

Organizational and Legal Aspects of Internal Control over Personal Data Processing in the Telecommunications Industry: The Russian Experience

Pelkova Svetlana Vladimirovna

Candidate of Economic Sciences,
Associate Professor
Department of Economic Security,
System Analysis and Control,
University of Tyumen, Tyumen,
E-mail: s.v.pelkova@utmn.ru
ORCID: 0000-0001-5367-2861

Tarkhanova Elena Aleksandrovna

Candidate of Economic Sciences,
Associate Professor
Department of Economics and Finance,
University of Tyumen, Tyumen,
E-mail: e.a.tarkhanova@utmn.ru
ORCID: 0000-0002-8292-4842

Tarkhanova Aleksandra Vladimirovna

4th year bachelor
School of Law and Management,
University of Tyumen, Tyumen,
E-mail: a.v.tarkhanova@mail.ru
ORCID: 0009-0001-3379-6186

Fricler Anhelica Viktorovna

Candidate of Economic Sciences,
Associate Professor
Department of Economics and Finance,
University of Tyumen, Tyumen,
E-mail: a.v.fricler@utmn.ru
ORCID: 0000-0003-0077-1115

Mazikova Ekaterina Vladimirovna

Candidate of Economic Sciences,
Associate Professor
Academic Department,
School of Computer Science,
University of Tyumen, Tyumen,
E-mail: e.v.mazikoova@utmn.ru
ORCID: 0000-0002-3673-8977

Abstract

This article presents the organizational and legal aspects of the internal control system for personal data processing amid the transformation of telecommunications companies into multifunctional digital ecosystems. The full life cycle of personal data is analyzed, and a classification by degree of criticality and risk is proposed. To effectively prevent threats, the necessity of implementing a risk-oriented "Three Lines of Defense" model is substantiated. The authors systematize the regulatory and legal framework governing personal data processing in Russia, with an emphasis on industry-specific legislation and regulatory requirements. A comparative analysis of federal legislation and the European GDPR is also conducted, identifying the applied challenges of forming a hybrid compliance framework. In assessing the market environment, it is established that the Russian telecommunications market constitutes an oligopoly with a high concentration around the "big four" companies. Based on data from the four largest telecom operators, an assessment is made of the maturity of control procedures at all stages of personal data processing. The findings of this study can be used to improve the effectiveness of risk management systems in the telecommunications industry and to adapt compliance procedures to the current challenges of the digital economy. The article is intended for specialists in information security, internal audit, and corporate governance.

Introduction

Over the past decade, Russia's telecommunications industry has evolved from providing basic communication services to building multifunctional digital ecosystems (Tyshetskaya et al., 2026). This dynamic is explained not only by growing consumer demand but also by continuous technological development. In the modern sense, a digital ecosystem is an integrated environment in which a user, through single sign-on based on their personal data, gains access to educational, financial, entertainment, and other services (Kuzminov et al., 2026). However, the active expansion of ecosystems through the attraction of new partners and the creation of specialized business units creates a

fundamentally new problem. Each new link in this chain increases the number of points of interaction with personal data, thereby complicating the telecom operator's infrastructure (Kumara, 2025). This gives rise to unprecedented risks for the telecom operator's economic security. Reputational damage, subscriber churn, litigation costs, multimillion-dollar fines, and loss of investment appeal all have lasting negative consequences for both the internal control system and the economic security of the telecom operator.

There is also a tightening of state regulation regarding telecom operators' use of customers' personal data (Cheng & Bilal, 2025). Recent years have been marked by increasing amounts of administrative fines and the application of increasingly stringent sanctions by regulators for personal data breaches, which requires telecom operator managers to establish adaptive organizational and legal internal control (Bouraffa & Hui, 2025). Today, a problem area for operators is bringing internal local regulatory acts into compliance with the constantly changing requirements of regulatory bodies and federal legislation. Classical methods of ensuring information security used by telecom operators, aimed only at external protection, are not fully effective under conditions of telecom operator ecosystem development (Kumara, 2025). Large-scale digitalization of the telecommunications industry is transforming personal data from a technological resource into a core asset that requires systematic risk management (Sahnouni & Kadri, 2025). A need arises to protect the personal data not only of customers but also of employees, counterparties, and partners of telecom operators. At the same time, it becomes more difficult to determine the precise boundaries of responsibility among participants in business processes, there is no unified approach to systematizing personal data by criticality level, and the process of timely detection and localization of incidents becomes more complex. All of this is compounded by an insufficient level of awareness among telecom operator personnel regarding information security standards and rules. Therefore, it becomes essential to implement a risk-oriented model of internal control that could adapt to the large-scale use of digital services. The specific features of the telecommunications industry

