Non-final version of Churshina, Anna and Kruglikova; Anna. The personal data architecture of Russia; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

THE PERSONAL DATA ARCHITECTURE OF RUSSIA

Anna Churshina and Anna Kruglikova

Abstract

As consumer demand and geopolitical evolutions continues to drive technology trends, the stakes for data processing have never been higher. In 2020, data privacy visibly became an even greater concern as many people had to move even more of their personal and professional lives online. The ever-changing privacy landscape and patchwork of compliance obligations globally will only continue to grow more complex and are likely to lead to increased regulatory scrutiny and potential enforcement actions despite best compliance efforts. As the privacy landscape evolves and lawmakers globally aim to find the balance between privacy rights, ease of doing business, and security needs, it is clear that regulation will continue to be a work in progress 2022 has prompted significant changes into privacy legislation that shaped Russian privacy framework with some of the amendments becoming effective in 2023. In this chapter, we will examine the current legal landscape governing data protection in Russia, explore the key local legislative requirements concerning data privacy and security and offer guidance on how to ensure regulatory compliance.

Non-final version of Churshina, Anna and Kruglikova; Anna. The personal data architecture of Russia; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

CONTENTS

Non-final version of Churshina, Anna and Kruglikova; Anna. The personal data architecture of Russia; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

1. THE PERSONAL DATA ARCHITECTURE OF RUSSIA

1.1. Preliminary Section: A Brief Overview of The Russian Legal System

1.1.1. General background

Russian legal structure developed at a fast pace during the 1990s. During this time, significant reforms were made to support the country's transition toward a market economy, including liberalization of markets and trade, privatization, and fiscal stabilization.

The Russian legal system is generally classified as a civil law system. It is based on the Constitution, federal and regional laws, and municipal acts. Primary legislation is supported by decisions of ministers, Russian Government decrees and Presidential executive orders.

The Constitution, which was adopted at the national referendum on December 12, 1993, states that both universally recognized principles of international law and international treaties to which Russia is a party are a component of the Russian legal system. Consequently, when an international treaty provides for provisions contrary to those envisaged in domestic law, the international treaty provisions shall prevail. At the same time, the Constitution takes precedence over any controverting statements of an international treaty.

The Russian Civil Code (the "Civil Code") sets out the main provisions of civil law, which are used by private individuals and businesses. A number of significant amendments to the Civil Code with regard to corporate law and contract law were introduced in September 2014 and June 2015. The key changes included the introduction of certain concepts into Russian law which have for a long time been common in international practice but had been previously missing in the Russian regulatory framework, such as the concept of warranties (an equivalent of warranties as used in contracts under English law), the concept of reimbursement of losses arising from the occurrence of certain circumstances or conditions specified in a contract (an equivalent of indemnity in English law), new types of civil law contracts, such as options and framework agreements, new mechanisms to ensure the performance of contractual obligations by the parties, and a few others. While the Civil Code does not explicitly address personal data, it contains provisions relevant to personal data processing, such as Article 152, which protects an individual's honor, dignity, and reputation. Inappropriate use of personal data can infringe upon these rights, potentially leading to claims for compensation.

Similarly, the Brazilian Civil Code includes specific provisions protecting privacy, such as Article 21, which declares the inviolability of private life and empowers judges to take necessary actions to prevent or halt violations of this right. The General Principles of Civil Law of the People's Republic of China also stipulate that "the personal information of a natural person shall be protected by law," reinforcing the legal protection of personal data and establishing safeguards against unauthorized disclosure or use. In summary, while Russia, Brazil, and China each have distinct legal frameworks, they all emphasize the protection of personal data and privacy through various provisions in their civil codes and specific laws, highlighting the importance of safeguarding individuals' personal information.

Russian legislation has evolved rapidly over the past decade, and data security laws constitute no exception. As the data economy has grown, lawmakers have increasingly sought to regulate transparency into how personal data is used and to clearly define the rights of businesses and individuals as it relates to personal data, with steps being taken to implement the core international principles of privacy and security laws.

1.2. Russian Data Protection Laws: historical overview and current trends

Fundamental provisions of personal data protection are laid down in the Constitution of the Russian Federation[1], international treaties, and Russian specific laws. The Russian Constitution (enacted in 1993) guarantees privacy and data protection rights. Article 23 of the Constitution established the right to privacy as one of the principal rights of citizens of Russia (this right may be challenged only by a court decision)[2], and article 24 crates the base for the right to data protection, confirming "consent" as one of the main legal bases for data processing. It requires that "the collection, keeping, use and dissemination of information about the private life of a person shall not be allowed without his or her consent". Enactment of specific laws and regulations is required to support these rights' execution. It is important to note that Brazilian Constitution also guarantee both right to privacy and data protection.

As a logical step of further development in personal data protection, in 2005, Russia ratified the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[3]. Several countries have built their data protection regime based on the Council of Europe Convention.

In order to ensure the effective implementation of the Convention and the adoption of country-specific technical requirements for the processing of personal data, in 2006 Russian State Duma adopted two primary laws governing personal data protection: Federal Law No. 149-FZ "On information, information technologies and data protection" (the “Data Protection Act”) and Federal Law No. 152-FZ "On Personal Data" (the “Personal Data Law”)[4]. The Personal Data Law is mainly based on Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such. The experience of its application and interpretation in Europe allows us to resolve issues related to personal data in the Russian Federation.

The Data Protection Act serves to protect the information in general and partially covers personal data. Article 2(7) of the Data Protection Act is an important pillar for the right to confidentiality. It guarantees confidentiality of information and requires a person who got access to information to seek the consent of the holder of such information prior to transferring it to third parties (clause 7, article 2).

The Personal Data Law regulates many aspects of data protection, including, but not limited to the definition of personal data, data types, and technical and organizational measures that must be applied by those who process personal data. Unlike European law, the Personal Data Law does not distinguish between data controllers and data processors. Therefore, any individual or entity working with personal data is considered a personal data operator governed by the Personal Data Law.

Thus, both acts play a significant role to guarantee privacy and confidentially of information.

Constitutional Court of the Russian Federation confirmed that the Personal Data Law is the main legislative act that regulates relations concerning the processing of personal data and defines the

[1] The Constitution of the Russian Federation December 25, 1993.

[2] Article 23: 1. Everyone is entitled to privacy of personal life, personal and family secrets, protection of one's honour and good name. 2. Limitations of this right shall be allowed only by court decision.", translation of the Constitution is provided by Garant Service (Garant.ru).

[3] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981.

[4] English verison of the law can be found at the website of The CyberBRICS project https://cyberbrics.info/

principles, conditions and rules for the processing of personal data[5]. According to article 3 of the Constitution, the regulation of relations concerning the processing of personal data is carried out exclusively at the federal level. Federal subjects of the Russian Federation cannot adopt legal acts in this area.

Additionally, the leading regulator in data protection — Federal Service for Communications, Information Technology and Mass Communications Supervision (the "Roskomnadzor") was established in 2008. It is controlled by and reports to The Ministry of Digital Development, Communications and Mass Media of the Russian Federation (also known as MinTsifry Rossii). This is a ministry of the Government of Russia responsible for telecommunications, media and the post. Thus, Roskomnadzor is a part of the federal executive body that performs the functions of developing state policy and legal regulation in the established field of telecommunications, media and the post.

In contrast, in each EU Member State there are data protection authorities (DPA). They are "independent public authorities that monitor and supervise, through investigative and corrective powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints that may have breached the law"[6]. For instance, independent authority Information Commissioner's Office in the UK is set up to uphold information rights in the public interest.

When comparing Russia's data protection regulatory framework to those in other BRICS countries, notable differences arise in terms of the independence and scope of authority of the data protection agencies. In China, the data protection authority operates within a framework that is not fully independent. The Chinese government maintains significant control over the regulatory processes related to data privacy and cybersecurity, which is evident in the close relationship between the data protection agency and the government. This centralized control allows the government to maintain a strong influence over how personal data is handled and monitored, often with a focus on state security and surveillance.

In contrast, Brazil and South Africa have regulatory bodies that operate with a greater degree of independence. Brazil's data protection authority, the National Data Protection Authority (ANPD), was established under the General Data Protection Law (LGPD), and it operates autonomously from the government, although it is still subject to some oversight by the Executive. The ANPD has the power to issue guidelines, monitor compliance, and impose fines for non-compliance, allowing it to act independently when it comes to enforcing data protection regulations.

Similarly, in South Africa, the Information Regulator is an independent authority tasked with enforcing the Protection of Personal Information Act (POPIA). The Information Regulator has significant powers, including the authority to investigate data breaches, monitor compliance with the law, and issue fines. Its independence from the government ensures that data protection issues are handled impartially, with a focus on safeguarding the privacy of individuals and upholding their rights.

Thus, while Russia's data protection regulator, Roskomnadzor, reports directly to the Ministry of Digital Development, Communications, and Mass Media, making it more government-controlled, Brazil and South Africa have created a more autonomous framework for data protection enforcement.

[5] The Definition of the Constitutional Court of the Russian Federation dated May 30, 2024, No. 1176-O "On the refusal to accept for consideration the complaint of citizen Ivanov Vladislav Vladimirovich regarding the violation of his constitutional rights by the provisions of Article 9 of the Federal Law 'On Personal Data.'

[6] https://commission.europa.eu/

Until 2014, data privacy had not been a topic of significant discussions or enforcement, and no significant changes were made to the existing order of personal data regulation.

Below we will touch upon the most essential updates that crucially influenced the current Russian data protection framework. The overview will briefly cover the enforcement provisions, which will be discussed in more detail in the next chapter.

The Russian Government has taken several large-scale measures to regulate relations involving the use of the Internet. The state's first response to the socially and politically significant use of the Internet was the introduction of some severe prohibitions and restrictions to ensure the state's security which we will cover below in more detail.

1.2.1. Data Localization Law

In 2014, the Russian parliament adopted amendments[7] to the Personal Data Law. These amendments are known as Data Localization Law, and they came into force on September 1, 2015. It requires data operators that collect personal data of Russian citizens to store and process such personal data using databases located in Russia as a "primary" database. Data can be transferred for further processing abroad (subject to compliance with the requirements for data transfers). Businesses and the media highly criticized these amendments. Supporters of the amendments argue that they created significant opportunities for profit for Russian data centres. At the same time, opponents confirm that it raised operational costs for ordinary businesses that required redesigning their data storage infrastructure. However, not all companies strive to comply with this law. For example, LinkedIn refused to comply with localization requirements[8]. As a result, the company's website and access to the social network were blocked in the territory of Russia. As a result, ordinary residents do not have the opportunity to freely use this social network.

The trend towards internet sovereignty is not confined to Russia; it is also evident in several other BRICS countries, including China and India. These countries are increasingly seeking to assert control over information flows within their national segments of the internet. Notably, China's data localization laws serve as a key example of this movement, mandating that data generated within its borders be stored and processed locally, further reinforcing national control over digital infrastructure and information.

Both Russia and China's data localization laws reflect a strong desire to control the flow of information within their borders, ensuring that data related to their citizens, businesses, and national security remains under domestic jurisdiction.

India has also taken steps toward data localization, particularly with the Personal Data Protection Bill (PDPB), which proposes that critical personal data must be stored in India. While some categories of data can be transferred abroad under specific conditions, the bill emphasizes that certain types of data should remain within the country to enhance privacy and security.

In contrast, Brazil and South Africa do not have strict data localization requirements. Instead, they focus more on ensuring adequate protection of personal data, regardless of where the data is stored. Brazil's LGPD and South Africa's POPIA allow for cross-border data transfers, provided that the

[7] Federal Law No. 242-FZ was approved by upper chamber of Russian parliament on July 9, 2014 and signed by the President on July 21, 2014 to make amendments to the Data Protection Act.
[8] https://iapp.org/news/a/why-linkedin-was-banned-in-russia/

destination country has an adequate level of protection in place or appropriate safeguards are provided.

Thus, while Russia, India, and China emphasize data localization, Brazil and South Africa adopt more flexible frameworks that allow international data transfers under certain conditions.

1.2.2. Yarovaya Law

The set of amendments to various laws that aimed to implement measures against terroristic activity was implemented in 2016[9]. They became known under one of its authors' name – Irina Yarovaya. A part of the initiative was to amend the Data Protection Act. The amendments introduced the concept of the "organizer of dissemination of information". The organizer of the dissemination of information on the Internet is a person carrying out activities to ensure the functioning of information systems and (or) programs for electronic computers that are intended and (or) used for receiving, transmitting, delivering and (or) processing electronic messages of network users on the "Internet". Such companies have to store communications data (images, video, voice and text messages) for six months and provide it to security services in the case of a court order with decryption keys if the messages are encrypted. They also have to register with Roskomnadzor via a designated website. A few messenger apps were blocked in Russia (e.g., Zello, WeChat[10], and Telegram, which was blocked from 2018 to 2020[11]) as a consequence of this law.

1.2.3. Sovereign Internet

In 2019 a set of amendments was enacted related to the functioning of the Internet in Russia. They become known as the Sovereign internet law[12]. The explanatory note to Sovereign Internet Law stated that its goal is to protect the country from cyberattacks and ensure the Internet's performance in Russia via "Runet" if it were to be disconnected from the global Internet.[13] In order to ensure the independent functioning of the Internet in Russia, the following new requirements were established: databases and programs associated with the provision of public government services must be located in Russia, and Roskomnadzor received the right to block traffic in case of Internet attacks. Many argue that proposed measures are beneficial only to Roskomnadzor, which received even more powers to block traffic on the Internet, which may be seen as a new form of censorship.[14]

Digital sovereignty, in the context of BRICS, refers to the ability to control digital infrastructure, data, and policies, promoting national interests, data security, and privacy. It emphasizes autonomy in digital

[9] Federal Law "On Amendments to the Criminal Code of the Russian Federation and the Code of Criminal Procedure of the Russian Federation in terms of establishing additional measures to counter terrorism and ensure public security" dated 06.07.2016 N 375-FZ and Federal Law "On Amendments to the Federal Law "On Countering Terrorism" and Certain Legislative Acts of the Russian Federation Regarding the Establishment of Additional Measures to Counter Terrorism and Ensuring Public Security" dated 06.07.2016 N 374-FZ.
[10] It was blocked for about one week and then unblocked as company decided to comply with the law.
[11] In 2020 Roskomnadzor announced the waiver of the requirement to restrict access to the Telegram messenger. It explained its decision by the willingness of the founder of Telegram to "counter terrorism and extremism."
[12] The Sovereign Internet Law is the informal name for a set of 2019 amendments to existing Russian legislation that mandate internet surveillance and grants the Russian government powers to partition Russia from the rest of the Internet: Federal Law No. 90-FZ of May 1, 2019 "On Amendments to the Federal Law "On Communications" and the Data Protection Act.
[13] Sovereign Internet Law Signed By The President Of Russia by Dr. Andrey Shcherbovich https://cyberbrics.info/cybersecurity-convergence-in-the-brics-countries/
[14] Cybersecurity Convergence In The BRICS Countries by Luca Belli https://cyberbrics.info/sovereign-internet-law-signed-by-the-president-of-russia/

governance, allowing each nation to set its own regulations for data protection, cybersecurity, and digital trade. The aim is to reduce dependence on foreign technologies and create a more balanced global digital landscape as well as to assert control over countries digital infrastructure, safeguard national security, and protect citizens' data.

