuses primarily on the analysis of administrative and legal frameworks within a limited number of jurisdictions. This approach does not allow for a full reflection of the diversity of global regulatory strategies. The limited geographical coverage potentially reduces the generalizability of the results, especially with regard to states with different legal traditions or mixed models of personal data management.

2. Challenges associated with technological dynamics. The article examines legal mechanisms in the context of the current state of digital technologies. At the same time, the rapid development of information systems, in particular the implementation of state platforms based on AI, may lead to a rapid loss of relevance of some regulatory conclusions. This creates risks for the long-term stability and adaptability of the formulated legal provisions.

3. Limited empirical verification. The methodological background of the study is largely based on doctrinal analysis and the study of regulatory acts. The lack of empirical data on the practical application of these norms in administrative activities narrows the possibilities of objectively assessing their effectiveness and practical feasibility in specific administrative contexts.

7. RECOMMENDATIONS

1. Expanding comparative legal analysis. Further research should cover a wider range of legal systems within the framework of comparative legal analysis, in particular jurisdictions undergoing digital transformation. Involving civil, common, and mixed law systems will allow for a more comprehensive understanding of the most effective practices for regulating the processing of personal data in SIS.

2. Applying empirical legal approaches. It is appropriate to supplement doctrinal research with empirical approaches. These include the analysis of administrative practice, the assessment of law enforcement indicators, as well as interviews with representatives of state bodies and other stakeholders. This will enable not only to more

deeply assess the effectiveness of current regulation, but also to identify key challenges associated with its practical application.

3. Developing adaptive regulatory models. Given the rapid development of digital technologies, administrative and legal mechanisms should provide for flexibility and scalability. Particular attention should be paid to regulatory models that take into account the integration of new technologies, including blockchain solutions, biometric systems, and AI. It is extremely important to ensure compliance with constitutional principles and guarantees for the protection of human rights.

7.1. Differences from Prior Literature

Unlike previous studies that primarily focus either on technical cybersecurity mechanisms or on abstract legal guarantees of personal data protection, this research integrates administrative, legal, and technological dimensions into a unified analytical framework. Existing studies mainly analyse isolated aspects of digital governance, including biometric privacy risks, anonymization procedures, or GDPR interpretation. In contrast, the present study evaluates the operational interaction between legal norms, institutional accountability, and technological implementation in state information systems.

A key distinction of this study is the application of Digital Legal-Twin Modelling (DLTM) combined with the Algorithmic Audit Matrix (AAM) and the Administrative Efficiency Index (AEI). Previous literature rarely applies quantitative comparative indicators to assess the practical effectiveness of administrative regulation in public digital infrastructures. Moreover, prior studies insufficiently address the role of user autonomy, legal clarity, and institutional enforcement capacity as measurable indicators of regulatory effectiveness.

Another difference lies in the comparative assessment of centralized and decentralized state digital architectures. While earlier studies often discuss digitalization benefits conceptually, this study demonstrates that decentralized systems such as Estonia's X-Road provide stronger accountability and legal resilience compared to centralized models. Furthermore, the integration of Delphi-based expert validation increases the methodological reliability of the obtained results and reduces interpretative bias.

Consequently, the study extends existing scholarship by proposing an interdisciplinary model for evaluating the legal and administrative sustainability of state information systems under conditions of rapid digital transformation.

8. CONCLUSIONS

The study of the administrative and legal regulation of personal data processing in SIS demonstrates the growing importance of ensuring the legal and secure management of digital information in public sector infrastructures. In the context of digital transformation and growing dependence on e-government, the personal data protection is becoming a key legal and administrative priority. This aspect directly affects the efficiency of the functioning of state bodies, the transparency of procedures, and the level of public trust.

The results of the analysis show that the current administrative and legal frameworks in individual jurisdictions demonstrate a fragmented and often unsystematic approach to regulating the processing of personal data in SIS. The average LCS indicates a different degree of legal maturity of digital ecosystems in the studied countries. The main problems identified include: the lack of unified standards for inter-system interaction; limited accountability mechanisms for civil servants; insufficient implementation of risk-based models in regulatory practice.