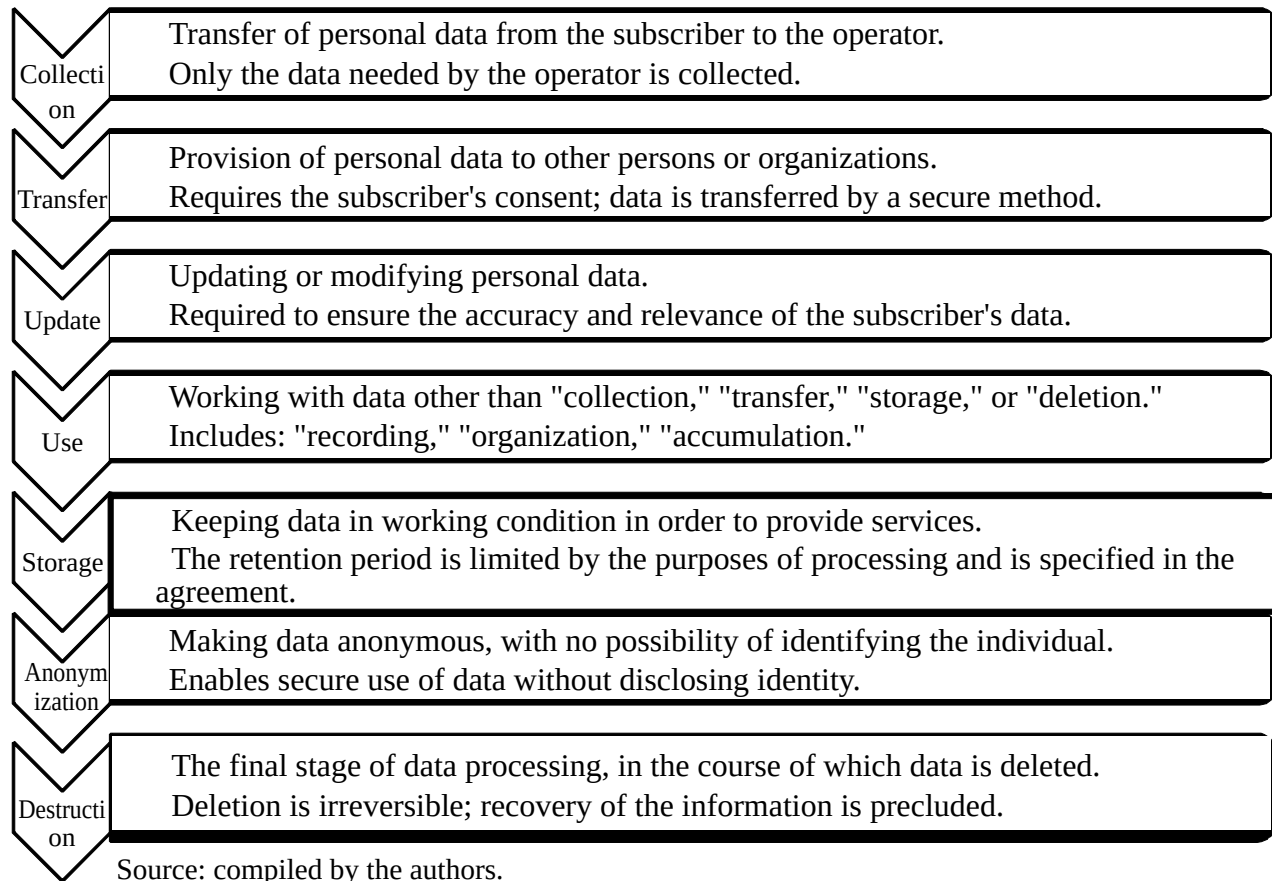
require communication operators to build hybrid internal control systems based on a combination of regulatory and legal compliance with digital solutions (Eulerich et al., 2025). The effective implementation of such strategies correlates with a clear distribution of functions among security divisions, the legal department, and the operational unit. Under conditions of continuous growth in the volume of personal data processed, classical internal control and audit are not fully effective in preventing information threats (Boubouh & Ghanim, 2025). Therefore, the challenges that arise require a thorough study of the theoretical aspects and practical tools of organizing internal control, which will allow telecom operators both to reduce regulatory and operational risks and to build a pool of trust-based relationships with customers regarding digital products and services.

Literature Review

Under conditions of the rapid development of information technology, every company, including telecom operator companies, processes the personal data of employees, counterparties, customers, visitors, and so on (Yas et al., 2025). Accordingly, companies act as personal data operators and are obligated to comply with the requirements of legislation in the field of personal data processing and ensuring their security (Kun, 2025). If violations are identified in the processes of collecting, processing, using, and storing personal data, a company may incur not only material but also reputational damage, which will subsequently have a negative effect on its operations (Al-Obaidi et al., 2025).

Personal data is any information relating to a directly or indirectly identified or identifiable natural person (Mayuna et al., 2025). The set of stages of personal data processing from the moment of collection to destruction is called the personal data life cycle (Lim & Oh, 2025) (Fig. 1). This term denotes all actions that may be performed with personal data after their transfer to the operator or to another party carrying out processing on the operator's instructions.