While China, Russia, and to some extent India have implemented stringent measures like data localization and sovereign internet laws, Brazil and South Africa are advancing data protection laws and initiatives that strengthen local governance while fostering global cooperation. These countries are balancing national interests with the need for global interconnectedness, ensuring that digital sovereignty is a central part of their future technological strategies.

For example, Brazil issued Decree No. 11.856 on December 27, 2023, establishing the National Cybersecurity Policy and creating the National Cybersecurity Committee. This policy focuses on enhancing national cybersecurity, safeguarding data, combating cybercrime, and boosting organizational resilience, with the committee responsible for updating the policy, assessing cybersecurity measures, and promoting international cooperation.

1.2.4. New Requirement for Localization of Major Internet Companies in Russia

On 1 July 2021, Federal Law No. 236-FZ on the Internet Activities of Foreign Entities in the Russian Federation came into force, requiring foreign Internet companies whose information resource is accessed by 500,000 or more Russian users daily to establish and maintain a local presence, such as a branch, a representative office, or a subsidiary, effective January 1, 2022.

Establishing a local presence means that such companies have to open representative offices in Russia, cooperate with Roskomnadzor (in particularly responding to their notices) and place a feedback form on their websites (specifically, for receiving messages from Russian citizens). Opening a representative office in Russian territory means that companies shall have to comply with local requirements, prohibitions, and restrictions, and it will be easier for Roskomnadzor to enforce data protection requirements against such companies.

Roskomnadzor has the power to investigate whether foreign companies are following the conditions that require them to establish a presence in Russia. The regulator shall maintain a list of such companies on one of its websites.[15]

Legislators adopted many enforcement measures that allow the regulator to take action against the violator. Most of them are intended to restrict the online presence of the website. Among them are excluding websites from web-search results, completely blocking access to the website etc. The most discussed one is slowing down the internet speed in relation to a website (throttling). Such a measure requires targeted action on specific sites, and it is important to ensure that other websites will not be affected. The possibility to slow down a particular website became possible after the realization of a set of amendments that require data operators to install special equipment to their network that is required as an implementation of the Sovereign Internet Law. One of the famous examples is the throttling of Twitter.[16]

[15] 236-fz.rkn.gov.ru, accessed on January 5, 2022
[16] https://www.rbc.ru/technology_and_media/10/03/2021/6048ca449a7947480d4791de, as of January 15 2022.

1.2.5. Current trend: Digitalization of Russian Society and Economy, use of AI

Digital transformation encompasses the strategic use of digital technologies to revolutionize and enhance multiple facets of society, the economy, and governance. This process involves incorporating advanced technologies like artificial intelligence, machine learning, the Internet of Things (IoT), and data analytics to foster innovation, streamline operations, and stimulate growth across various industries and public services.

In 2017, the President of Russia approved the Strategy for the Development of the Information Society in the Russian Federation for 2017 – 2030[17] which fixed priority areas for the use of digitalization. The strategy is designed to contribute to the implementation of such national interests as the information security of citizens and the state, improving the efficiency of public administration, developing the economy and the social sphere, and ensuring law and order. The strategy is supported by measures taken at the federal and regional levels to adapt legislation to new technological conditions in various fields of activity[18].

Russia has been working on several initiatives related to the development and deployment of digital technologies, including AI, facial recognition. These initiatives are part of a broader strategy to modernize the country's technological infrastructure, improve public services, and ensure that AI technologies are integrated into society in a controlled and regulated manner.

On the federal level, the following documents, initiatives, and laws must be taken into account: the Government's National program "Digital Economy of the Russian Federation"; an experiment on the creation and use of a citizen "**Digital profile**"[19]. The participants of the experiment are credit, insurance, and microfinance organizations and operators of financial platforms. The legal basis for the experiment to function is set in the Decree of the Government of the Russian Federation of June 3, 2019, No. 710 "On conducting an experiment to improve the quality and connectivity of data contained in state information resources".

Appendix 2 to the Decree No. 710 lists information that forms the digital profile (it includes about 40 items). Mainly, they are considered as personal data (passport data, residential address, taxpayer identification number, etc.) and information from public registers (for instance, about owned real estate). But it also contains information that is usually considered more "sensitive", such as information about work records/labour books[20] in an electronic format, information on income and taxes paid and data on the business reputation of certain individuals such as founders of banks, non-state pension funds, etc.).

With the help of the digital profile infrastructure, the following can be provided: 1) identification and authentication of specified persons; 2) access to the digital profile and provision of information included in the digital profile in electronic form; 3) provision and updating, at the request of the relevant authorized bodies, of information about the person contained in the digital profile; 4) obtaining and withdrawing consent to the processing of personal data of citizens in cases involving the receipt of information about a person using the digital profile infrastructure; 5) providing information

[17] Decree of the President of the Russian Federation of May 9, 2017 N 203 "On the Strategy for the Development of the Information Society in the Russian Federation for 2017 - 2030" // SZ RF. 2017. N 20. Art. 2901.
[18] Information law: a textbook for universities / M.A. Fedotov and others; ed. M.A. Fedotov. M.: Yurayt, 2020. S. 122.
[19] https://digital.ac.gov.ru/, accessed on January 15, 2022.
[20] Serves as confirmation of employment in the Russian Federation and contains the history of the places of work of an individual.

for the formation of requests for state and municipal services; 6) storage of information and results of the provision of the above services in electronic form.

Mochalov[21] notes that based on the analysis of Decree No. 710, it can be concluded that a digital profile is not just a collection of information, but a certain ordered array of official data about a citizen or legal entity, the reliability of which is confirmed by the competent authorities of the state.

Undoubtedly, the Digital Profile system will help citizens quickly receive services where confirmation of various information is required. In turn, this will also simplify the interaction between the state and the citizen, allowing citizens and foreigners to get certain services faster.

However, consolidating such a large amount of data in one place raises questions about the security of such data. It is important that access to such data should be provided on a need-to-know basis in strictly necessary cases. Data subjects should be informed as to what part of their Digital Profile will have access to various systems. Data subjects should freely decide whether to provide their data or not.

In addition to reforms on the Federal level, larger cities have also seen some emerging technologies. In October 2021 the Moscow Metro launched a new **facial-recognition payment system** as the first mass-scale use of a technology that is aimed at bringing greater convenience to people's everyday lives – but at the same time has raised reasonable concerns about the system's possible misuse for surveillance purposes. A facial recognition system will scan the face and check it against its database[22]. A required step is to upload biometric data (face image) into the database of the system and provide consent for its use. A passenger will only need to register in a mobile application, upload a photo of his/her face and link a bank card or Troika (a contactless reusable card that is designed to pay for public transport in Moscow). As a result, the system compares the face with its data bank and lets a person enter the metro. Money is debited from the card automatically. Thus, the system allows easy payments without the need to carry cash or phone/bank cards.

Before such a system was introduced for payments, a facial recognition system was already operating in the Moscow metro[23]. Its goal was to find wanted offenders as well as missing people (including children). The system's collaboration with law enforcement ensures safety and security for passengers. It significantly helps to detain wanted criminals and suspects were detained by dint of this system. The system is used by responsible state bodies that are engaged in the investigation and prevention of crimes. The city authorities provide law enforcement officers with access to the system.

However, privacy professionals and activists express their concerns in regard to the privacy of individuals. They require that the system be more transparent and accountable with guarantees of protection against abuse by the authorities and third parties.[24] They are also concerned about mass surveillance of all visitors of the metro. The creation of such systems and their operation may present some benefits in such large cities as Moscow. At the same time, it is certainly necessary to observe and guarantee the fundamental rights and freedoms of citizens.

Another initiative of the Russian government that fall inthe scope of digitalization of the services is the is creation of the Unified Biometric System ("UBS"). The UBS is a state digital platform that allows the confirmation of a person's identity based on their biometric characteristics. Through biometrics and

[21] Mochalov A.N. Digital profile: main risks for constitutional human rights in the context of legal uncertainty // Lex russica. - 2021. - T. 74. - No. 9.
[22] https://facepay.mosmetro.ru/ accessed on of January 10, 2020
[23] https://transport.mos.ru/mostrans/all_news/107391
[24] https://roskomsvoboda.org/post/facepay-dlya-nazemki-v-msk/, accessed on January 15, 2022

the UBS, government and commercial services can be obtained remotely or in person — conveniently and securely. Use of the system and processing of personal data is being regulated by Federal Law "On the Identification and/or Authentication of Individuals Using Biometric Personal Data, Amending Certain Legislative Acts of the Russian Federation, and Repealing Certain Provisions of Legislative Acts of the Russian Federation" dated December 29, 2022, No. 572-FZ ("Federal Law on the Use of Biometric Data").

According to the article 3 of the Federal Law on the Use of Biometric Data: the UBS is used for the identification and/or authentication of individuals by various entities, including:

1. Government bodies and local authorities.
2. The Central Bank of the Russian Federation.
3. Banks, other credit organizations, and non-credit financial organizations engaged in activities listed under Article 76.1 of the Federal Law No. 86-FZ "On the Central Bank of the Russian Federation (Bank of Russia)" dated July 10, 2002.
4. Entities that are part of the national payment system.
5. Individuals providing professional services in the financial market (e.g., lawyers, notaries)
6. Other organizations, individual entrepreneurs, and notaries.

Additionally, the Unified Biometric System may be used in other legal relationships as stipulated by the laws of the Russian Federation.

The primary objective behind the implementation of the UBS is to enhance the accessibility of services that necessitate identity confirmation, fostering a more streamlined and secure user experience.

Providing biometric personal data is a right of citizens but not an obligation. Biometrics streamline interactions when accessing services but do not exclude other methods of identification and authentication. The refusal of an individual to undergo identification and/or authentication using their biometric personal data cannot be grounds for denying them the provision of state, municipal, or other services, the performance of state or municipal functions, the sale of goods, the execution of work, or refusal of service.

Individuals have the right to request the deletion of their biometric data from the UBS, and one method to initiate this process is by submitting a request through Multifunctional centers for the provision of public services. This centers are government-run facilities designed to provide a wide range of public services to citizens in a convenient and accessible manner. These centers serve as one-stop-shops where individuals can apply for various government services, access information, and handle bureaucratic procedures without needing to visit multiple government offices. They form part of Russia's efforts to modernize and simplify public administration, improve service delivery, and create more transparent and efficient government interactions.

While centralizing data does raise legitimate privacy concerns, it is crucial to highlight that such trends are integral part of the technological progress that can significantly enhance efficiency and improve public services. Access to unified data can streamline governmental processes, optimize decision-making, and improve the provision of the services including the timeline. Transparency, accountability, and robust safeguards at every stage are components of successful operation of the system. By carefully addressing the associated risks, governments can create an environment where innovation and privacy are balanced, ultimately benefiting both individuals and society as a whole.

To enhance the protection of biometric personal data and create a deterrent for both individuals and organizations from violating biometric personal data laws, on 5th of December 2023, members of the State Duma have approved a law on tightening penalties for violations of requirements in the field of placement of citizens' biometric personal data[25]. According to the document, a new Article 13.11.3 of the Code of the Russian Federation on Administrative Offenses introduces independent administrative liability for violations of requirements regarding the placement of citizens' biometric personal data.

Thus, fines for unauthorized placement, updating of such data and collection without consent are introduced: for officials, ranging from 100,000 (approx. USD 1,350) to 300,000 rubles (approx. USD 4,050), and for organizations, from 500,000 (approx. USD 6,750) to 1 million rubles (approx. USD 13,500). Upon a repeated commission of this offense, officials will be held accountable with fines ranging from 300,000 to 500,000 rubles, individual entrepreneurs from 500,000 to 1 million rubles, and organizations from 1 million to 1.5 million rubles (approx. USD 20,250).

According to the amendments, in cases where protocols are issues by officials of Roskomnadzor, courts will be responsible for considering cases of violations related to the placement and updating of biometric information. Additionally, within their authority, the Central Bank of the Russian Federation will also have the ability to adjudicate such cases.

Moreover, Russia has established an evolving AI regulatory framework that addresses legal, technical, and ethical considerations. The legal framework includes laws like the Federal Law on Personal Data (No. 152-FZ), which governs the processing of personal data for AI systems, and the Law on Experimental Legal Regimes in Digital Innovation (No. 258-FZ, 2020), which allows AI to be tested in flexible regulatory environments. To support AI development, the government created the AI.gov.ru portal (available in English), providing a centralized hub for legal documents, guidelines, and resources for businesses and researchers. These efforts help Russia foster AI innovation while ensuring safety, privacy, and ethical standards in its applications.

In recent years, use of biometric technologies and digital profiles have been increasingly adopted across several BRICS nations, each integrating them into various sectors to improve public services, enhance security, and streamline everyday activities, all in pursuit of broader goals like economic growth, digital inclusion, and cybersecurity.

In Russia, facial recognition systems are becoming more common in public spaces such as transportation, retail, and law enforcement. This is part of Russia's broader strategy to improve digital infrastructure, enhance security, and foster economic development by leveraging technology.

Similarly, India has made significant strides through its Digital India initiative, launched in 2015. A cornerstone of this initiative is Aadhaar, one of the world's largest biometric identification systems. Aadhaar uses data to verify identities for accessing government services and subsidies. Managed by the Unique Identification Authority of India (UIDAI), Aadhaar has become a key driver of digital inclusion, providing millions of Indians with access to essential services and promoting digital literacy across the nation. These efforts also contribute to India's goal of improving digital access and reducing inequality.

Meanwhile, China has been more advanced in integrating facial recognition technologies into everyday life, utilizing them in various sectors like public transportation, law enforcement, banking, and consumer services. While China's approach to biometric surveillance is among the most extensive, it highlights a global trend of using biometrics to improve efficiency, security, and innovation across

[25] http://duma.gov.ru/news/58432/, accessed on December 5th, 2023.

sectors. This global trend also reflects a shared goal of economic growth within the BRICS countries, as digital technologies play a vital role in boosting productivity and enhancing services.

1.2.6. Latest developments in the privacy legislation

Several amendments were introduced into the Law No. 152-FZ "On Personal Data" and other acts governing personal data processing in Russia[26]. We will briefly describe these changes. There are several changes that came into effect from September 1, 2022. For example, the response time to requests has been lowered to 10 working days, and the personal data subject now has the right to obtain information on the operator's compliance with Law No. 152-FZ responsibilities. Also, requirements for personal data subjects' consent increased. Consent must be specific and unambiguous. This change forces businesses to adapt and amend their standard consent form. Incident notification requirements become more comprehensive. New obligations related to reporting obligations for security incidents were introduced. They contain 2 steps. In case a data incident resulted in the unlawful transfer (provision, distribution, access) of personal data, an operator must notify Roskomnadzor within 24 hours from the discovery of the incident. The 24-hour report must include the following details: the causes of the data breach, the potential harm caused, the security measures taken in response, and the contact information of the authorized representative from the data controller responsible for addressing the breach. The report should be submitted within 72 hours of concluding the internal investigation. However, data controllers are not obligated to notify affected individuals. Also, Law No. 152-FZ become applicable to foreign legal entities and individuals if they process personal data of citizens of the Russian Federation on the basis of a contract or other agreement to which citizens of the Russian Federation are parties, or on the basis of the consent of a citizen of the Russian Federation to process their personal data. It means that amendments confirmed the extra-territorial application of the law. Additionally, some form of obligatory registry of the record of processing activities was introduced. Such registry should include: the categories and types of personal data; categories of personal data subjects; data retention and types of processing as well as how personal data are being destroyed. Another amendment came into force from 1st of March 2023. Companies who want to perform the cross-border transfer of personal data must notify Roskomnadzor of their intention to carry out cross-border transfer of personal data and obtain permission if the recipient country does not belong to the list of countries that provide adequate protection of the data subjects.