Germany (BundID system) demonstrates a high regulatory certainty, which is ensured by clear administrative obligations enshrined in federal data protection legislation. In contrast, Ukraine (Diia platform) is undergoing transformation of the legal system and institutional mechanisms. It is also worth noting that the rapid development of digital technologies often outpaces the ability of legal and administrative mechanisms to adapt. This leads to the emergence of regulatory gaps and complicates the implementation of legal norms in practice. Secure access to personal data in state systems is ensured by user identification through MFA, which increases the level of data protection. After each transfer of information, transactions are recorded in an audit log using blockchain technology, which ensures transparency and immutability of access history. The study findings emphasize the need to develop a balanced and dynamic regulatory model that would combine legal certainty with flexible administrative tools. The proposed conceptual approaches to improving oversight mechanisms, increasing legal clarity, and implementing preventive regulatory technologies have practical implications for lawmakers, government agencies,

and information system developers. The Delphi methodology showed that the average value of preliminary assessments was 12% of cases. At the same time, significant discrepancies were recorded in the assessment of criteria such as "data minimization" and "user autonomy." This indicates the ambiguity of approaches to key aspects of personal data protection in different legal systems.

The obtained results can be used in the process of reforming national legislation and designing state digital infrastructure. They are also important for the development of international legal mechanisms for personal data protection that involve government agencies. Further research should focus on the integration of AI into the administrative management of personal data. Particular attention should be paid to the legal implications of algorithmic regulation and its impact on the legitimacy of managerial decision-making. In addition, comparative legal research can help identify effective practices for harmonizing administrative procedures across jurisdictions to ensure the efficient, accountable, and lawful processing of personal data in SIS.

REFERENCES:

[1] World Bank, "Identification for Development. Data Protection and Privacy Laws", 2025. [Online]. Available: https://id4d.worldbank.org/guide/data-protection-and-privacy-laws [Accessed: Aug 08, 2025].

[2] European Commission, "Legal Framework of EU Data Protection", 2025. [Online]. Available: https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en [Accessed: Aug 08, 2025].

[3] International Comparative Legal Guide, "Data Protection Laws and Regulations—Ukraine", *Data Protection Laws and Regulations 2025*, July 21, 2025. [Online]. Available: https://iclg.com/practice-areas/data-protection-laws-and-regulations/ukraine [Accessed: Aug 08, 2025].

[4] V. Yermachenko, "Theory and Practice of Public Management of Smart Infrastructure in the Conditions of the Digital Society' Development: Socio-economic Aspects", *Economic Affairs*, Vol. 68, No. 1, 2023. https://doi.org/10.46852/0424-2513.1.2023.29

[5] S. A. Pragma, "Personal Data Processing Policies" [Privacy policy], March 1, 2023. [Online]. Available: https://www.pragma.co/privacy-policy [Accessed: Aug 08, 2025].

[6] Nortal, "X-Road: Estonia's Digital Backbone", June 10, 2022. [Online]. Available: https://nortal.com/insights/x-road-estonias-digital-backbone [Accessed: Aug 08,2025].

[7] O. Bulavina, D. Kyslenko, V. Hmil-Chuprina, S. Artemenko, & L. Cherednyk, "Efficiency of Virtual Reality Technologies in the Development of Strategic Thinking of Future Professionals", *Journal of Theoretical and Applied Information Technology*, Vol. 102, No. 18, 2024, pp. 6750–6760. https://www.jatit.org/volumes/Vol102No18/15Vol102No18.pdf

[8] Y. Ishchenko, V. Artemov, P. Syniavskyi, M. Shilin, & V. Ahmadov, "The Impact of Immigration Law and Policy on Crime Rates in Immigrant Communities in the United States", *Pakistan Journal of Life and Social Sciences (PJLSS)*, Vol. 22, No. 2, 2024. https://doi.org/10.57239/pjlss-2024-22.2.00368