Figure 1. Stages of the Personal Data Life Cycle



Understanding the personal data life cycle helps ensure competent management of data flows at every stage. However, not all data can be classified as high-risk (Mangala, 2026). To build an effective protection system,

gradation of the data is necessary (Table 1). Central to the telecom operator's ecosystem is classification by degree of criticality and associated risks.

Table 1: Classification of Personal Data in the Telecom Operator's Ecosystem by Degree of Criticality and Associated Risks

Category of Personal Data	Type of Personal Data	Risk Level	Nature of Threat and Potential Damage
Special categories	Biometric data, health data	Very high	Irreversibility of compromise. Maximum fines, irreparable reputational damage.
Basic identifiers	Full name, passport data, taxpayer ID (INN), social insurance number (SNILS), phone number	High	Direct threat of identity fraud, identity theft, unauthorized access to other services. Significant financial and reputational losses.
Behavioral and digital traces	Call history and metadata, real-time geolocation, website visit history (within legal limits), traffic consumption patterns	High-medium	Risks of privacy violations, unethical use. Damage — loss of trust, litigation by data subjects, regulatory restrictions on processing.

Category of Personal Data	Type of Personal Data	Risk Level	Nature of Threat and Potential Damage
Derived and analytical data	Scoring points (credit, loyalty), customer segments and profiles	Medium	Risks of incorrect, biased, or discriminatory algorithms. Damage — flawed business decisions, reputational losses, financial losses from ineffective marketing campaigns.
Publicly available data	Data made publicly available by the data subject themselves (public social media posts, data in open registers)	Medium-low	Risk of excessive public exposure, disclosure of information from a restricted-access account. Damage — mainly reputational, in cases of violation of ethical use principles.

Source: compiled by the authors.

In the digital ecosystem of a telecom operator, personal data acquires multidimensional value, as well as a high degree of criticality and risk (Khan et al., 2025). This indicates a direct correlation between the security of the telecom operator and the scale of damage in the event of compromise or unlawful processing of personal data.

Threats and vulnerabilities in personal data processing are continuously expanding and radically complicating the attack surface of internal systems. Risks cease to be local and become systemic, requiring a comprehensive analysis of threat sources and internal vulnerabilities (Fawareh & Saeed, 2026).

Threats to personal data security originate from various spheres, each of which requires specific countermeasures (Țălu, 2025). Sources of threats may be:

- external: targeted cyberattacks, competitor activity, regulatory actions, global sanction-related risks.
- internal: employee errors and negligence, malicious insider actions, outdated or non-compliant regulations.

To prevent the emergence of threats at every stage of personal data processing, a risk-oriented system of protection and internal control assessment must be built, in which resources are focused on the most valuable and vulnerable categories of information (Rusu & Mantulescu, 2025). This system is structured using the "Three Lines of Defense" model (Rieg et al., 2025):

- first line – operational management – the direct management of operational risks and the execution of control procedures.
- second line – risk management and internal control – the

units that develop standards, coordinate, and evaluate the work of the first line.

- third line – internal audit – an independent and objective assessment of the first two lines, providing an independent evaluation of the effectiveness of the internal control and risk management system, including in the area of personal data processing.

The effectiveness of the model depends on a clear delineation of roles and well-established interaction among the lines of defense (Rieg et al., 2025). This makes it possible to assess how productively the system functions and whether the established protective measures are meeting their objectives. Evaluation activities include analysis of:

- the structural features of the internal control system for personal data;
- the sufficiency of internal documentation and its compliance with the requirements set out in regulatory and legal acts;
- the technological aspects of processing subscribers' personal data and the composition of the software and technology base;
- the correct determination of the level of protection for personal data and the methods of protection for each;
- the level of staff training, awareness, and distribution of responsibility;
- the status of work performed to maintain the stable functioning of the internal control system.

To reach a final verdict on the effectiveness of the system's

operation, specialists must analyze compliance with organizational and technical requirements and test the implemented protective measures against potential threats (Rieg et al., 2025). Following each test and stage, protocols are completed, and the conclusions are reflected in the final report.

Organizational and technical requirements are fulfilled within the framework of the personal data life cycle (Emon, 2026). Control is exercised through a set of organizational and technical measures. These include documents, regulations, and software and hardware tools, by means of which full control over the process of identifying the stages of the personal data life cycle is implemented (Emon, 2026). Responsibility rests with the head of the telecom operator, as well as with the person formally designated as responsible for personal data processing and the information security service.