Still, there is a huge interest and further developments for the use of the Unified Biometric Systems. Related acts could be found on the system's webpage[27]. One of the main goals it to collect biometric personal data in one place to allow further use by public and private organizations. Collecting biometric personal data in one place for use by public and private organizations raises several important ethical, legal, and privacy concerns. While there can be legitimate reasons for collecting biometric data, such as for security or identification purposes, it must be done with great care and in accordance with established legal and ethical principles. There are some key considerations such as informed consent, data security and retention as well as purpose limitation, transparency and other.

Also, several amendments were introduced into the Federal Law No. 149-FZ "On information, information technologies and data protection". In particular, hosting providers must register with

[26] Federal Law of 14 July 2022 No. 266-FZ on Amending the Federal Law on Personal Data ('the Amendment Law'). English version of the text law is published on Roskomnadzor website as of 25.07.2011. Most of the amendments described in this paper were introduced between 2011 and 2021 (the lates were made on 02.07.2021 by N 331-FZ) https://pd.rkn.gov.ru/authority/p146/p164/

[27] https://ebs.ru/

Roskomnadzor and must meet several requitements such as reporting the initiation of their operations to Roskomnadzor; ensuring the stable, secure, and seamless functioning of the internet within Russia's borders; offering hosting services only following user identification procedures as determined by the government and guarantee compliance with information security requirements. Starting from February 1, 2024, hosting providers not included in the registry are not allowed to operate.

Identification procedures are currently allowed by use of the following mechanisms: use of telecommunications operator for identification purpose; use of biometric identifiers by available systems or use of other information systems that meet the legal requirements for information security, owned by Russian citizens without citizenship in another state or Russian legal entities. "Other information systems" for example includes mail service providers like mail.ru. Foreign email addresses will be banned to use for the registration purposes in such information systems.

Such changes arouse concerns since they pose technical challenges for users, necessitating the conversion of international addresses to Russian addresses, among other things. In principle, these amendments seek to gradually replace foreign servers and systems with Russian ones, which is consistent with the recent trend toward the localization of personal data and the formation of a sovereign Internet.

1.2.7. Human rights and rule of law context

In recent years, there has been a notable surge in the global discussion on human rights and the rule of law, with particular emphasis on the protection of personal data. This topic becomes particularly pronounced when considered in the framework of data transfers governed by the General Data Protection Regulation (GDPR). The scope of data transfer involves the various actions of sharing, sending, or facilitating access to personal data, all of which may involve diverse entities or systems situated in various countries or regions. The GDPR imposes specific requirements and safeguards to ensure that such data transfers comply with the regulation's principles for the protection of individuals' rights and privacy. When personal data is transferred outside the European Economic Area (EEA), organizations must follow certain mechanisms and safeguards to ensure that the data continues to be adequately protected. Execution of the EU Standard Contractual Clauses (“SCCs”) is one mechanism that allows data transfer. The Court of Justice of the European Union (CJEU) when deciding on the case C-311/18 initiated by Max Schrems, affirmed the validity of SCCs, providing that they include effective mechanisms to ensure compliance in practice with the “essentially equivalent” level of protection guaranteed by the GDPR to EU citizens. Transfer Impact Assessment (TIA) serves as a tool for performing such assessment. TIA is an individual case-by-case assessment to determine whether the recipient country affords an essentially equivalent level of data protection and if the safeguards of the transfer in question would be effective.

TIA, among its various aspects, necessitates the examination of the legal framework in the third country. The Transfer Impact Assessment should comprehensively evaluate relevant laws and practices governing third-party access, with a specific focus on government or intelligence agency surveillance.

Key considerations entail scrutinizing the third country's commitment to human rights protection, adherence to data security standards, and the alignment of its legal system with that of the EU, among other crucial factors. In essence, providing a thorough and detailed account of the applicable legal prerequisites in the third country is imperative for a comprehensive TIA.

Hence, considerations related to human rights and the rule of law are pivotal in the context of a TIA. In this section, we will delve into some aspects of these critical topics in Russia.

Over the years, Russia has undertaken substantial efforts to bring its legislative landscape in harmony with international norms, as described earlier. At the same time, questions persist regarding the practical implementation and enforcement of these regulations. Despite adhering to international human rights standards, particularly the Universal Declaration of Human Rights, it is important to ensure that it should not only be well-established on paper but shall be effectively put into practice through enforcement measures.

One of the primary challenges is the potential tension between national security interests and individual privacy rights. The deployment of surveillance practices in public spaces has become a focal point of concern for human rights advocates, emphasizing the intricate task of striking a delicate balance between ensuring the safety of citizens and upholding their fundamental right to privacy. Balance of these rights remains a delicate and evolving aspect of the rule of law in Russia.

Moreover, the increasing digitalization of society introduces an array of challenges pertaining to issues such as consent, data breaches, and the cross-border transfer of personal data.

Navigating these issues requires a nuanced approach that safeguards individual rights hindering the progress of technological advancements that underpin societal development.

In response to these challenges, recent developments in Russia include amendments to the Federal Law on Personal Data. These revisions underscore the government's commitment to remaining at the forefront of technological progress and adapting the legal framework to effectively address emerging challenges. This proactive stance reflects an awareness of the evolving landscape of technology and data processing, aligning legislative efforts with the dynamic technological developments.

The Personal Data Laws impose several limitations on the rights of data subjects and the processing of sensitive categories of personal data. Article 14 of the Personal Data Law specifically governs the data subject's right to access their personal data, detailing the limitations on these rights (refer to section 8).

These restrictions, as outlined in Article 14, are subject to federal laws and include the following scenarios:

1. Processing for National Defense and Security:

When personal data processing, including information acquired through operational, counterintelligence, and intelligence activities, serves national defense, state security, and law enforcement purposes[28].

2. Detention or Criminal Accusation:

In cases where authorities detaining the data subject on suspicion of a crime or accusing them in a criminal case, or applying preventive measures before filing charges, restrict access to personal data. Exceptions may apply under the criminal procedural legislation of the Russian Federation[29].

[28] Art. 14, section 8 of the Federal law On Personal Data "The processing of the personal data, including the personal data obtained as the
result of operative-search operations, counter-intelligence and intelligence activities takes
place for the purposes of national defence, state security and law and order";

[29] "The personal data are processed by the bodies which have detained the personal

3. Legal Compliance for Crime Prevention:

When the personal data are processed in accordance with the legislation on countering the legalisation of incomes received through crime (money laundering) and the financing of terrorism.

4. Protection of Third-Party Rights:

When the data subject's access to their personal data would infringe upon the rights and legitimate interests of third parties.

5. Transport Security Legislation:

In cases outlined by the legislation of the Russian Federation on transport security, where personal data processing is essential for ensuring the sustainable and safe functioning of the transport complex and protecting the interests of individuals, society, and the state from unlawful interference.

Article 10 of the Personal Data Law explicitly prohibits the processing of special categories of personal data, such as race, nationality, political views, religious or philosophical beliefs, health status, and intimate life. Exceptions are allowed under specific circumstances detailed in parts 2 and 2.1 of Article 10, permitting the processing of special categories of personal data by Russian authorities for purposes such as security, counterterrorism, transport security, and anti-corruption efforts.

It is interesting to observe limitations to the right or privacy in other BRICS countries. For example, in India, public bodies are granted certain exemptions from fully complying with personal data protection laws. These exemptions are designed to strike a balance between robust data protection and the practical needs of governmental functions, particularly in areas like national security, law enforcement, and public welfare. Under the India's Digital Personal Data Protection Act, 2023 (DPD Act), public bodies and government entities are permitted to process personal data without strictly adhering to the law's provisions in cases related to national security, law enforcement, or public order. This ensures that the government can effectively carry out its essential duties in these critical areas, without being overly constrained by data protection requirements.

1.3. Introduction to the Key Features of the PERSONAL DATA Law

1.3.1. Scope and Key Definitions

The Personal Data Law defines the terms "personal data" and "data processing", establishing a comprehensive framework governing the rights of data subjects. It outlines the responsibilities of data controllers, including guidelines on consent, policies for data localization, and regulations concerning cross-border data transfers. This legislation predominantly addresses personal data operators functioning within the territorial bounds of the Russian Federation.

---

data subject on suspicions of having committed a crime or which have presented criminal-case charges to the personal data subject or have imposed a measure of restraint on the personal data subject before presenting charges, except for the cases envisaged by the criminal procedural legislation of the Russian Federation when the suspect or accused is allowed to get acquainted with such personal data"

In contrast to the broad territorial scope of the GDPR[30], which safeguards the personal data of any EU citizen regardless of the company's geographical or jurisdictional location, the Personal Data Law is geographically more circumscribed. Specifically, it applies to personal data operators registered and functioning within the Russian Federation. Importantly, foreign data operators situated outside Russia are mandated to comply with data localization rules when collecting personal data from Russian residents. This underscores an extraterritorial dimension in ensuring robust data protection for individuals in Russia.

The Russian definition of personal data is generally consistent with the European framework. The Personal Data Law defines personal data as any information referring directly or indirectly to an identified or identifiable individual, known as a personal data subject or data subject.[31] Encompassing a wide variety of information, personal data may also include data collected by cookies, information about geolocation, IP address or subscriber traffic. The Personal Data Law also sets forth special categories of personal data (also known as sensitive personal data), which are subject to a higher level of protection and can be processed in limited scenarios. Sensitive personal data include a person's racial or ethnic origin, religious or political beliefs, medical data, and criminal record. In addition, the processing of personal biometric data, which a data operator may only process with data subject consent or under other exceptions, is also regulated by the Personal Data Law.

The Personal Data Law defines the processing of personal data rather broadly as any action or combination of actions involving personal data, carried out with or without computer equipment, including collection, recording, systematization, accumulation, storage, clarification (updating and modification), retrieval, use, transfer (dissemination, disclosure and access), depersonalization, blocking, deletion and destruction of personal data[32]. The Personal Data Law regulates both the manual and automated data processing of personal data.

1.3.2. Key Requirements for Data Processing

The Personal Data Law requires data controllers to have a lawful basis for processing personal data. Typically, this means that the personal data controller must process personal data on the basis of consent. For example, consent may be given by data subjects in any verifiable form, including in writing, electronically or by means of implied consent.

However, there are certain types of processing[33] to which the Personal Data Law does not apply. For example, personal data processing by individuals solely for personal and family needs, provided that processing does not infringe the data subject's rights; processing personal data for archival purposes; and personal data processing that includes state secrets.

In the legislative framework of the Russian Federation, there is no formal notion of "anonymized data", though it is a well-recognized concept within the domain of information security specialists. Legislation does, however, incorporate the term "depersonalization". Depersonalization of personal data is identified as a method of processing personal data where, upon completion, it becomes practically impossible, without the aid of supplementary information, to identify the specific individual to whom the personal data belongs. The guidelines and methodologies for anonymizing personal data are outlined in Roskomnadzor Order No. 99639, issued on September 5, 2013.

---

30 https://eur-lex.europa.eu/eli/reg/2016/679/oj
31 Federal Law No. 152-FZ "On Personal Data" Article 3(1)
32 Federal Law No. 152-FZ "On Personal Data" Article 3(3)
33 Article 1(2) of the Personal Data Law.

While the terms "anonymization" and "depersonalization" may appear similar, they imply distinct techniques for handling personal data. The concept of depersonalization bears resemblance to the GDPR's pseudonymization, although each involves different approaches to safeguarding personal data.

The classification of depersonalized data as personal remains a subject of debate. Generally, it is presumed that personal data laws do not apply to anonymized data, a stance supported by case law.[34] Conversely, Roskomnadzor contends that personal data obtained as a result of depersonalization is still personal data and remains subject to the relevant legislation.[35]

Recent statements from Roskomnadzor indicate plans to regulate and process depersonalized data in line with the Personal Data Law, with anticipated legislative amendments within a year.[36]

Certain data protection operations, such as marketing, require prior opt-in consent. For instance, processing of personal data for direct marketing purposes requires each individual's explicit opt-in consent. Every marketing communication must contain a link enabling individuals to revoke their consent (unsubscribe) at any time or otherwise contain specific guidelines as to how this consent may be revoked. Once an individual revokes their consent, the data controller must immediately terminate direct marketing communications and related data processing – the applicable laws do not provide any grace period in this instance.

Data operators may transfer data to third parties (including affiliated companies[37]) under the following conditions:

- under the data subject's consent or based on other legal bases from the closed list established by the Personal Data Law [38] (e.g., when the processing of personal data is necessary for the performance of a contract to which the data subject is a party or beneficiary or guarantor; the processing of personal data is necessary to protect the life, health or other vital interests of the data subject, if obtaining the consent of the data subject is impossible);
- pursuant to a separate data transfer agreement or based on a contractual clause that includes confidentiality provisions imposed on the recipient.

Additional obligatory provisions must be included if the recipient acts in the capacity of a data processor pursuant to the operator's instructions: (i) purposes of data processing (must be consistent with the purpose that was initially mentioned during data collection); (ii) allowed actions that may be performed on personal data; and (iii) organizational and technical data protection measures.

Data may be transferred outside Russia in one of the following cases:

- transfer is made to the jurisdictions that ensure adequate protection of personal data subjects' rights (the country is considered adequate by default if it ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data);

[34] Decision of the Supreme Court of the Russian Federation dated January 26, 2011 No. GKPI10-1510
[35] https://pravo.ru/lf/story/231731/, accessed on December 15, 2021
[36] https://www.pnp.ru/social/obezlichennye-dannye-mogut-nachat-obrabatyvat-kak-personalnye.html, accessed on January 21, 2022.
[37] According to Article 4 of the Law "On Protection of Competition" dated July 26, 2006 No. 135-FZ, affiliates are those companies or employees (as well as representatives of the "same group", including related ones) that can influence the activities of the organization and adopted its management team strategic decisions.
[38] Closed list of grounds for transferring data to the third party without the consent of the data subject is established by article 6 of the Personal Data Law.

- subject to the written consent of a data subject;
- for the purpose of performing a contract to which the data subject is a party;
- subject to an international treaty to which Russia is a signatory;
- the transfer is required pursuant to federal laws for the protection of the Constitution, state defence, security, and transport system;
- it is necessary to protect the data subject's vital interests (if it is not possible to get the written consent of the data subject).

Russian laws permit the transfer of data to countries that are parties to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and to a number of certain non-signatory countries deemed by Roskomnadzor to have adequate data privacy protections policies in place[39]. The latest Order of Roskomnadzor came into force on 01.03.2023. It is interesting to note that prior to March 2023, India and China (BRICS members) were not considered as countries providing adequate protection of the rights of personal data subjects. However, the United States, not being a signatory to the Convention and not listed by Roskomnadzor as having adequate privacy protection policies, is not authorized for the transfer of personal data from Russia.