[9] N. Lytvyn, H. Andrushchenko, Y. V. Zozulya, O. V. Nikanorova, L. M. Rusal, "Enforcement of Court Decisions as a Social Guarantee of Protection of Citizens Rights and Freedoms", *Prawo i Więź*, Vol. 1, No. 39, 2022, pp. 80–102. https://doi.org/10.36128/priw.vi39.351

[10] M. Potwora, O.Vdovichena, D. Semchuk, L. Lipych, & V. Saienko, "The Use of Artificial Intelligence in Marketing Strategies: Automation, Personalization and Forecasting", *Journal of Management World*, Vol. 2, 2024, pp. 41–49. https://doi.org/10.53935/jomw.v2024i2.275

[11] Estonian Transport Administration, "Processing of Personal Data", May 26, 2023. [Online]. Available: https://transpordiamet.ee/en/administration-news-and-contact/administration/processing-personal-data [Accessed: Aug 08, 2025].

[12] E. Olca, & O. Can, "DICON: A Domain-Independent Consent Management for Personal Data Protection", *IEEE Access*, Vol. 10, 2022, pp. 95479–95497. https://doi.org/10.1109/access.2022.3204970

[13] M. Joo, & H. Kwon, „Comparison of Personal Information De-Identification Policies and Laws Within the EU, the US, Japan, and South Korea", *Government Information Quarterly*, Vol. 40, No. 2, 2023, Article 101805. https://doi.org/10.1016/j.giq.2023.101805

[14] A. Krupnova, "Legal Regulation of Information Security in Ukraine", *Analytical and Comparative Jurisprudence*, Vol. 5, 2023, pp. 348–354. https://doi.org/10.24144/2788-6018.2023.05.62

[15] D. Utegen, & B. Z. Rakhmetov, "Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models", *Journal of Digital Technologies and Law*, Vol. 1, No. 3, 2023, pp. 825–844. https://doi.org/10.21202/jdtl.2023.36

[16] W. R. Haryadi, "Consumer Protection of Personal Data in the Era of the Industrial Revolution", *Journal of Legal and Cultural Analytics*, Vol. 3, No. 1, 2024, pp. 89–104. https://doi.org/10.55927/jlca.v3i1.8150

[17] A. G. Duisenkul, D. A. Ospanova, G. D. Taigamitov, & S. M. Madykhan, "Legal Regulation of State Electronic Services: Relevant Issues and Ways of Improvement", *Data Science Journal*, Vol. 22, 2023. https://doi.org/10.5334/dsj-2023-015

[18] A. Calvi, "Data Protection Impact Assessment under the EU General Data Protection Regulation: A Feminist Reflection", *Computer Law & Security Review*, Vol. 53, 2024, Art. 105950. https://doi.org/10.1016/j.clsr.2024.105950

[19] S. Hanisch, J. Todt, J. Patino, N. Evans, & T. Strufe, "A False Sense of Privacy: Towards a Reliable Evaluation Methodology for the Anonymization of Biometric Data", *Proceedings on Privacy Enhancing Technologies*, Vol. 2024, No. 1, 2023, pp. 116–132. https://doi.org/10.56553/popets-2024-0008

[20] P. Delgado-Santos, et al., "SwipeFormer: Transformers for Mobile Touchscreen Biometrics", *Expert Systems with Applications*, Vol. 237, 2023, p. 121537. https://doi.org/10.1016/j.eswa.2023.121537

[21] M.S.M. Alfatni, A. M. Ebiad, M. A. Al-Bahbouh, L. A. Esmeda, "Electronic Health File System based on Fingerprint Sensor Technology", *Journal of Advanced Research in Applied Sciences and Engineering Technology*, Vol. 33, No. 2, 2023, pp. 209–224. https://doi.org/10.37934/araset.33.2.209224

[22] MiniTAB, "Data Analysis, Statistical & Process Improvement Tools", 2025. [Online]. Available: https://www.minitab.com/en-us/ [Accessed: Aug 08, 2025].

[23] European Commission, Directorate-General for Justice and Consumers, *Commission Staff Working Document: Country Reports on the Functioning of the Adequacy Decisions Adopted under Directive 95/46/EC*, SWD (2024) 3 final, CELEX: 52024SC0003, Jan 15, 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024SC0003 [Accessed: Aug 08, 2025].