Overall, personal data is the central object of risk management in the digital ecosystem (Mahendra & Oktaviani, 2025). Its protection is not simply a set of assorted measures, but a coordinated complex of methods and actions capable of regulating the smooth operation of each stage. A violation at any stage of control indicates the ineffectiveness of the entire system and calls into question the feasibility of its application at subsequent stages (Yu et al., 2026). This underscores the necessity of working with personal data within a strictly defined legal framework. Personal data is transferred by the subscriber at the stage of contract conclusion. The operator and its ecosystem partners use this data to provide services throughout the entire period of subscriber service (Kuzovkova et al., 2025). The operator is obligated to ensure the security of personal data processing through coordinated work in accordance with federal legislation and other regulatory and legal acts (Table 2).

Table 2: Regulatory and Legal Framework Governing Personal Data

Documents	Areas of Regulation
Federal laws	1. Establish the basic legal foundations for the protection of personal data and the rights and freedoms of citizens in the course of its processing. 2. Define the procedure for the functioning of the digital environment, the rules for data anonymization, and the status of information system operators. 3. Establish sector-specific obligations for communication operators regarding subscriber identification and fraud prevention. 4. Set general mandatory requirements for the organization and implementation of an internal control system within companies.
Subordinate legislation (government resolutions, departmental orders, Bank of Russia regulations)	1. Establish specific requirements for data protection in information systems, database classification, and the accounting and use of cryptographic protection tools. 2. Define the rules for building communication networks and ensuring the security of transmitted voice and text data. 3. Regulate the procedure for conducting inspections of operators, the application of a risk-oriented approach, and compliance with licensing conditions. 4. Set industry standards and Bank of Russia recommendations on risk management and internal control (including for public companies and financial subsidiary structures).

Source: compiled by the authors.

In international practice, a regulatory act known as the "General Data Protection Regulation" (GDPR) is used. This is a European Union regulatory act that defines the rules for the collection, processing, storage, and dissemination of personal data within its territory. The application of the GDPR to the activities of Russian telecom operators is determined not by the territorial principle but by the nature of the data processing. In accordance with Article 3 of the GDPR, the regulation applies if the processing of personal data concerns data

subjects located in the EU, even if the operator itself is registered in another jurisdiction.

For a telecom operator developing a service ecosystem, compliance with both Russian and European personal data legislation becomes critically important. This is due to the presence of subscribers who are EU citizens, the use of services and infrastructure located in Europe, or cooperation with international partners. A comparative analysis of Russian federal legislation and the GDPR is presented in Table 3.

Table 3: Comparative Analysis of Russian Federal Personal Data Legislation and the GDPR

Criterion	Federal Law of the Russian Federation "On Personal Data"	General Data Protection Regulation (GDPR)	Practical Challenges for the Telecom Operator's Ecosystem
1. Legal basis for processing (interpretation of consent)	A clear list of grounds. Consent must be specific and informed.	Consent must be freely given (cannot be made conditional on the core service), specific, and informed.	Conflict of "non-free" consent: marketing consent cannot be "tied" to the main contract. Separate consent forms are required for different services.
2. Right to data portability	The right to obtain one's data is established, but not the right to transfer it to another operator.	The right to receive data in a machine-readable format for transfer to another operator is explicitly established.	Technological challenge: tools for data export need to be developed, creating a cost imbalance (no such obligation exists under federal law).
3. Time limits for responding to data subject requests	30 calendar days, with a possible extension of up to 30 days.	1 month (30 calendar days), with a possible extension of up to 2 months.	Risk of GDPR violation: internal regulations configured for federal law may fail to account for the possibility of an extension. Flexible processes accommodating both scenarios are required.
4. Liability and fines	Administrative fines for legal entities. Focus on formal compliance.	Administrative fines. Focus on demonstrating effective compliance.	Existential risks: GDPR violations carry enormous fines. More mature and costly data management systems are required.
5. Accountability principle	Implemented through the obligation to notify supervisory authorities of the commencement of processing and to provide documents upon request.	A key principle. The operator is obligated to comply not only with the requirements but also to document proof of compliance (registers, policies).	Differing depth of compliance: operating in the international market requires implementing costly compliance management systems (GRC systems), since simple notification of the supervisory authority is not sufficient.
6. Requirements for data protection by default and by design (Privacy by Design/Default)	Protection requirements are determined by the security level of the personal data.	A mandatory requirement. The operator is obligated to implement protective measures both at the system design stage and by default.	High development cost: the ecosystem is constantly creating new products. Embedding these systems into data requires additional investment in secure development.
7. Procedure for incident notification	Obligation to notify supervisory authorities of breach incidents. Deadlines are being tightened (24 hours).	A two-tier system: notification of the supervisory authority within 72 hours. Also notification of data subjects if the risks to their rights are high.	Jurisdictional chaos: the operator must simultaneously comply with different notification procedures. GDPR requires dual dialogue with both the state and the data subject, which is not always provided for by local regulations.

Source: compiled by the authors.