1.3.3. Data Localization Requirement

The Data Localization requirement mandates that entities acting as data controllers, responsible for the collection of personal data, must adhere to the stipulation that the recording, systematization, accumulation, storage, verification, and extraction of personal data belonging to Russian citizens should exclusively occur within data centers located within the borders of Russia. This regulation is applicable to both domestic and foreign data controllers, thereby impacting a great number of major international companies operating in Russia. Notable examples include Uber, Booking.com, Facebook, Aliexpress, eBay, and PayPal, all of whom have had to adjust their data management practices in order to comply with this legislation. To align with the mandate, corporations had to either establish new data centers in Russia or relocate existing ones, reflecting the considerable impact of this regulatory framework on the operational dynamics of these entities.

An illustrative instance of the regulatory consequences is LinkedIn, whose network activities within Russia were officially blocked in 2016 due to non-compliance with the Data Localization requirement. This high-profile case serves as a potent reminder of the strict enforcement of this regulation, emphasizing that even major players in the tech industry are not exempt from the legal ramifications of failing to adhere to data localization guidelines.

It is noteworthy that this legislative provision not only affects the current landscape but also holds implications for potential market entrants. Any foreign websites or applications entering the Russian market must meticulously adhere to these data localization laws to avoid the risk of being blocked. In

[39] Order of Roskomnadzor No. 128 dated August 5, 2022, "On Approval of the List of Foreign States Providing Adequate Protection of the Rights of Personal Data Subjects.
Prior the Order No. 274 of March 15, 2013 "On endorsement of the List of the Foreign States Which are Not Parties to the EC Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data" was in force.

essence, the requirement serves as a pivotal factor influencing the operational and strategic decisions of companies operating within the digital ecosystem in Russia.

1.3.4. Essential Steps to Manage Data Risks and Sustain Regulatory Compliance

The Personal Data Law requires companies to implement a range of measures designed to ensure and demonstrate that they are in compliance with the regulation. Data controllers must take appropriate technical and organizational measures against unauthorized or unlawful processing and accidental loss, changing, blocking or destruction of personal data.

In order to manage possible risks and maintain regulatory compliance, companies must consider the following steps:

- create data mapping, data flows and identify relevant data categories;
- appoint a local data protection officer who will be in charge of the compliance procedures;
- adopt local data protection policies and other required privacy documents;
- implement appropriate security measures;
- meet specific requirements including data localization laws.

It is important to carry out regular data protection audits to help ensure ongoing data privacy compliance with national data protection requirements and regulations.

Also, it is obligatory for data controllers to file a notice with the Roskomnadzor prior to the commencement of data processing. Such notice must contain the details of the data controller and data processor, the purposes of data processing, categories of personal data processed and categories of data subjects whose personal data is processed, period of data processing, legal grounds for data processing, list of security measures undertaken by the data controller (including encryption tools), and certain other details. This notice shall be filed once and with respect to all data processing activities of the particular data controller and may be submitted online or alternatively by post. All changes in the data processing activities must be notified to Roskomnadzor within ten business days. There are certain exemptions from the notification obligation. For instance, no notice is necessary when data processing is conducted for the purpose of executing a contract with the data subject.

Under the Personal Data Law, legal entities are required to appoint a Data Protection Officer. A Data Protection Officer is responsible for evaluating the existing data protection framework and ensuring the company's policy is in accordance with the relevant laws and codes of practice, providing data protection advice and support for staff members who are involved in processing data, and carrying out regular compliance audits. They also serve as the key point of contact between the company and the data protection authority. The role of a Data Protection Officer is mandatory for all organizations that process or collect personal data. Failure to appoint a Data Protection Officer is a violation of the data protection policy and may result in the imposition of fines and enforcement protocols.

1.3.5. Liability for Non-Compliance with Data Protection Laws

The broad material and personal scope of Russian data protection laws make data protection apply to nearly anyone processing any information at any time, and the threat of certain sanctions is omnipresent.

A data controller may face civil, administrative or criminal liability if there is a violation of the Personal Data Law. Data protection officers responsible for the offence may also face disciplinary action.

The fines for violations of data protection laws could vary depending on the nature and severity of the breach. Administrative fines vary according to the type of violation. In some cases, more than one fine may be imposed for a single breach (e.g., each affected data subject may result in an imposed fine). Fines start from RUB 75,000 (approx. USD 800) and go higher. For instance, RUB 500,000 (approx. USD 5,500) for violation of direct marketing requirements, RUB 6,000,000 (approx. USD 66,200) for the data localization violation for the first offence, and up to RUB 18,000,000 (approx. USD 198,050) for a repeated offence.

In addition to fines, there could be other administrative penalties for non-compliance, including warnings, suspension of data processing activities, or even a complete ban on processing personal data. Individuals affected by a data breach may also have the right to seek compensation for damages resulting from the violation.

Moreover, unlawful data processing practices may entail forced termination of respective data processing activities and blockage of a website and/or app, where they relate to personal data processing on such website and/or app.

1.4. A brief overview of the enforcement of Data Protection Law in Russia

Data subjects in Russia have the right to directly assert their data protection rights by initiating legal action against data operators, seeking monetary damages, or claiming compensation for moral harm. Criminal liability may be incurred for illegal access, modification of computer information (including personal data), and the unauthorized disclosure of personal data related to an individual's private life. Alternatively, individuals can file complaints with Roskomnadzor, the regulatory authority overseeing data protection.

Roskomnadzor has several key enforcement mechanisms under the Governmental Decree issued in 2019.[40] It can investigate and rectify data protection infringements, imposing administrative fines in line with the Code of the Russian Federation on Administrative Offenses. The regulator may initiate investigations independently or respond to private individuals' requests, with the authority to represent individuals in court or act in the public interest.

In the investigation process, the regulator may conduct on-site inspections at data operators' premises, or monitor their activities remotely, or perform unscheduled visits. New rules introduced in 2019 prioritize scrutiny of companies processing sensitive or biometric data on behalf of data controllers having no presence in Russia or those transferring data to countries deemed inadequate in data protection under Russian law. Unscheduled inspections may also be triggered based on online monitoring, public domain information, or data subject requests.

As a part of its corrective powers, Roskomnadzor can block websites or specific internet pages found to contain prohibited information or violate data localization laws. Based on a court decision[41], Roskomnadzor added LinkedIn to the database on the Register of Infringers of Rights of Personal Data Subjects and obliged telecommunications companies to block access to LinkedIn in

[40] the Decree of the Government "On Adopting the Regulations on Organizing and Performing State Control and Supervision over Personal Data Processing" dated February 13, 2019 №146

[41] Decision of the Moscow City Court ('MCC') of November 10 2016 Case No. 33-38783/16 on the restriction of the access to LinkedIn Corporation from Russia

Russia.[42]Additionally, there were several cases that involved significant fines that were imposed on well-known messenger companies. For example, Facebook and Twitter were fined multiple times for breaching data localization laws. More recently, in August 2021, both platforms were fined RUB 15 million (approx. USD 165,500) and RUB 17 million (approx. USD 187,500) for violations of data localization laws[43].

Also, in 2021, Roskomnadzor imposed fines on Facebook for its refusal to remove content that violated Russian legislation[44]. A Roskomnadzor spokesperson reported that in 2021, the regulatory body initiated 23 protocols against the owner of Facebook. As per court decisions, Facebook was directed to pay fines amounting to RUB 83 million (approx. USD 915,000)[45].

While some argue that these fines may be insignificant to tech giants like Google and Facebook, questions arise about Roskomnadzor's authority to enforce court orders and collect fines from foreign companies. The recent trend of requiring foreign companies to establish a presence in Russia may strengthen the regulator's ability to enforce measures against violations by such entities.

1.5. Conclusion

Since the early 1990s, Russia has undergone notable strides in acknowledging and upholding the right to privacy, demonstrating a commitment to safeguarding the personal information of its citizens. The country has actively participated in key international treaties, translating these commitments into practical implementations. Notably, Russia has embraced modern technologies integral to processing personal data, including the incorporation of personal biometric information. The introduction of the Digital Profile has streamlined interactions between citizens and the State, facilitating the swift delivery of services.

However, despite these advancements, there remains a need for further refinement to make these technologies more appealing to the public, with a particular emphasis on addressing privacy concerns. A pivotal issue is the centralized storage of data, which raises apprehensions about the security of such information and the potential ulterior motives behind its utilization. The fact that Roskomnadzor is inherently a part of the Russian Government, rather than an independent regulatory body, adds to individuals' unease, as there is a lingering fear that collected data may be exploited for surveillance or other government-centric purposes.

Several other factors compound concerns regarding individual privacy. The concentration of power within the realm of information control can lead to the isolation of the Russian information society and the potential for abuse by surveillance structures. Strident data localization laws have already resulted in the prohibition of certain popular social networks in Russia. LinkedIn, for instance, opted not to comply with data localization requirements, leading to its subsequent blockage within the country. Proponents of data localization argue that this strategy is designed to protect the information of Russian citizens while simultaneously fostering commercial benefits and creating opportunities for Russian data centers.

The existing scenario underscores the need for substantial improvements in Russia's data privacy legislation, with a specific focus on enhancing transparency and fostering collaboration with the public. It is evident that further efforts are required to fortify the protection of personal data and information.

---

[42] https://iapp.org/news/a/why-linkedin-was-banned-in-russia/, accessed on January 20, 2022
[43] https://www.rbc.ru/business/30/09/2021/6154e0d69a79473e0a35e6d1, accessed on January 20, 2022
[44] Art. 13.41 Code of Administrative Offenses
[45] https://www.vedomosti.ru/media/articles/2021/12/24/902582-facebook-oshtrafovali, accessed on January, 2022

This entails comprehensive development from both technical and legal standpoints, marking the prioritization of personal data regulation as a key focus area for Russia's overall development.

Looking ahead, it is crucial to prioritize the ongoing improvement and evolution of personal data regulation in Russia. This imperative extends beyond mere refinement of existing legal frameworks; it requires a proactive embrace of technological innovations that align with international standards for privacy protection. Transparency and collaboration should be at the forefront of these endeavours, ensuring that the public is not only informed but actively involved in shaping the trajectory of personal data governance. By designating the protection of personal data as a priority, Russia can contribute significantly to the global discourse on privacy rights while fostering a more secure and trusted digital environment for its citizens.

Globally, as we look at the regulatory frameworks of BRICS countries, it is clear that while there are variations in how each nation approaches privacy, data protection, and AI development, there is a common goal among them. Russia, China, and India are among the leading BRICS nations striving to become pioneers in the use of modern technologies, particularly AI and biometrics. These countries are actively working to develop cutting-edge technologies and build infrastructure to enhance their digital economies and improve their global standing in innovation.

The BRICS countries' approaches to key data protection issues, such as data localization, data transfers, and the powers and independence of data protection authorities, highlight their varied strategies towards achieving digital sovereignty. While data localization laws are increasingly being enforced, as seen in Russia and China, other countries are working towards ensuring that data is processed within their borders, but with a focus on international cooperation. In terms of data transfers, countries are balancing national interests with global trade and digital flow requirements, with mechanisms to ensure secure cross-border data movement.

The powers and remit of data protection authorities in the BRICS nations differ in scope and independence. China and Russia maintain more centralized control over their data protection agencies, while Brazil and South Africa ensure that their agencies operate with greater autonomy. The enforcement of data protection laws varies as well, with some countries relying solely on the data protection authority for enforcement, while others, like India (Cyber Appellate Tribunal), integrate tribunals and other agencies for more comprehensive action.

Regarding the automated processing of personal data, BRICS countries are increasingly focusing on setting clear guidelines and obligations to protect citizens from the risks of automation and AI, while still fostering technological development.

These varied approaches highlight the complex and evolving landscape of data protection and digital sovereignty within the BRICS countries, as they seek to balance individual rights, national security, and economic interests in the digital age.

2. APPENDIX A – RUSSIAN FEDERAL LAW ON PERSONAL DATA (NO. 152-FZ)

RUSSIAN FEDERATION
FEDERAL LAW

Non-final version of Churshina, Anna and Kruglikova; Anna. The personal data architecture of Russia; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

ON PERSONAL DATA

Accepted
State Duma
8 July 2006.

Approved
Federation Council
14 July 2006

List of amending documents
(ed. Federal Laws of 25.11.2009 N 266-FZ,
27.12.2009 N 363-FZ, 28.06.2010 N 123-FZ, 27.07.2010 N 204-FZ,
of 27.07.2010 N 227-FZ, of 29.11.2010 N 313-FZ of 23.12.2010 N 359-FZ,
of 04.06.2011 N 123-FZ, of 25.07.2011 N 261-FZ, of 05.04.2013 N 43-FZ,
dated 23.07.2013 N 205-FZ, dated 21.12.2013 N 363-FZ, dated 04.06.2014 N 142-FZ,
21.07.2014 N 216-FZ, 21.07.2014 N 242-FZ, 03.07.2016 N 231-FZ,
22.02.2017 N 16-FZ, 01.07.2017 N 148-FZ, 29.07.2017 N 223-FZ,
31.12.2017 N 498-FZ, 27.12.2019 N 480-FZ, 24.04.2020 N 123-FZ,
dated 08.12.2020 N 429-FZ, dated 30.12.2020 N 515-FZ, dated 30.12.2020 N 519-FZ,
11.06.2021 N 170-FZ, 02.07.2021 N 331-FZ, 14.07.2022 N 266-FZ,
of 06.02.2023 N 8-FZ)

Chapter 1: GENERAL PROVISIONS

Article 1: Scope of this Federal Law

1. This Federal Law regulates relations connected with the processing of personal data carried out by federal state authorities, state authorities of constituent entities of the Russian Federation, other state authorities (hereinafter - state authorities), local self-government authorities, other municipal authorities (hereinafter - municipal authorities), legal entities and natural persons with or without the use of means of automation, including in information and telecommunications networks
(part 1 in edition of the Federal Law of 25.07.2011 N 261-FZ)

1.1 The provisions of this Federal Law shall apply to the processing of personal data of citizens of the Russian Federation carried out by foreign legal entities or foreign individuals on the basis of a contract to which citizens of the Russian Federation are a party, other agreements between foreign legal entities, foreign individuals and citizens of the Russian Federation or on the basis of the consent of a citizen of the Russian Federation to the processing of his/her personal data.
(part 1.1 introduced by the Federal Law of 14.07.2022 N 266-FZ)

2. The effect of this Federal Law shall not extend to relations arising under:

1) processing of personal data by individuals exclusively for personal and family needs, if the rights of personal data subjects are not violated;

2) organisation of storage, acquisition, accounting and use of documents of the Archive Fund of the Russian Federation and other archival documents containing personal data in accordance with the legislation on archiving in the Russian Federation;

3) ceased to be in force. - Federal Law of 25.07.2011 N 261-FZ;

4) processing of personal data classified as state secret in accordance with the established procedure;

5) has lost force. - Federal Law of 29.07.2017 N 223-FZ.

3. Provision, dissemination, transfer and receipt of information on the activities of courts in the Russian Federation containing personal data, maintenance and use of information systems and information and telecommunication networks in order to create conditions for access to the said information shall be carried out in accordance with the Federal Law of 22 December 2008 N 262-FZ "On Ensuring Access to Information on the Activities of Courts in the Russian Federation".
(part 3 introduced by the Federal Law dated 29.07.2017 N 223-FZ)

Article 2: Purpose of this Federal Law

The purpose of this Federal Law is to ensure the protection of human and civil rights and freedoms in the processing of personal data, including the protection of the rights to privacy, personal and family secrecy.