[24] European Data Protection Board, "Annual Report 2023 of Schengen Information System Statistics", February 26, 2025. [Online]. Available: https://www.edpb.europa.eu/our-work-tools/our-documents/csc-documents/annual-report-2023-schengen-information-system_en [Accessed: Aug 08, 2025].

[25] European Data Protection Board, *Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR (Version 1.0)*, Oct 8, 2024. [Online]. Available: https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf [Accessed: Aug 08, 2025].

[26] Bundesamt für Sicherheit in der Informationstechnik, *IND 2.7: Safety Instrumented Systems (IT-Grundschutz-Kompendium Edition 2023)*, 2023. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/08_IND_Industrielle_IT/IND_2_7_Safety_Instrumented_Systems_Edition_2023.pdf?__blob=publicationFile&v=3 [Accessed: Aug 08, 2025].

[27] X-Road Project, "X-Road Documentation", 2025. [Online]. Available: https://docs.x-road.global [Accessed: Aug 08, 2025].

[28] Ministerstwo Cyfryzacji, „EPUAP – Strefa Klienta", 2025. [Online]. Available: https://epuap.gov.pl/wps/portal [Accessed: Aug 08, 2025].

[29] Government of Croatia, "Gov.hr – Portal of the Government of the Republic of Croatia", 2025. [Online]. Available: https://gov.hr [Accessed: Aug 08, 2025].

[30] State Services Online, "Diia", 2025. [Online]. Available: https://diia.gov.ua/en [Accessed: Aug 08, 2025].

[31] OECD, "Digital Government", 2025. [Online]. Available: https://www.oecd.org/en/topics/digital-government.html [Accessed: Aug 08, 2025].

[32] European Commission, "Estonia: Digital Public Administration Factsheet 2024 (NIFO–DPAF Estonia, final version)", *Interoperable*

Europe, 2024. [Online]. Available: https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/NIFO_2024%20DPAF_Estonia_vFinal.pdf?utm_source=chatgpt.com [Accessed: Aug 08, 2025].

[33] United Nations Development Programme, "2024 Provincial Governance and Public Administration Performance Index (PAPI) Report. UNDP Vietnam", April 15, 2025. [Online]. Available: https://www.undp.org/vietnam/publications/2024-provincial-governance-and-public-administration-performance-index-papi-report [Accessed: Aug 08, 2025].

[34] Visual Paradigm, "Business Process Modelling with Powerful BPMN Software", 2024. [Online]. Available: https://www.visual-paradigm.com/features/bpmn-diagram-and-tools/ [Accessed: Aug 08, 2025].

[35] STP Informationstechnologie GmbH, "Legal Twin: Case Knowledge – Use Legal Twin for Advoware to Dramatically Accelerate Access to Client Information and Clear Case Overviews", 2025. [Online]. Available: https://www.stp.one/en/use-cases/legal-twin-for-advoware [Accessed: Aug 08, 2025].

[36] Digital Twin Consortium, "Legal", 2025. [Online]. Available:https://www.digitaltwinconsortium.org/legal/ [Accessed: Aug 08, 2025].

[37] European Commission, Directorate-General for Climate Action, Ricardo Energy & Environment, & E4tech, *Determining the Environmental Impacts of Conventional and Alternatively Fuelled Vehicles through Life Cycle Assessment: Summary of the Delphi Survey Round 1 Responses (Appendix A21),* 2020. [Online]. Available: https://climate.ec.europa.eu/document/download/e8d1c9ff-4661-46cd-b5ac-1d53440b9a57_en?filename=2020_study_appendix_a21_en.pdf [Accessed: Aug 08, 2025].

[38] Stat59, "Web-Based Statistics Software for Delphi Method", 2025. [Online]. Available: https://www.stat59.com/about/delphi-method-software [Accessed: Aug 08, 2025].

[39] University of Turku Futures Research Centre (eDelphi), "Delphi Method Software", 2025. [Online]. Available: https://www.edelphi.org/ [Accessed: Aug 08, 2025].