The main difficulty in building a unified control system within the ecosystem of a telecom operator, operating under the simultaneous effect of Russian and international legislation, lies in the fact that these two regimes require different compliance structures (Umanskiy & Tikhvinskiy, 2025). These discrepancies manifest at several levels: first, in the interpretation of consent — while Russian legislation permits obtaining "bundled" consent for all ecosystem services, international legislation requires separate consent for each processing purpose, which compels the control system to differentiate data flows. Second, there is a conflict in response times to data subject requests, which requires the internal control system to be able to operate under different time regimes. Third, approaches to technical protection differ.

Thus, the regulatory framework presented, comprising sector-specific federal legislation and detailed implementing orders, together with the international GDPR standard, forms a multilayered legal environment for building an internal control system within the telecom operator's ecosystem.

Methodology

The research methodology is based on a comprehensive approach combining a set of theoretical and empirical methods, ensuring a systematic analysis of the organizational and legal aspects of internal control over personal data processing in the Russian telecommunications industry. The study applies a synthesis of qualitative and quantitative methods of data collection

and processing, which ensures a high degree of research accuracy. The empirical research methods are based on the analysis of statistical data on the dynamics of the telecommunications market for 2022–2025, including market volume, growth rates, and service structure. The CR3 and HHI indices are used to assess the level of market concentration, which makes it possible to confirm the oligopolistic structure of the industry. An analysis is conducted of the internal control practices of the largest Russian telecom operators comprising the "big four," which makes it possible to assess the maturity of control procedures, including the presence of centralized security systems, the use of certified cryptographic protection tools, the maintenance of personal data registers, and the frequency of staff training. The data sources include regulatory and legal acts, scientific literature, statistical reports, operators' financial statements, as well as empirical data on internal control practices.

Research Results

The telecommunications services market of the Russian Federation constitutes a complex, multilevel system currently undergoing active transformation. The scale of the market, its competitive structure, and technological trends directly determine the volume of personal data processed, the number of data collection points, and the potential risks associated with information leaks.

The Russian telecommunications market for 2023–2025 demonstrates steady positive dynamics, presented in Table 4.

Table 4: Dynamics of the Volume of the Russian Telecommunications Services Market, 2022–2025

Indicator	2022	2023	2024	2025
Market volume, billion rubles	1,806.5	1,951.3	2,096.4	2,278.3
Absolute growth, billion rubles	—	144.8	145.1	181.9
Growth rate (% , vs. prior year)	—	108.0	107.4	108.6
Growth increment (% , vs. prior year)	—	+8.0	+7.4	+8.6

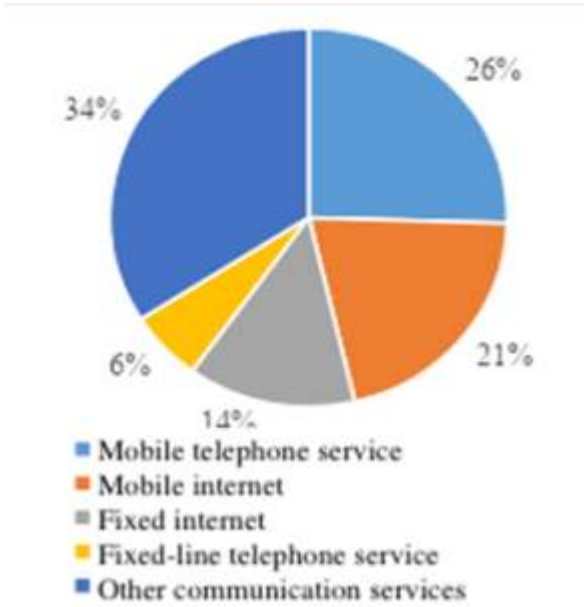
Source: compiled by the authors.

The volume of the telecommunications services market in 2025 increased by 8.6%, reaching 2,278.3 billion rubles. It should be noted that the growth rate in 2025 was the highest for the period under study, which is attributable to the high level of mobile and internet usage, as well as the demand for digital services. The share of telecom services in Russia's GDP within the structure of the "Information and Communication" sector stood at 3.8% in 2025. It should be noted that the share of communication services in Russia's GDP does not occupy a leading position within the structure, and even a slight increase or decrease in the share of telecommunications services does not reflect its strategic role as an infrastructural foundation for the entire national economy. Therefore, the significance of this study lies at the level of the individual economic entity, namely telecom operators, rather than the country as a whole.

The market structure, presented in Figure 2, shows a stable dominance of the "other communication services" segment.

The "other communication services" segment includes specialized telecommunications applications, messengers and social networks, voice-over-internet technologies, pay TV, and cloud services. The online cinema market deserves separate mention, as it is comparable in scale to the TV services segment.

Figure 2. Structure of the Telecommunications Services Market by Type, 2025



Source: compiled by the authors.

The Russian cellular communications market is a classic example of an oligopoly, dominated by four key federal operators. The "big four" operators (ranked from first to fourth tier) control an overwhelming share of the market (Table 5).