Article 3: Basic concepts used in this Federal Law

(ed. Federal Law of 25.07.2011 N 261-FZ)

For the purposes of this Federal Law, the following basic concepts shall be used:

1) personal data - any information relating to a directly or indirectly defined or identifiable natural person (subject of personal data);

1.1) personal data authorised by the subject of personal data for dissemination - personal data, access to which is provided by the subject of personal data to an unlimited number of persons by giving consent to the processing of personal data authorised by the subject of personal data for dissemination in the manner prescribed by this Federal Law;
(paragraph 1.1 introduced by the Federal Law of 30.12.2020 N 519-FZ)

2) operator - a state authority, municipal authority, legal or natural person, independently or jointly with other persons organising and (or) carrying out processing of personal data, as well as determining the purposes of personal data processing, composition of personal data subject to processing, actions (operations) performed with personal data;

3) processing of personal data - any action (operation) or set of actions (operations) performed with or without the use of automation means with personal data, including collection, recording, systematisation, accumulation, storage, clarification (update, change), extraction, use, transfer (distribution, provision, access), depersonalisation, blocking, deletion, destruction of personal data;

4) automated processing of personal data - processing of personal data by means of computer equipment;

5) dissemination of personal data - actions aimed at disclosure of personal data to an indefinite number of persons;

6) provision of personal data - actions aimed at disclosure of personal data to a certain person or a certain circle of persons;

7) blocking of personal data - temporary cessation of personal data processing (except for cases when processing is necessary to clarify personal data);

8) destruction of personal data - actions as a result of which it becomes impossible to restore the content of personal data in the personal data information system and (or) as a result of which material carriers of personal data are destroyed;

9) depersonalisation of personal data - actions, as a result of which it becomes impossible to determine the belonging of personal data to a particular subject of personal data without using additional information;

10) personal data information system - a set of personal data contained in databases and information technologies and technical means ensuring their processing;

11) cross-border transfer of personal data - transfer of personal data to the territory of a foreign state to a foreign authority, a foreign natural person or a foreign legal entity.

Article 4: Legislation of the Russian Federation in the field of personal data

1. The legislation of the Russian Federation in the field of personal data shall be based on the Constitution of the Russian Federation and international treaties of the Russian Federation and shall consist of this Federal Law and other federal laws determining the cases and peculiarities of personal data processing.

2. On the basis of and in pursuance of federal laws, state bodies, the Bank of Russia, local self-government bodies within the limits of their authority may adopt regulatory legal acts, normative acts, legal acts (hereinafter - regulatory legal acts) on certain issues related to the processing of personal data. Such acts may not contain provisions restricting the rights of personal data subjects, establishing restrictions on the activities of operators not provided for by federal laws or imposing obligations on operators not provided for by federal laws, and are subject to official publication.
(part 2 in edition of the Federal Law dated 25.07.2011 N 261-FZ)

3 The specifics of personal data processing carried out without the use of means of automation may be established by federal laws and other regulatory legal acts of the Russian Federation, taking into account the provisions of this Federal Law.

3.1 The normative legal acts adopted in accordance with paragraph 2 of this Article shall be subject to mandatory coordination with the competent authority for the protection of the rights of personal data subjects in cases where the said normative legal acts regulate the relations related to the transborder transfer of personal data, processing of special categories of personal data, biometric personal data, personal data of minors, provision, dissemination of personal data obtained as a result of the transfer of personal data to the competent authority for the protection of the rights of personal data subjects. The term of the mentioned approval cannot exceed thirty days from the date of receipt of the respective normative legal act by the authorised authority for the protection of the rights of personal data subjects.
(part 3.1 introduced by the Federal Law of 14.07.2022 N 266-FZ)

4. If an international treaty of the Russian Federation establishes rules other than those provided for by this Federal Law, the rules of the international treaty shall apply.

5. Decisions of interstate bodies adopted on the basis of the provisions of international treaties of the Russian Federation in their interpretation contradicting the Constitution of the Russian Federation shall not be subject to execution in the Russian Federation. Such contradiction may be established in accordance with the procedure determined by federal constitutional law.
(part 5 introduced by the Federal Law of 08.12.2020 N 429-FZ)

Chapter 2: PRINCIPLES AND CONDITIONS OF PERSONAL DATA PROCESSING

Article 5: Principles of personal data processing

(ed. Federal Law of 25.07.2011 N 261-FZ)

1 The processing of personal data must be carried out on a lawful and fair basis.

2 The processing of personal data must be limited to the achievement of specific, predetermined and legitimate purposes. Processing of personal data incompatible with the purposes of personal data collection is not allowed.

3 It is not allowed to merge databases containing personal data processed for incompatible purposes.

4. only personal data that fulfils the purposes for which it is processed shall be processed.

5. The content and scope of processed personal data shall correspond to the stated purposes of processing. The processed personal data shall not be redundant in relation to the stated purposes of their processing.

6. When processing personal data, the accuracy of personal data, their sufficiency and, where necessary, relevance to the purposes of personal data processing shall be ensured. The operator shall take the necessary measures or ensure that they are taken to remove or clarify incomplete or inaccurate data.

7. Personal data shall be stored in a form that allows identification of the subject of personal data for no longer than required by the purposes of personal data processing, unless the period of personal data storage is established by federal law, contract to which the subject of personal data is a party, beneficiary or guarantor. Processed personal data shall be destroyed or depersonalised once the purposes of processing have been achieved or if it is no longer necessary to achieve these purposes, unless otherwise provided for by federal law.

Article 6: Conditions of personal data processing
(ed. Federal Law of 25.07.2011 N 261-FZ)

1. personal data processing shall be carried out in compliance with the principles and rules stipulated by this Federal Law. Processing of personal data is allowed in the following cases:

1) processing of personal data shall be carried out with the consent of the personal data subject to the processing of his/her personal data;

2) the processing of personal data is necessary to achieve the purposes provided for by the international treaty of the Russian Federation or by law, to perform and fulfil the functions, powers and obligations imposed on the operator by the legislation of the Russian Federation;

3) processing of personal data is carried out in connection with the participation of a person in constitutional, civil, administrative, criminal proceedings, proceedings in arbitration courts;
(p. 3 in the edition of the Federal Law of 29.07.2017 N 223-FZ)

3.1) processing of personal data is necessary for the execution of a judicial act, act of another authority or official subject to execution in accordance with the legislation of the Russian Federation on enforcement proceedings (hereinafter - execution of a judicial act);
(item 3.1 introduced by the Federal Law dated 29.07.2017 N 223-FZ)

4) processing of personal data is necessary for the execution of the powers of federal executive authorities, state extra-budgetary funds, executive state authorities of the constituent entities of the Russian Federation, local self-government bodies and functions of organisations involved in the provision of state and municipal services, respectively, provided for by the Federal Law of 27 July 2010 N 210-FZ "On the organisation of the provision of state and municipal services", including the registration of the subject of personal data.
(ed. Federal Law of 05.04.2013 N 43-FZ)

5) the processing of personal data is necessary for the fulfilment of an agreement to which the personal data subject is a party or a beneficiary or guarantor, as well as for the conclusion of an agreement at the initiative of the personal data subject or an agreement under which the personal data subject will be a beneficiary or guarantor. The contract concluded with the personal data subject may not contain provisions restricting the rights and freedoms of the personal data subject, establishing cases of processing personal data of minors, unless otherwise provided for by the legislation of the Russian Federation, as well as provisions allowing inaction of the personal data subject as a condition for the conclusion of the contract;
(ed. Federal Laws of 21.12.2013 N 363-FZ, of 03.07.2016 N 231-FZ, of 14.07.2022 N 266-FZ)

6) processing of personal data is necessary for the protection of life, health or other vital interests of the personal data subject, if it is impossible to obtain the consent of the personal data subject;

7) the processing of personal data is necessary for the exercise of the rights and legitimate interests of the operator or third parties, including in cases provided for by the Federal Law "On Protection of the Rights and Legitimate Interests of Individuals in Overdue Debt Recovery Activities and on Amendments to the Federal Law "On Microfinance Activities and Microfinance Organisations", or for the achievement of socially significant goals, provided that the rights and freedoms of the personal data subject are not violated;
(ed. Federal Law of 03.07.2016 N 231-FZ)

ConsultantPlus: note.
On the identification of the constitutional and legal meaning of paragraph 8 of part 1 of Art. 6. 1 part 1 of Art. 6 see. Resolution of the Constitutional Court of the Russian Federation of 25.05.2021 N 22-P.

8) the processing of personal data is necessary for the performance of the journalist's professional activity and (or) the legitimate activity of a mass media outlet or scientific, literary or other creative activity, provided that the rights and legitimate interests of the personal data subject are not violated;

9) processing of personal data shall be carried out for statistical or other research purposes, except for the purposes specified in Article 15 of this Federal Law, subject to mandatory depersonalisation of personal data;

9.1) the processing of personal data obtained as a result of depersonalisation of personal data is carried out in order to improve the efficiency of state or municipal administration, as well as for other purposes provided for by the Federal Law of 24 April 2020 N 123-FZ "On conducting an experiment to establish special regulation to create the necessary conditions for the development and implementation of artificial intelligence technologies in the subject of the Russian Federation - the city of federal significance Moscow and amendments to Articles 6 and 10 of the Federal Law of 24 April 2020 N 123-FZ "On conducting an experiment to establish special regulation to create the necessary conditions for the development and implementation of artificial intelligence technologies in the subject of the Russian Federation - Moscow
(p. 9.1 introduced by Federal Law of 24.04.2020 N 123-FZ; in ed. by Federal Law of 02.07.2021 N 331-FZ)

10) ceased to be in force as of 1 March 2021. - Federal Law of 30.12.2020 N 519-FZ;

11) processing of personal data subject to publication or mandatory disclosure in accordance with federal law is carried out.

1.1 The processing of personal data of state protection objects and their family members shall be carried out taking into account the peculiarities stipulated by the Federal Law of 27 May 1996 N 57-FZ "On State Protection".
(part 1.1 introduced by the Federal Law dated 01.07.2017 N 148-FZ)

2 The specifics of processing of special categories of personal data, as well as biometric personal data shall be established by Articles 10 and 11 of this Federal Law, respectively.

3 The operator has the right to entrust the processing of personal data to another person with the consent of the personal data subject, unless otherwise provided for by federal law, on the basis of an agreement concluded with this person, including a state or municipal contract, or through the adoption by a state or municipal authority of a relevant act (hereinafter referred to as the operator's instruction). A person processing personal data on behalf of the operator is obliged to comply with the principles and rules of personal data processing stipulated by this Federal Law, to observe confidentiality of personal data, to take necessary measures aimed at ensuring fulfilment of obligations stipulated by this Federal Law. The operator's instruction shall define the list of personal data, the list of actions (operations) with personal data to be performed by the person processing personal data, the purposes of their processing, the obligation of such a person to observe the confidentiality of personal data, the requirements stipulated by Article 18.5 and Article 18.1 of this Federal Law, the obligation, upon request of the operator of personal data during the term of validity of the operator's instruction, including before the processing of personal data, to take the necessary measures to ensure the fulfilment of the obligations stipulated by this Federal Law.
(part 3 in the edition of the Federal Law of 14.07.2022 N 266-FZ)

4. A person processing personal data on behalf of the operator is not obliged to obtain the consent of the personal data subject to the processing of his/her personal data.

5. If the operator entrusts the processing of personal data to another person, the operator shall be liable to the subject of personal data for the actions of the said person. The person who processes personal data on behalf of the operator shall be liable to the operator.

6. If the operator entrusts the processing of personal data to a foreign individual or a foreign legal entity, the responsibility to the subject of personal data for the actions of these persons shall be borne by the operator and the person processing personal data on behalf of the operator.
(part 6 introduced by the Federal Law of 14.07.2022 N 266-FZ)

Article 7: Confidentiality of personal data

(ed. Federal Law of 25.07.2011 N 261-FZ)

Operators and other persons who have access to personal data are obliged not to disclose to third parties and not to disseminate personal data without the consent of the subject of personal data, unless otherwise provided for by federal law.

Article 8: Publicly accessible sources of personal data

1. Publicly available sources of personal data (including directories, address books) may be created for information purposes. Publicly available sources of personal data may include, with the written consent of the personal data subject, his/her surname, name, patronymic, year and place of birth, address, subscriber number, information on profession and other personal data provided by the personal data subject.
(ed. Federal Law of 25.07.2011 N 261-FZ)

2. Information about the subject of personal data shall be excluded from publicly available sources of personal data at any time at the request of the subject of personal data or by decision of the court or other authorised state bodies.
(ed. Federal Law of 25.07.2011 N 261-FZ)

Article 9. Consent of the personal data subject to the processing of his/her personal data

(ed. Federal Law of 25.07.2011 N 261-FZ)

1. The personal data subject decides to provide his/her personal data and consents to its processing freely, of his/her own free will and in his/her own interest. Consent to the processing of personal data must be specific, substantive, informed, conscious and unambiguous. Consent to the processing of personal data may be given by the subject of personal data or his/her representative in any form allowing to confirm the fact of its receipt, unless otherwise provided by federal law. In case of obtaining consent for personal data processing from the representative of the personal data subject, the authority of this representative to give consent on behalf of the personal data subject shall be verified by the operator.
(ed. Federal Law of 14.07.2022 N 266-FZ)

2. Consent to the processing of personal data may be withdrawn by the subject of personal data. In case of withdrawal of consent to processing of personal data by the subject of personal data, the operator has the right to continue processing of personal data without the consent of the subject of personal data if there are grounds specified in paragraphs 2 - 11 of Part 1 of Article 6, Part 2 of Article 10 and Part 2 of Article 11 of this Federal Law.

(3) The obligation to provide proof of obtaining the personal data subject's consent to the processing of his/her personal data or proof of the existence of the grounds specified in paragraphs 2 - 11 of Article 6, paragraph 1, paragraph 1, Article 10, paragraph 2 and Article 11, paragraph 2 of this Federal Law shall be imposed on the operator.

4. In cases provided for by the federal law, personal data processing shall be carried out only with the written consent of the personal data subject. The consent in the form of an electronic document signed in accordance with the federal law with an electronic signature shall be recognised as equal to the consent in writing on paper containing the handwritten signature of the personal data subject. The written consent of the personal data subject to the processing of his/her personal data shall include, in particular:

1) surname, name, patronymic, address of the personal data subject, number of the main personal identification document, information on the date of issue of the said document and the issuing authority;

2) surname, name, patronymic, address of the representative of the personal data subject, number of the main personal identity document, information on the date of issue of the said document and the issuing authority, details of the power of attorney or other document confirming the powers of this representative (when obtaining consent from the representative of the personal data subject);

3) the name or surname, first name, patronymic and address of the operator receiving the consent of the personal data subject;

4) the purpose of personal data processing;

5) the list of personal data, for the processing of which the consent of the personal data subject is given;

6) the name or surname, first name, patronymic and address of the person who processes personal data on behalf of the operator, if the processing will be entrusted to such a person;

7) list of actions with personal data, for the performance of which consent is given, general description of the methods of personal data processing used by the operator;

8) the period during which the consent of the personal data subject is valid, as well as the method of its withdrawal, unless otherwise provided for by the federal law;

9) signature of the personal data subject.

5. The procedure for obtaining in the form of an electronic document the consent of a personal data subject to the processing of his/her personal data for the purposes of providing state and municipal services, as well as services that are necessary and mandatory for the provision of state and municipal services, shall be established by the Government of the Russian Federation.

6. In case of incapacity of the personal data subject, the consent to the processing of his/her personal data shall be given by the legal representative of the personal data subject.

7. In case of death of the personal data subject, consent to the processing of his/her personal data shall be given by the heirs of the personal data subject, if such consent was not given by the personal data subject during his/her lifetime.

8. Personal data may be obtained by the operator from a person who is not the subject of personal data, provided that the operator is provided with confirmation of the existence of the grounds specified in paragraphs 2 - 11 of Article 6, paragraph 1, paragraph 1, Article 10, paragraph 2 and Article 11, paragraph 2 of this Federal Law.

9. The requirements for the content of the consent to the processing of personal data allowed by the personal data subject for dissemination shall be established by the authorised body for the protection of the rights of personal data subjects.
(part 9 introduced by the Federal Law of 30.12.2020 N 519-FZ)

Article 10. Special categories of personal data

1. Processing of special categories of personal data concerning racial, national origin, political opinions, religious or philosophical beliefs, state of health, intimate life is not allowed, except for the cases provided for in paragraphs 2 and 2.1 of this Article.
(ed. Federal Law of 24.04.2020 N 123-FZ)

2 The processing of special categories of personal data referred to in paragraph 1 of this Article shall be allowed in cases where:

1) the personal data subject has consented in writing to the processing of his/her personal data;

2) the processing of personal data authorised by the personal data subject for dissemination shall be carried

out in compliance with the prohibitions and conditions provided for by Article 10.1 of this Federal Law;
(paragraph 2 in the edition of the Federal Law of 30.12.2020 N 519-FZ)

2.1) processing of personal data is necessary in connection with the implementation of international readmission agreements of the Russian Federation;
(item 2.1 introduced by the Federal Law dated 25.11.2009 N 266-FZ)

2.2) personal data processing is carried out in accordance with the Federal Law of 25 January 2002 N 8-FZ "On the All-Russian Population Census";
(paragraph 2.2 introduced by the Federal Law of 27.07.2010 N 204-FZ)

2.3) processing of personal data is carried out in accordance with the legislation on state social assistance, labour legislation, pension legislation of the Russian Federation;
(p. 2.3 introduced by Federal Law of 25.07.2011 N 261-FZ, in the edition of Federal Law of 21.07.2014 N 216-FZ)

3) processing of personal data is necessary to protect the life, health or other vital interests of the personal data subject or the life, health or other vital interests of other persons and it is impossible to obtain the consent of the personal data subject;
(paragraph 3 in the edition of the Federal Law of 25.07.2011 N 261-FZ)

4) personal data processing is carried out for medical and preventive purposes, in order to establish a medical diagnosis, to provide medical and medical-social services, provided that personal data processing is carried out by a person professionally engaged in medical activity and obliged to keep medical confidentiality in accordance with the legislation of the Russian Federation;

5) processing of personal data of members (participants) of a public association or religious organisation shall be carried out by the respective public association or religious organisation, acting in accordance with the legislation of the Russian Federation, in order to achieve the legitimate purposes provided for in their constituent documents, provided that the personal data will not be disseminated without the consent in writing of the personal data subjects;

6) the processing of personal data is necessary for establishing or exercising the rights of the personal data subject or third parties, as well as in connection with the exercise of justice;
(paragraph 6 in the edition of the Federal Law of 25.07.2011 N 261-FZ)

7) processing of personal data shall be carried out in accordance with the legislation of the Russian Federation on defence, security, counter-terrorism, transport security, anti-corruption, operative-search activity, enforcement proceedings, criminal enforcement legislation of the Russian Federation;
(paragraph 7 in the edition of the Federal Law of 25.07.2011 N 261-FZ)

7.1) processing of personal data obtained in cases established by the legislation of the Russian Federation shall be carried out by prosecutor's offices in connection with their prosecutorial supervision;
(item 7.1 introduced by the Federal Law dated 23.07.2013 N 205-FZ)

8) processing of personal data shall be carried out in accordance with the legislation on compulsory types of insurance, insurance legislation;
(paragraph 8 in the edition of the Federal Law of 25.07.2011 N 261-FZ)

9) processing of personal data is carried out in cases stipulated by the legislation of the Russian Federation, by state bodies, municipal bodies or organisations for the purpose of placement of children left without parental care in the families of citizens;
(paragraph 9 introduced by the Federal Law of 25.07.2011 N 261-FZ)

10) processing of personal data shall be carried out in accordance with the legislation of the Russian Federation on citizenship of the Russian Federation.
(paragraph 10 introduced by the Federal Law of 04.06.2014 N 142-FZ)

2.1 The processing of personal data related to the state of health, obtained as a result of depersonalisation

of personal data, is allowed in order to improve the efficiency of state or municipal administration, as well as for other purposes provided for by the Federal Law of 24 April 2020 N 123-FZ "On conducting an experiment to establish a special regulation to create the necessary conditions for the development and implementation of artificial intelligence technologies in the subject of the Russian Federation - the city of federal significance Moscow and the introduction of artificial intelligence technologies in the subject of the Russian Federation - the city of federal significance Moscow".
(part 2.1 introduced by Federal Law of 24.04.2020 N 123-FZ; in ed. by Federal Law of 02.07.2021 N 331-FZ)

3. processing of personal data on criminal record may be carried out by state bodies or municipal bodies within the limits of powers granted to them in accordance with the legislation of the Russian Federation, as well as by other persons in cases and in the manner determined in accordance with federal laws.

4 The processing of special categories of personal data, carried out in the cases provided for in paragraphs 2 and 3 of this Article, shall be immediately stopped if the reasons for which the processing was carried out are eliminated, unless otherwise provided for by federal law.
(ed. Federal Law of 25.07.2011 N 261-FZ)

Article 10.1. Peculiarities of processing personal data authorised by the personal data subject for dissemination

(introduced by the Federal Law of 30.12.2020 N 519-FZ)

1. Consent to processing of personal data authorised by the subject of personal data for dissemination shall be executed separately from other consents of the subject of personal data to processing of his/her personal data. The Operator shall provide the personal data subject with an opportunity to determine the list of personal data for each category of personal data specified in the consent to processing of personal data authorised by the personal data subject for dissemination.

2. In case of disclosure of personal data to an indefinite number of persons by the subject of personal data himself without giving the operator the consent provided for by this Article, the obligation to provide evidence of the legality of subsequent dissemination or other processing of such personal data shall be borne by each person who carried out such dissemination or other processing.

3. If personal data have been disclosed to an indefinite number of persons due to an offence, crime or force majeure circumstances, the obligation to provide evidence of the lawfulness of subsequent dissemination or other processing of such personal data rests with each person who has disseminated or otherwise processed such personal data.

4. If it does not follow from the consent provided by the personal data subject to the processing of personal data authorised by the personal data subject for dissemination that the personal data subject has consented to the dissemination of personal data, such personal data shall be processed by the operator to whom they have been provided by the personal data subject without the right of dissemination.

5. In case it does not follow from the consent provided by the personal data subject to the processing of personal data authorised by the personal data subject for dissemination that the personal data subject has not established prohibitions and conditions for the processing of personal data provided for in paragraph 9 of this Article, or if the consent provided by the personal data subject does not specify the categories and list of personal data for the processing of which the personal data subject establishes conditions and prohibitions in accordance with paragraph 9 of this Article.

6. Consent to the processing of personal data authorised by the personal data subject for dissemination may be granted to the operator:

1) directly;

2) using the information system of the authorised body for the protection of the rights of personal data subjects.

7. The rules of use of the information system of the authorised body for the protection of the rights of personal data subjects, including the procedure of interaction of the personal data subject with the operator, shall be determined by the authorised body for the protection of the rights of personal data subjects.

8. The silence or inaction of the personal data subject may under no circumstances be considered consent to the processing of personal data authorised by the personal data subject for dissemination.

9. In the consent to the processing of personal data authorised by the subject of personal data for dissemination, the subject of personal data has the right to establish prohibitions on the transfer (except for granting access) of these personal data by the operator to an unlimited number of persons, as well as prohibitions on the processing or conditions of processing (except for obtaining access) of these personal data by an unlimited number of persons. Refusal of the operator to establish by the subject of personal data the prohibitions and conditions stipulated by this Article is not allowed.

10. The Operator shall be obliged to publish information on the conditions of processing and the existence of prohibitions and conditions for processing by an unlimited number of persons of personal data authorised by the personal data subject for dissemination within three working days from the date of obtaining the relevant consent of the personal data subject.

11. The prohibitions established by the personal data subject on the transfer (except for granting access), as well as on the processing or conditions of processing (except for obtaining access) of personal data authorised by the personal data subject for dissemination shall not apply to cases of personal data processing in the state, public and other public interests defined by the legislation of the Russian Federation.

12. The transfer (dissemination, provision, access) of personal data authorised by the subject of personal data for dissemination shall be stopped at any time at the request of the subject of personal data. This request shall include the surname, first name, patronymic (if any), contact information (telephone number, e-mail address or postal address) of the personal data subject, as well as a list of personal data whose processing is to be stopped. The personal data specified in this request may be processed only by the operator to whom it is sent.

13. The validity of the personal data subject's consent to the processing of personal data authorised by the personal data subject for dissemination shall be terminated from the moment the operator receives the request specified in paragraph 12 of this Article.

14. The subject of personal data has the right to address with a demand to stop the transfer (dissemination, provision, access) of his personal data, previously authorised by the subject of personal data for dissemination, to any person processing his personal data in case of non-compliance with the provisions of this Article or to address such a demand to the court. Such person shall be obliged to stop the transfer (dissemination, provision, access) of personal data within three working days from the moment of receipt of the personal data subject's request or within the term specified in the court decision that has entered into legal force, and if such term is not specified in the court decision, then within three working days from the moment the court decision enters into legal force.

15. The requirements of this Article shall not apply in the case of processing of personal data for the purpose of fulfilment of functions, powers and duties imposed by the legislation of the Russian Federation on state bodies, municipal bodies, as well as on organisations subordinated to such bodies.
(part 15 in the edition of the Federal Law of 14.07.2022 N 266-FZ)

Article 11: Biometric personal data

(ed. Federal Law of 25.07.2011 N 261-FZ)

1. Information that characterises physiological and biological features of a person, on the basis of which it is possible to establish his/her identity (biometric personal data) and which is used by the operator to establish the identity of the personal data subject, may be processed only with the written consent of the personal data subject, except in cases provided for in paragraph 2 of this Article.

2 Biometric personal data may be processed without the consent of the personal data subject in connection with the implementation of international readmission agreements of the Russian Federation, in connection with

the administration of justice and the execution of judicial acts, in connection with mandatory state fingerprint registration, mandatory state genomic registration, as well as in cases stipulated by the legislation of the Russian Federation on defence, on security, on countering terrorism, on transport security, and also in cases stipulated by the legislation of the Russian Federation on defence, on security, on countering terrorism, and on transport security
(ed. Federal Laws of 04.06.2014 N 142-FZ, of 31.12.2017 N 498-FZ, of 27.12.2019 N 480-FZ, of 06.02.2023 N 8-FZ)

3. Provision of biometric personal data may not be mandatory, except for cases provided for by Part 2 of this Article. The operator shall not have the right to refuse service in case the personal data subject refuses to provide biometric personal data and (or) give consent to the processing of personal data, if, in accordance with the federal law, obtaining the operator's consent to the processing of personal data is not mandatory.
(part 3 introduced by the Federal Law of 14.07.2022 N 266-FZ)

Article 12: Transborder transfer of personal data
(ed. Federal Law of 14.07.2022 N 266-FZ)

1. cross-border transfer of personal data shall be carried out in accordance with this Federal Law and international treaties of the Russian Federation.

2. The competent authority for the protection of the rights of personal data subjects shall approve the list of foreign states ensuring adequate protection of the rights of personal data subjects. The list of foreign states ensuring adequate protection of the rights of personal data subjects shall include the states that are parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, as well as foreign states that are not parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, provided that the legal provisions in force in the respective state and the measures applied to ensure the protection of the rights of personal data subjects comply with the provisions of the said Convention.

3. The operator shall notify the authorised body for the protection of the rights of personal data subjects of its intention to carry out transborder transfer of personal data prior to the commencement of transborder transfer of personal data. This notification shall be sent separately from the notification of intention to carry out personal data processing provided for by Article 22 of this Federal Law.

4. The notification provided for in paragraph 3 of this Article shall be sent in the form of a document on paper or in the form of an electronic document and shall be signed by an authorised person. The notification on the intention to carry out transborder transfer of personal data shall contain the following information:

1) the name (surname, first name, patronymic), address of the operator, as well as the date and number of the notice of intention to process personal data previously sent by the operator in accordance with Article 22 of this Federal Law;

2) name (surname, first name, patronymic) of the person responsible for the organisation of personal data processing, contact telephone numbers, postal and e-mail addresses;

3) legal basis and purpose of transborder transfer of personal data and further processing of transferred personal data;

4) categories and list of personal data to be transferred;

5) categories of personal data subjects whose personal data are transferred;

6) the list of foreign states in the territory of which the transborder transfer of personal data is planned;

7) the date of the operator's assessment of compliance by foreign authorities, foreign natural persons, foreign legal entities, to whom the transborder transfer of personal data is planned, with the confidentiality of personal data and ensuring the security of personal data during their processing.

5. Before submitting the notification provided for in paragraph 3 of this Article, the operator shall be obliged to obtain the following information from the authorities of a foreign state, foreign natural persons, foreign legal entities to whom a trans-border transfer of personal data is planned:

1) information on measures taken by foreign authorities, foreign natural persons, foreign legal entities, to whom transborder transfer of personal data is planned, to protect the transferred personal data and on the conditions of termination of their processing;

2) information on the legal regulation in the field of personal data of the foreign state under whose jurisdiction the authorities of the foreign state, foreign natural persons, foreign legal entities, to whom the transborder transfer of personal data is planned (in case the transborder transfer of personal data to the authorities of the foreign state, foreign natural persons, foreign legal entities under the jurisdiction of the foreign state is planned, not being a

3) information on foreign state authorities, foreign natural persons, foreign legal entities to whom the trans-border transfer of personal data is planned (name or surname, first name and patronymic, as well as contact telephone numbers, postal addresses and e-mail addresses).

6. In order to assess the reliability of the information contained in the operator's notification of its intention to perform transborder transfer of personal data, the information provided for in paragraphs 1 - 3 of point 5 of this Article shall be provided by the operator upon request of the authorised body for the protection of the rights of personal data subjects within ten working days from the date of receipt of such request. The said term may be extended, but not more than for five working days in case the operator sends a motivated notification to the authorised body for the protection of the rights of personal data subjects, indicating the reasons for extending the term for providing the requested information.

7. Transborder transfer of personal data may be prohibited or restricted in order to protect the foundations of the constitutional order of the Russian Federation, morality, health, rights and legitimate interests of citizens, to ensure national defence and security of the state, to protect the economic and financial interests of the Russian Federation, to ensure by diplomatic and international legal means the protection of the rights, freedoms and interests of citizens of the Russian Federation, sovereignty, security, territorial integrity of the Russian Federation and its other constituent entities, and to protect the rights, freedoms and interests of the Russian Federation.

8. The decision on prohibition or restriction of transborder transfer of personal data for the protection of morality, health, rights and legitimate interests of citizens shall be adopted by the authorised body for the protection of the rights of personal data subjects, based on the results of examination of the notification provided for in paragraph 3 of this Article.