Table 5: Performance Indicators of the Largest Operators, 2025

Operator	Revenue, billion rubles	Revenue growth, %	Subscriber base, million people	Market share, %
Tier-1 telecom operator	476.8	3.9	81.6	31
Tier-2 telecom operator	525.6	7.9	79.4	29
Tier-3 telecom operator	334.7	7.2	48.9	15
Tier-4 telecom operator	306.4	10.3	48.9	15

Source: compiled by the authors.

The tier-2 telecom operator is the leader in revenue and revenue growth. However, the tier-1 telecom operator has the largest subscriber base and is the second-largest company by revenue, yet has the lowest revenue growth. Nevertheless, these companies maintain the market's oligopoly. This is confirmed by the CR3 concentration

index and the Herfindahl-Hirschman Index (HHI) — indicators used to assess the level of market concentration and the degree of industry monopolization (Table 6).

Based on the assessment of market concentration, it can be said that the market share held by the "big four" demonstrates a high level of concentration. The combined

share of the four companies is 90% of the market, according to the CR3 concentration index. The Herfindahl-Hirschman Index (HHI) stands at 9,000, which corresponds

to a high level of concentration and confirms the companies' oligopoly.

Table 6: Market Concentration Level and Degree of Industry Monopolization Among Telecom Operators

Operator	Market share, %	CR3 concentration index	Herfindahl-Hirschman Index (HHI)
Tier-1 telecom operator	31	90	9,000
Tier-2 telecom operator	29		
Tier-3 telecom operator	15		
Tier-4 telecom operator	15		

Source: compiled by the authors.

The companies' oligopoly creates difficulties for new telecom operators entering the market. This gives rise to barriers to entry, namely: strict licensing policy and a high level of investment in spectrum resources, the capital intensity of infrastructure, and the enormous scale of subscriber bases. Nevertheless, virtual operators are experiencing a certain degree of development, though they do not create real competition for the "big four," since the entire infrastructure is occupied by the large companies on which the development of the whole industry depends. In addition to the established competitive structure, the trends of digital transformation constitute the most important factor determining the industry's development.

An analysis of the activities of the "big four" operators makes it possible to identify three key trends in digital transformation that are directly relevant to the internal control system for personal data:

1. Shift from voice services to data transmission. Traditional voice communication has ceased to be the main growth driver, having been replaced by mobile internet traffic. Growth is also primarily driven by data consumption, namely social networks and messengers, application updates, and cloud services.
2. Development of ecosystem models. The "big four" operators are transforming into digital ecosystems, offering customers financial services, cloud services, cybersecurity, and advertising platforms.

3. Investment in new technologies. Despite difficulties with foreign equipment and software, telecom operators are investing in high-speed networks and cloud platforms, as well as in cybersecurity, thereby advancing the IT industry and the modernization of telecom services.

Today, the scale of personal data processing in the telecommunications industry is extremely high. The combined subscriber base of the four federal operators exceeds 200 million active subscribers, which significantly surpasses the population of Russia. Each operator accumulates data on subscribers' actions, geolocation, preferences, and creditworthiness. At the same time, data collection points are multiplying many times over due to the development of ecosystem services. These volumes of data processing automatically increase the risk of information compromise. The market consequences of data breaches for operators are critical, entailing administrative fines, reputational losses, subscriber churn, and an increase in class-action litigation practices. The foreign context also confirms the tightening of requirements for personal data protection, which carry colossal fines for telecom operators under the GDPR law.

The analysis of the internal control system for personal data processing was conducted using the example of three of the largest operators in the Russian telecom industry, and is justified by several factors. First, these companies are part

of the "big four" communication operators, whose combined subscriber base exceeds 200 million subscribers. Second, all three operators are actively developing digital ecosystems that include financial services, cloud platforms, and cybersecurity products, which creates a multiple increase in personal data collection points and complicates the internal control system. Third, the availability of open financial reporting makes it possible to analyze the maturity of control procedures, identify common industry-wide problems, and determine best practices in the field of personal data protection. It should be noted that it is

precisely the companies under study that most frequently appear in incident statistics related to personal data breaches, which makes them representative for assessing the vulnerability of the internal control system and for developing practical recommendations for strengthening it.

A comparative analysis of the organizational and technical measures at each stage of the personal data life cycle of the companies under study makes it possible to identify common features and notable differences in the approaches of different operators (Table 7).

Table 7: Maturity of Control Procedures Among the Largest Telecom Operators

Criterion	Content of Control Procedures
Presence of a centralized security system	Data leak prevention system, anomalous activity monitoring system, round-the-clock monitoring and management of personal data, threat detection analytics, high-throughput traffic security gateway.
Use of certified cryptographic protection tools	Encryption of communication channels and stored personal data, security system for communication channels during data collection over the internet, secure communication channels, cloud-based data cybersecurity service.
Existence of a separate personal data register with designated responsible persons	Verification of the existence and correctness of consent to personal data processing, appointment of a person responsible for organizing personal data processing, approval of the list of employees with access to personal data, personal data classification commission, accounting of physical media containing personal data.
Frequency of staff training	Conducting briefings, completion of a log with employee signature following the session, periodic employee training.
Transparency for the subscriber	Personal account — a system for tracking changes to personal data, control over access rights to modify personal data, backup of personal data, enabling the data subject to update data through customer service, account management, self-service portal, providing the ability to review personal data and make corrections.