9. The decision specified in paragraph 8 of this Article shall be adopted by the authorised body for the protection of the rights of personal data subjects within ten working days from the date of receipt of the notification provided for in paragraph 3 of this Article, in accordance with the procedure established by the Government of the Russian Federation. In case the authorised body for the protection of the rights of personal data subjects sends a request in accordance with paragraph 6 of this Article, the examination of such notification shall be suspended until the date of submission by the operator of the requested information.

10. After sending the notification referred to in paragraph 3 of this Article, the operator shall have the right to carry out transborder transfer of personal data in the territories of the foreign states specified in such notification, which are parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data or are included in the list provided for in paragraph 2 of this Article, until the adoption of the decision referred to in paragraph 8 or 12 of this Article.

11. After sending the notification provided for in paragraph 3 of this Article, the operator, until the expiry of the terms specified in paragraph 9 of this Article, shall not be entitled to carry out transborder transfer of personal data to the territory of foreign states specified in the notification, which are not parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and are not included in the list provided for in paragraph 2 of this Article, except for the case when such transborder transfer of personal data is necessary for the protection of individuals with regard to automatic processing of

personal data.

12. The decision on prohibition or restriction of transborder transfer of personal data shall be adopted by the authorised body for the protection of the rights of personal data subjects in order to:

1) protection of the foundations of the constitutional order of the Russian Federation and the security of the state - upon the submission of the federal executive body authorised in the field of security;

2) ensuring the defence of the country - upon submission by the federal executive body authorised in the field of defence;

3) protection of economic and financial interests of the Russian Federation - upon submission by federal executive authorities authorised by the President of the Russian Federation or the Government of the Russian Federation;

4) ensuring by diplomatic and international legal means the protection of the rights, freedoms and interests of citizens of the Russian Federation, sovereignty, security, territorial integrity of the Russian Federation and other interests of the Russian Federation in the international arena - upon the submission of the federal executive authority responsible for the development and implementation of state policy and normative-legal regulation in the sphere of international relations of the Russian Federation.

13. The decision provided for in paragraph 12 of this Article shall be adopted by the authorised body for the protection of the rights of personal data subjects within five working days from the date of receipt of the relevant submission. The procedure for adopting such a decision and the procedure for informing operators of the adopted decision shall be established by the Government of the Russian Federation.

14. In case the authorised body for the protection of the rights of personal data subjects adopts the decision provided for in paragraph 8 or 12 of this Article, the operator shall be obliged to ensure the destruction by the foreign state authority, foreign natural person, foreign legal entity of the personal data previously transferred to them.

15. The Government of the Russian Federation shall determine the cases in which the requirements of Parts 3 - 6, 8 - 11 of this Article shall not apply to operators carrying out trans-border transfer of personal data for the purpose of fulfilment of functions, powers and obligations imposed on state bodies, municipal bodies by an international treaty of the Russian Federation, legislation of the Russian Federation.

Article 13. Peculiarities of personal data processing in state or municipal information systems of personal data

1. State bodies, municipal bodies shall create, within the limits of their powers established in accordance with federal laws, state or municipal information systems of personal data.

2. Federal laws may establish peculiarities of personal data recording in state and municipal information systems of personal data, including the use of different ways of marking the belonging of personal data contained in the relevant state or municipal information system of personal data to a particular subject of personal data.

3. Human and civil rights and freedoms may not be restricted for reasons related to the use of different methods of personal data processing or designation of the affiliation of personal data contained in state or municipal information systems of personal data to a particular subject of personal data. It is not allowed to use methods that offend the feelings of citizens or humiliate human dignity to indicate the affiliation of personal data contained in the state or municipal information systems of personal data to a particular personal data subject.

4. In order to ensure the realisation of the rights of personal data subjects in connection with the processing of their personal data in state or municipal information systems of personal data, a state register of population may be created, the legal status of which and the procedure for working with it shall be established by federal law.

Chapter 3: PERSONAL DATA SUBJECT RIGHTS

Article 14. The right of the personal data subject to access his/her personal data

(ed. Federal Law of 25.07.2011 N 261-FZ)

1. The subject of personal data has the right to receive the information specified in paragraph 7 of this Article, except in cases provided for in paragraph 8 of this Article. The subject of personal data has the right to demand from the operator to clarify his/her personal data, block or destroy it if the personal data is incomplete, outdated, inaccurate, illegally obtained or not necessary for the stated purpose of processing, as well as to take measures provided for by law to protect his/her rights.

2. The information specified in paragraph 7 of this Article shall be provided to the subject of personal data by the operator in an accessible form, and shall not contain personal data relating to other subjects of personal data, unless there are legitimate grounds for disclosure of such personal data.

3. The information specified in paragraph 7 of this Article shall be provided to the personal data subject or his/her representative by the operator within ten working days from the moment of application or receipt by the operator of the request of the personal data subject or his/her representative. The specified term may be extended, but not more than for five working days in case the operator sends to the address of the personal data subject a motivated notification indicating the reasons for extending the term for providing the requested information. The request shall contain the number of the main personal data subject's or his/her representative's identity document, information on the date of issue of the said document and the issuing authority, information confirming the personal data subject's participation in relations with the operator (contract number, date of contract conclusion, conventional word designation and (or) other information), or information otherwise confirming the fact of personal data processing by the operator, signature of the personal data subject or his/her representative. The request may be sent in the form of an electronic document and signed with an electronic signature in accordance with the legislation of the Russian Federation. The operator shall provide the information specified in paragraph 7 of this Article to the personal data subject or his/her representative in the form in which the relevant application or request was sent, unless otherwise specified in the application or request.
(ed. Federal Law of 14.07.2022 N 266-FZ)

4. In case the information referred to in paragraph 7 of this Article, as well as the processed personal data were provided for familiarisation to the personal data subject upon his/her request, the personal data subject has the right to reapply to the operator or to send him/her a repeated request in order to obtain the information referred to in paragraph 7 of this Article and familiarisation with such personal data not earlier than thirty days after the initial application or sending the initial request, unless a shorter term is established by the federal law of the Republic of Moldova.

5. The personal data subject has the right to reapply to the operator or to send him/her a repeated request in order to obtain the information specified in paragraph 7 of this Article, as well as in order to familiarise himself/herself with the processed personal data before the expiry of the term specified in paragraph 4 of this Article, if such information and (or) the processed personal data were not provided to him/her for familiarisation in full following the results of consideration of the initial request. The repeated request, along with the information specified in paragraph 3 of this Article, shall contain the justification for the repeated request.

6. The operator shall have the right to refuse the personal data subject to fulfil a repeated request that does not meet the conditions provided for in paragraphs 4 and 5 of this Article. Such refusal shall be motivated. The obligation to provide evidence of the justification of the refusal to fulfil a repeated request lies with the operator.

7. The personal data subject has the right to receive information regarding the processing of his/her personal data, including information containing:

1) confirmation of the fact of personal data processing by the operator;

2) legal grounds and purposes of personal data processing;

3) the purposes and methods of personal data processing applied by the operator;

4) name and location of the operator, information about persons (except for the operator's employees) who have access to personal data or to whom personal data may be disclosed on the basis of a contract with the operator or on the basis of federal law;

5) processed personal data related to the respective personal data subject, the source of their obtaining, unless another procedure for submission of such data is provided for by the federal law;

6) the terms of personal data processing, including the terms of their storage;

7) the procedure for exercising by the personal data subject of the rights provided for by this Federal Law;

8) information on transborder data transfers that have taken place or are expected to take place;

9) the name or surname, first name, patronymic and address of the person who processes personal data on behalf of the operator, if the processing is or will be entrusted to such a person;

9.1) information on the ways in which the operator fulfils the obligations established by Article 18.1 of this Federal Law;
(item 9.1 introduced by the Federal Law of 14.07.2022 N 266-FZ)

10) other information provided for by this Federal Law or other federal laws.

8. The right of the subject of personal data to access his/her personal data may be restricted in accordance with federal laws, including if:

1) processing of personal data, including personal data obtained as a result of operative investigation, counterintelligence and intelligence activities, shall be carried out for the purposes of national defence, state security and law enforcement;

2) personal data processing is carried out by the authorities that have detained the personal data subject on suspicion of committing a crime, or that have charged the personal data subject in a criminal case, or that have applied a preventive measure to the personal data subject prior to the indictment, except for cases provided for by the criminal procedure legislation of the Russian Federation, if the familiarisation of the suspect or the accused with such personal data is allowed;

3) processing of personal data shall be carried out in accordance with the legislation on combating money laundering and terrorism financing;

4) the personal data subject's access to his/her personal data violates the rights and legitimate interests of third parties;

5) processing of personal data shall be carried out in cases stipulated by the legislation of the Russian Federation on transport security in order to ensure sustainable and safe functioning of the transport complex, to protect the interests of individuals, society and the state in the sphere of the transport complex from acts of unlawful interference.

Article 15. Rights of personal data subjects when processing their personal data for the purpose of promoting goods, works, services on the market, as well as for political agitation purposes

1. Processing of personal data for the purpose of promotion of goods, works, services on the market by means of direct contacts with potential consumers through means of communication, as well as for political campaigning purposes is allowed only with the prior consent of the personal data subject. The said processing of personal data is recognised as being carried out without the prior consent of the personal data subject, unless the operator proves that such consent was obtained.

2. the Operator shall be obliged to immediately cease, at the request of the personal data subject, the processing of his/her personal data referred to in paragraph 1 of this Article.

Article 16. Rights of personal data subjects when taking decisions on the basis of exclusively automated processing of their personal data

1. It is prohibited to take decisions based solely on automated processing of personal data that give rise to legal consequences with regard to the personal data subject or otherwise affect his/her rights and legitimate interests, except for the cases provided for in paragraph 2 of this Article.

2. A decision generating legal consequences in relation to the personal data subject or otherwise affecting his/her rights and legitimate interests may be made on the basis of exclusively automated processing of his/her personal data only with the consent in writing of the personal data subject or in cases provided for by federal laws establishing also measures to ensure observance of the rights and legitimate interests of the personal data subject.

3. the Operator is obliged to explain to the personal data subject the procedure of decision-making on the basis of exclusively automated processing of his/her personal data and the possible legal consequences of such decision, to provide the possibility to object to such decision, as well as to explain the procedure of defence by the personal data subject of his/her rights and legitimate interests.

4. the Operator shall be obliged to consider the objection referred to in paragraph 3 of this Article within thirty days from the date of its receipt and notify the personal data subject of the results of consideration of such objection.
(ed. Federal Law of 25.07.2011 N 261-FZ)

Article 17. Right to appeal against actions or omissions of the operator

1. If the subject of personal data believes that the operator processes his/her personal data in violation of the requirements of this Federal Law or otherwise violates his/her rights and freedoms, the subject of personal data has the right to appeal against the actions or inaction of the operator to the authorised body for the protection of the rights of subjects of personal data or in court.

2. The subject of personal data has the right to protect his/her rights and legitimate interests, including compensation for losses and (or) compensation for moral damage in court.

Chapter 4: DUTIES OF THE OPERATOR

Article 18. Obligations of the operator when collecting personal data
(ed. Federal Law of 25.07.2011 N 261-FZ)

1. When collecting personal data, the operator shall be obliged to provide the subject of personal data, at his request, with the information provided for in paragraph 7 of Article 14 of this Federal Law.

2. If, in accordance with federal law, providing personal data and (or) obtaining consent to the processing of personal data by the operator is mandatory, the operator shall explain to the subject of personal data the legal consequences of refusal to provide his/her personal data and (or) consent to their processing.
(part 2 in the edition of the Federal Law of 14.07.2022 N 266-FZ)

3. If personal data are not obtained from the personal data subject, the operator, except in cases provided for in paragraph 4 of this Article, shall be obliged to provide the following information to the personal data subject prior to the commencement of processing of such personal data:

1) name or surname, first name, patronymic and address of the operator or its representative;

2) the purpose of personal data processing and its legal basis;

2.1) list of personal data;
(item 2.1 introduced by the Federal Law of 14.07.2022 N 266-FZ)

3) the intended users of the personal data;

4) the rights of the personal data subject established by this Federal Law;

5) the source of obtaining personal data.

4. the Operator shall be released from the obligation to provide the personal data subject with the information provided for in paragraph 3 of this Article in cases where:

1) the personal data subject is notified about the processing of his/her personal data by the respective operator;

2) the personal data have been obtained by the operator on the basis of federal law or in connection with the execution of an agreement to which the personal data subject is a party, beneficiary or guarantor;

3) processing of personal data authorised by the personal data subject for dissemination shall be carried out in compliance with the prohibitions and conditions stipulated in Article 10.1 of this Federal Law;
(paragraph 3 in the edition of the Federal Law of 30.12.2020 N 519-FZ)

4) the operator processes personal data for statistical or other research purposes, for carrying out the professional activity of a journalist or scientific, literary or other creative activity, if the rights and legitimate interests of the personal data subject are not violated;

5) the provision to the personal data subject of the information provided for in paragraph 3 of this Article violates the rights and legitimate interests of third parties.

5. When collecting personal data, including through the information and telecommunications network "Internet", the operator is obliged to ensure the recording, systematisation, accumulation, storage, clarification (update, change), extraction of personal data of citizens of the Russian Federation using databases located on the territory of the Russian Federation, except for cases specified in paragraphs 2, 3, 4, 8 of Part 1 of Article 6 of this Federal Law.
(part 5 introduced by the Federal Law of 21.07.2014 N 242-FZ)

Article 18.1 Measures to ensure that the operator fulfils its obligations under this Federal Law

(introduced by Federal Law of 25.07.2011 N 261-FZ)

1 The Operator shall be obliged to take measures necessary and sufficient to ensure fulfilment of the obligations stipulated by this Federal Law and regulatory legal acts adopted in accordance with it. The Operator shall independently determine the composition and the list of measures necessary and sufficient to ensure fulfilment of obligations stipulated by this Federal Law and regulatory legal acts adopted in accordance therewith, unless otherwise stipulated by this Federal Law or other federal laws. Such measures include, in particular, the following:
(ed. Federal Law of 14.07.2022 N 266-FZ)

1) appointment by the operator, which is a legal entity, of the person responsible for organising the processing of personal data;

2) issuance by the operator, which is a legal entity, of documents defining the operator's policy with regard to personal data processing, local acts on personal data processing issues, defining for each purpose of personal data processing the categories and list of processed personal data, categories of subjects whose personal data are processed, methods, terms of their processing and storage, the procedure of personal data destruction upon achievement of the purposes of their processing or upon occurrence of other legal grounds, as well as the procedure of personal data destruction. Such documents and local acts may not contain provisions restricting the rights of personal data subjects, as well as imposing on the operators powers and obligations not provided for by the legislation of the Russian Federation;
(paragraph 2 in the edition of the Federal Law of 14.07.2022 N 266-FZ)

3) application of legal, organisational and technical measures to ensure the security of personal data in accordance with Article 19 of this Federal Law;

4) internal control and (or) audit of compliance of personal data processing with this Federal Law and regulatory legal acts adopted in accordance with it, personal data protection requirements, the operator's policy on personal data processing, local acts of the operator;

5) assessment of damage in accordance with the requirements established by the authorised body for the protection of the rights of personal data subjects, which may be caused to personal data subjects in case of violation of this Federal Law, the correlation between the said damage and the measures taken by the operator aimed at ensuring the fulfilment of the obligations stipulated by this Federal Law;
(ed. Federal Law of 14.07.2022 N 266-FZ)

6) familiarisation of the operator's employees directly involved in personal data processing with the provisions of the Russian Federation legislation on personal data, including requirements to personal data protection, documents defining the operator's policy on personal data processing, local acts on personal data processing, and (or) training of the said employees.