Source: compiled by the authors.

The largest telecom operators demonstrate a high level of maturity in matters of personal data protection. The operators use various tools for monitoring and preventing threats. All leading companies maintain personal data registers with designated responsible persons, which indicates compliance with legislative requirements. A common area for improvement remains the frequency of staff training, as it tends to be formal in nature and lacks mandatory testing, which may reduce the overall effectiveness of the internal control system.

Overall, the organizational and technical control measures

applied at every stage of personal data handling make it possible to minimize the risks of leaks, unauthorized access, and unlawful processing. This, in turn, confirms that all three operators can be considered reliable partners — for ordinary people, for business, and for the state. Nevertheless, even with such a high level of maturity in control procedures and compliance with all regulatory requirements, certain risks still remain within the internal control systems of telecom operators. The realization of these risks may result in information leaks, fines from regulatory bodies, reputational losses, and direct financial damages.

Discussion and Conclusions

The transformation of telecommunications companies from communication operators into multifunctional digital ecosystems contributes to the growing complexity of their organizational and technical infrastructure and, accordingly, to the creation of entirely new risks to their economic and information security. The increase in the number of partners of telecom operators and the introduction of digital products and services undoubtedly contribute to the growth in the number of points of interaction with customers' personal data, while the frequency of cyberattacks on this personal data is also increasing. Information leaks, regulatory sanctions, and litigation costs can inflict irreparable reputational and financial damage, as well as reduce the investment appeal of a telecom operator. The study conducted confirms the fact that personal data is a key object of risk management in the digital ecosystem of telecom operators. Building an effective internal control system requires a differentiated approach to information management based on its gradation by level of criticality. The assessment of the personal data life cycle showed that compliance procedures must be end-to-end in nature and cover all stages: from the moment consent is obtained to complete deletion or anonymization. The implementation of the risk-oriented "Three Lines of Defense" model ensures a clear distribution of authority among the operational unit, the compliance service, and internal audit. The specific nature of the ecosystem environment requires a move away from purely formal compliance with legislative requirements toward building a flexible and adaptive control system. The study of the regulatory and legal framework revealed gaps and legal conflicts that arise when attempting to apply classical regulatory norms to hybrid digital platforms. In particular, existing conflicts arise from differences in the interpretation of consent, response times to data subject requests, and requirements for ensuring data protection by default. Analysis of the market practices of the largest telecom operators demonstrated a high level of maturity in their technical means of threat prevention. The leading companies maintain complete personal data registers and designate responsible persons, which guarantees compliance with basic regulatory and legal acts. At the

same time, it was found that a common area for improvement across the industry remains the frequency and format of staff training on cybersecurity issues. The formal nature of briefings, without regular knowledge testing, reduces the overall level of protection against internal threats and employee negligence. To reduce risks, companies need to develop a corporate culture of information handling at all levels of management. The automation of data accounting, classification, and monitoring processes serves as a determining factor in the stability of control under conditions of the dynamic launch of new products. The methodological recommendations developed for conducting compliance control can be successfully extrapolated to other companies developing their own digital ecosystems. A promising direction for further research is the development and implementation of artificial intelligence algorithms for the automatic detection of anomalies and violations in personal data processing within ecosystems. Thus, only a comprehensive approach combining organizational, technical, and legal measures can ensure the reliability of the internal control system. The resulting control model makes it possible to achieve a balance between compliance with strict regulatory requirements and the preservation of high business process speed. Ultimately, the reliability of the internal control system becomes an important competitive advantage for a telecommunications company under conditions of large-scale digital transformation. Effective implementation of the solutions presented in this article will help reduce the likelihood of compliance risks materializing in the future.

References

- Al-Obaidi, B. S. H., Al-Kareem, R. S., Kadhim, A. T., & Korchova, H., 2025. The ripple effects of fraud on businesses: Costs, reputational damage, and legal consequences. *Encuentros. Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico.*, (23 (enero-abril)), pp. 345-371.
- Boubouh, I., & Ghanim, M., 2025. Internal Controls in the Digital Age: Simplification or Complication?. *International Journal of Research in Economics and Finance*, 2(2), pp. 149-163.

- Bouraffa, T., & Hui, K. L., 2025. Regulating information and network security: Review and challenges. *ACM Computing Surveys*, 57(5), pp. 1-38.
- Cheng, Y. W., & Bilal, A., 2025. Regulatory data privacy concerns in proliferating IoT era of telecommunication data monetisation: a systematic literature review. *Computing*, 107(9), p. 190.
- Emon, M. M. H., 2026. Navigating the digital labyrinth: Personal data privacy and security at individual and organizational levels. In *User-Centric Cybersecurity Implications for Sustainable Digital Transformation* (pp. 257-288). IGI Global Scientific Publishing.
- Eulerich, M., Bamberg, A., Bonrath, A., Kordes, J., & Wagener, M., 2025. How Deutsche Telekom Uses Emerging Technologies to Enhance the Internal Control System. *Journal of Emerging Technologies in Accounting*, 22(2), pp. 79-96.
- Fawareh, H., & Saeed, M., 2026. The Complex Dynamics of Network Security Threats that Effects Persons and Organizations Security. In *Artificial Intelligence for Sustainable Innovation Management and Risk Management: A Systems (and Network) Perspective*, pp. 2093-2113. Cham: Springer Nature Switzerland.
- Khan, M. A., Shah, M., & Ishaq, W., 2025. Towards a data-centric framework for 5G and beyond ecosystems. *Spectrum of Engineering Sciences*, pp. 272-285.
- Kumara, S., 2025. Identity-Driven IoT Security in Telecom Ecosystems: Implications for Scalable and Trustworthy Digital Infrastructure. *Int. J. Appl. Math*, 38(12s), pp. 2797-2816.
- Kun, E., 2025. Searching for the appropriate legal basis for personal data processing for cybersecurity purposes under the NIS 2 Directive: Legal obligation and/or legitimate interest?. *Computer Law & Security Review*, 56, 106098.
- Kuzminov, Y. I., Koshel, A. S., Kruchinskaia, E. V., & Dombaev, S. S., 2026. The Digital Ecosystem as a Novel Economic Phenomenon and Legal Concept. *BRICS Law Journal*, 13(2), pp. 5-36.
- Kuzovkova, T. A., Sharavova, O. I., Tikhvinskiy, V. O., & Devyatkin, E. E., 2025. Synchronization of Market, Production and Technological Capabilities of 5G and 6G Networks Based on Monetization Models. In *2025 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)* (pp. 1-7). IEEE.
- Lim, S., & Oh, J., 2025. Navigating privacy: A global comparative analysis of data protection laws. *IET Information Security*, 2025(1), 5536763.
- Mahendra, A., & Oktaviani, R., 2025. Legal Implications of Personal Data Protection in the National Digital Ecosystem after the Enactment of the Personal Data Protection Law: Examining the Urgency of Strengthening Data Security. *Journal of Lex et Justitia*, 1(2), pp. 38-56.
- Mangala, N., 2026. Responsible AI Data Architecture: Embedding GDPR and PII Compliance into MLOps Pipelines at Enterprise Scale. *Canadian Journal of Marketing Research*, 16(1), pp. 107-124.
- Mayuna, I. K., Dewantara, R., & Ruslijanto, P. A., 2025. Pseudonymization of personal data of crypto assets users: Issues of legal regulation in Indonesia. *Journal of digital technologies and law*, 3(2), pp. 275-303.
- Rieg, R., Vanini, U., & Gleißner, W., 2025. Risks, opportunities, and enterprise risk management. In *Enterprise Risk Management: A Modern Approach* (pp. 1-18). Cham: Springer Nature Switzerland.
- Rusu, D., & Mantulescu, M., 2025. Development of an application-based framework for information security management in SMEs. *Sustainability*, 17(18), p. 8314.
- Sahnouni, M., & Kadri, M., 2025. Investments in ICT in the Telecommunications Sector: A Strategic Imperative for Organizational Changes in Response to Market Transformations. *Financial Markets, Institutions and Risks*, 9(2), pp. 112-122.
- Țălu, M., 2025. Security and privacy in the IIoT: threats, possible security countermeasures, and future challenges. *Computing&AI Connect*, 2(1), pp. 1-10.

- Tyshetskaya, A., Vartanov, S., & Kalachikova, O., 2026. From banking and telephony to media: The case of Russian digital ecosystems. *World of Media. Journal of Russian Media and Journalism Studies*, 1, pp. 5-29.
- Umanskiy, R., & Tikhvinskiy, V., 2025, October. Designing a Business Model Controlling System for the Digital Ecosystem of a Mobile Network Operator. In *2025 International Conference on Engineering Management of Communication and Technology (EMCTECH)* (pp. 1-7). IEEE.
- Yas, H., Aldabbagh, Z., Khalifa, A. A., Faghiri, A., Bawazir, A. A., & Shwede, F., 2025. Role of artificial intelligence in the promotion of customer experiences: A legal administrative study and systematic review in the United Arab Emirates. *Humanities*, 6(4).
- Yu, Z., Xu, Z., & Qi, J., 2026. Data protection for persons with disabilities in AI-enabled assistive technologies: bridging gaps in China's legal framework. *AI and Ethics*, 6(4), p. 432.