2. the Operator is obliged to publish or otherwise provide unrestricted access to the document defining its policy on personal data processing, to the information on the personal data protection requirements implemented. The operator collecting personal data using information and telecommunication networks is obliged to publish in the relevant information and telecommunication network, including on the pages of the operator's website in the information and telecommunication network "Internet", through which personal data are collected, the document defining its policy on personal data processing and information on the implemented requirements to personal data protection, as well as to ensure the possibility of access to the document, which defines its policy on personal data processing and information on the implemented requirements to personal data protection.
(ed. Federal Law of 14.07.2022 N 266-FZ)

3. The Government of the Russian Federation shall establish a list of measures aimed at ensuring the fulfilment of the obligations stipulated by this Federal Law and the regulatory legal acts adopted in accordance therewith by operators that are state or municipal bodies.

4. the Operator shall be obliged to submit documents and local acts referred to in paragraph 1 of this Article and (or) otherwise confirm the adoption of the measures referred to in paragraph 1 of this Article upon the request of the authorised body for the protection of the rights of personal data subjects.

Article 19. Measures to ensure the security of personal data during their processing

(ed. Federal Law of 25.07.2011 N 261-FZ)

1 When processing personal data, the Operator is obliged to take the necessary legal, organisational and technical measures or ensure their adoption to protect personal data from unlawful or accidental access to them, destruction, modification, blocking, copying, provision, dissemination of personal data, as well as from other unlawful actions in relation to personal data.

2. ensuring the security of personal data shall be achieved, inter alia:

1) determination of threats to the security of personal data during their processing in personal data information systems;

2) application of organisational and technical measures to ensure the security of personal data during their processing in personal data information systems, necessary to meet the requirements to personal data protection, the execution of which ensures the levels of personal data protection established by the Government of the Russian Federation;

3) the use of information protection means that have passed the conformity assessment procedure in accordance with the established procedure;

4) assessment of the effectiveness of the measures taken to ensure personal data security before putting into operation of the personal data information system;

5) taking into account machine-readable personal data carriers;

6) detection of facts of unauthorised access to personal data and taking measures, including measures to detect, prevent and eliminate the consequences of computer attacks on personal data information systems and to respond to computer incidents therein;
(ed. Federal Law of 30.12.2020 N 515-FZ)

7) recovery of personal data modified or destroyed due to unauthorised access to them;

8) establishing rules of access to personal data processed in the personal data information system, as well as ensuring the registration and recording of all actions performed with personal data in the personal data information system;

9) control over the measures taken to ensure personal data security and the level of protection of personal data information systems.

3. The Government of the Russian Federation, taking into account possible harm to the subject of personal data, the volume and content of personal data processed, the type of activity in the performance of which personal data are processed, the relevance of threats to the security of personal data, shall establish:

1) levels of protection of personal data during their processing in personal data information systems depending on the security threats of such data;

2) requirements for the protection of personal data during their processing in personal data information systems, the fulfilment of which ensures the established levels of personal data protection;

3) requirements for material carriers of biometric personal data and technologies for storing such data outside personal data information systems.

4. The composition and content of the requirements for the protection of personal data for each level of security, organisational and technical measures to ensure the security of personal data during their processing in personal data information systems established by the Government of the Russian Federation in accordance with part 3 of this Article shall be established by the federal executive body authorised in the field of security and the federal executive body authorised in the field of information systems.

5. Federal executive authorities that are responsible for the development of state policy and normative and legal regulation in the established sphere of activity, state authorities of constituent entities of the Russian Federation, the Bank of Russia, bodies of state non-budgetary funds, other state authorities, within the limits of their powers, shall adopt normative legal acts that define threats to personal data security relevant to the processing of personal data in personal data information systems, ex

6. Along with the threats to personal data security defined in the normative legal acts adopted in accordance with paragraph 5 of this Article, associations, unions and other associations of operators have the right to define by their decisions additional threats to personal data security relevant for personal data processing in personal data information systems operated in the course of certain types of activities by members of such associations, unions and other associations of operators, taking into account the content of personal data.

7. Draft regulatory legal acts referred to in part 5 of this Article shall be subject to coordination with the federal executive body authorised in the field of ensuring security and the federal executive body authorised in the field of countering technical intelligence and technical protection of information. Draft decisions referred to in part 6 of this Article shall be subject to coordination with the federal executive body authorised in the field of security and the federal executive body authorised in the field of countering technical intelligence and technical protection of information in accordance with the procedure established by the Government of the Russian Federation. The decision of the federal executive power body authorised in the field of ensuring security and the federal executive power body authorised in the field of countering technical intelligence and technical protection of information to refuse to approve the draft decisions referred to in Part 6 of this Article shall be motivated.

8. Control and supervision over the implementation of organisational and technical measures to ensure the

security of personal data, established in accordance with this Article, during the processing of personal data in the state information systems of personal data shall be exercised by the federal executive body authorised in the field of security and the federal executive body authorised in the field of countering technical intelligence and technical protection of information, within the limits of their powers and without the need to take measures to ensure the security of personal data in the state information systems of personal data

9. The federal executive authority authorised in the field of security and the federal executive authority authorised in the field of countering technical intelligence and technical protection of information, by decision of the Government of the Russian Federation, taking into account the significance and content of the processed personal data, may be vested with the authority to monitor the implementation of organisational and technical measures to ensure the security of personal data established in accordance with this Article, in the course of their processing.

10. The use and storage of biometric personal data outside the personal data information systems may be carried out only on such material data carriers and with the use of such storage technology, which ensure the protection of these data from unlawful or accidental access to them, their destruction, modification, blocking, copying, provision, dissemination.

11. For the purposes of this Article, threats to the security of personal data shall mean a set of conditions and factors that create a danger of unauthorised, including accidental, access to personal data, which may result in the destruction, modification, blocking, copying, provision, dissemination of personal data, as well as other unlawful actions during their processing in the information system of personal data. The level of personal data security is understood as a complex indicator characterising the requirements, the execution of which ensures the neutralisation of certain threats to the security of personal data during their processing in personal data information systems.

12. The Operator shall, in accordance with the procedure determined by the federal executive body authorised in the field of security, ensure interaction with the state system of detection, prevention and liquidation of consequences of computer attacks on information resources of the Russian Federation, including informing it about computer incidents resulting in unlawful transfer (provision, distribution, access) of personal data.
(part 12 introduced by the Federal Law of 14.07.2022 N 266-FZ)

13. The information specified in paragraph 12 of this Article (except for information constituting a state secret) shall be transferred by the federal executive body authorised in the field of security to the authorised body for the protection of the rights of personal data subjects.
(part 13 introduced by the Federal Law of 14.07.2022 N 266-FZ)

14. The procedure for the transfer of information in accordance with paragraph 13 of this Article shall be established jointly by the federal executive body authorised in the field of security and the authorised body for the protection of the rights of personal data subjects.
(part 14 introduced by the Federal Law of 14.07.2022 N 266-FZ)

Article 20. Obligations of the operator when the personal data subject appeals to him or when receiving the request of the personal data subject or his representative, as well as the authorised body for the protection of the rights of personal data subjects

(ed. Federal Law of 25.07.2011 N 261-FZ)

1. The operator is obliged to inform the personal data subject or his/her representative about the availability of personal data pertaining to the respective personal data subject in accordance with the procedure stipulated by Article 14 of this Federal Law, as well as to provide an opportunity to get acquainted with this personal data at the request of the personal data subject or his/her representative or within ten working days from the date of receipt of the request of the personal data subject or his/her representative. The said term may be extended, but not more than for five working days in case the operator sends to the address of the personal data subject a motivated notice indicating the reasons for extending the term for providing the requested information.
(ed. Federal Law of 14.07.2022 N 266-FZ)

2. In case of refusal to provide information on the availability of personal data on the relevant personal data subject or personal data to the personal data subject or his/her representative upon their application or upon receipt of the request of the personal data subject or his/her representative, the operator shall be obliged to provide in writing a reasoned response containing a reference to the provision of paragraph 8 of Article 14 of this Federal Law or other federal law, which is the basis for such refusal, within a period not exceeding ten working days from the date of submission of the requested information to the personal data subject or his/her representative. The said term may be extended, but not more than for five working days in case the operator sends to the address of the personal data subject a motivated notification indicating the reasons for extending the term for providing the requested information.
(ed. Federal Law of 14.07.2022 N 266-FZ)

3. the Operator is obliged to provide free of charge to the personal data subject or his/her representative an opportunity to familiarise with personal data related to this personal data subject. Within a period not exceeding seven working days from the date of submission by the subject of personal data or his/her representative of information confirming that the personal data are incomplete, inaccurate or irrelevant, the operator is obliged to make the necessary changes to them. Within a period not exceeding seven working days from the date of submission by the personal data subject or his/her representative of information confirming that such personal data are illegally obtained or are not necessary for the stated purpose of processing, the operator shall destroy such personal data. The operator shall notify the personal data subject or his/her representative of the changes made and measures taken, and shall take reasonable measures to notify third parties to whom the personal data of this subject have been transferred.

4 The operator is obliged to inform the authorised body for the protection of the rights of personal data subjects, upon the request of this authority, the necessary information within ten working days from the date of receipt of such request. The said term may be extended, but not more than for five working days in case the operator sends a motivated notification to the authorised body for the protection of the rights of personal data subjects, indicating the reasons for extending the term for providing the requested information.
(ed. Federal Law of 14.07.2022 N 266-FZ)

Article 21. Obligations of the operator to eliminate violations of legislation committed during the processing of personal data, to clarify, block and destroy personal data
(ed. Federal Law of 25.07.2011 N 261-FZ)

1. In case of detection of unlawful processing of personal data upon application of the personal data subject or his/her representative or upon request of the personal data subject or his/her representative or the authorised body for protection of the rights of personal data subjects, the operator is obliged to block the unlawfully processed personal data related to this personal data subject or ensure their blocking (if personal data processing is carried out by another person acting on behalf of the operator) with the possibility to block the personal data (if the personal data processing is carried out by another person acting on behalf of the operator). In case of detection of inaccurate personal data upon application of the personal data subject or his/her representative or upon their request or upon request of the authorised body for the protection of the rights of personal data subjects, the operator is obliged to block personal data relating to this personal data subject or ensure their blocking (if personal data processing is carried out by another person acting on behalf of the operator) from the moment of such application or receipt of the said request for the period of verification, if the blocking is carried out by another person acting on behalf of the operator.

2. In case of confirmation of the fact of inaccuracy of personal data, the operator, based on the information submitted by the personal data subject or his representative or the authorised body for the protection of the rights of personal data subjects, or other necessary documents, is obliged to clarify personal data or ensure their clarification (if personal data processing is carried out by another person acting on behalf of the operator) within seven working days from the date of submission of such information and remove the blocking of personal data.

3. In case of detection of unlawful processing of personal data by the operator or a person acting on behalf of the operator, the operator shall, within a period not exceeding three working days from the date of such detection, be obliged to cease unlawful processing of personal data or ensure the cessation of unlawful processing of personal data by a person acting on behalf of the operator. If it is impossible to ensure the lawfulness of personal

data processing, the operator shall, within a period not exceeding ten working days from the date of detection of unlawful processing of personal data, destroy such personal data or ensure their destruction. The operator is obliged to notify the personal data subject or his/her representative about the elimination of the committed violations or about the destruction of personal data, and if the personal data subject's or his/her representative's appeal or the request of the authorised authority for the protection of the rights of personal data subjects was sent by the authorised authority for the protection of the rights of personal data subjects, also the said authority.

3.1 In case of establishing the fact of unlawful or accidental transfer (provision, dissemination, access) of personal data resulting in violation of the rights of personal data subjects, the operator is obliged to notify the authorised body for the protection of the rights of personal data subjects from the moment of detection of such incident by the operator, the authorised body for the protection of the rights of personal data subjects or other interested person:

1) within twenty-four hours about the incident that occurred, about the alleged causes that led to the violation of the rights of personal data subjects and the alleged damage caused to the rights of personal data subjects, about the measures taken to eliminate the consequences of the respective incident, as well as to provide information about the person authorised by the operator to interact with the authority authorised to protect the rights of personal data subjects on issues related to the identified incident;

2) within seventy-two hours on the results of the internal investigation of the identified incident, as well as provide information on the persons whose actions caused the identified incident (if any).
(part 3.1 introduced by the Federal Law of 14.07.2022 N 266-FZ)

4. If the purpose of personal data processing is achieved, the operator is obliged to stop processing personal data or ensure its termination (if personal data processing is carried out by another person acting on behalf of the operator) and destroy personal data or ensure its destruction (if personal data processing is carried out by another person acting on behalf of the operator) within a period not exceeding thirty days from the date when the purpose of personal data processing is achieved, unless otherwise provided for by the contract to which the operator is a party.

5. If the personal data subject withdraws his/her consent to the processing of his/her personal data, the operator is obliged to stop processing the personal data or ensure the termination of such processing (if the processing of personal data is carried out by another person acting on behalf of the operator) and, if the preservation of personal data is no longer required for the purposes of personal data processing, destroy the personal data or ensure their destruction (if the processing of personal data is carried out by another person acting on behalf of the operator) with the consent of the personal data subject.

5.1 In case the personal data subject appeals to the operator with a request to stop processing of personal data, the operator is obliged within a period not exceeding ten working days from the date of receipt of the relevant request by the operator to stop their processing or to ensure the cessation of such processing (if such processing is carried out by a person who processes personal data), except in cases provided for by paragraphs 2 - 11 of Part 1 of Article 6, Part 2 of Article 10 and Part 2 of Article 11 of this Federal Law. The said term may be extended, but not more than for five working days in case the operator sends to the address of the personal data subject a motivated notification indicating the reasons for extending the term for providing the requested information.
(part 5.1 introduced by the Federal Law of 14.07.2022 N 266-FZ)

6. If it is not possible to destroy personal data within the period specified in paragraphs 3 - 5.1 of this Article, the operator shall block such personal data or ensure their blocking (if personal data processing is carried out by another person acting on behalf of the operator) and ensure the destruction of personal data within a period not exceeding six months, unless another period is established by federal laws.
(ed. Federal Law of 14.07.2022 N 266-FZ)

7. Confirmation of personal data destruction in cases provided for by this Article shall be carried out in accordance with the requirements established by the authorised body for the protection of the rights of personal data subjects.
(part 7 introduced by the Federal Law of 14.07.2022 N 266-FZ)

Article 22. Notification of personal data processing

1. Prior to the commencement of personal data processing, the operator shall be obliged to notify the authorised body for the protection of the rights of personal data subjects of its intention to process personal data, except for the cases provided for in paragraph 2 of this Article.

2. the Operator has the right to carry out personal data processing without notifying the authorised body for the protection of the rights of personal data subjects:

1) - 6) ceased to be in force from 1 September 2022. - Federal Law of 14.07.2022 N 266-FZ;

7) included in the state information systems of personal data created for the purpose of protection of state security and public order;
(p. 7 in the edition of the Federal Law of 14.07.2022 N 266-FZ)

8) in case the operator carries out the activity of personal data processing exclusively without the use of means of automation;
(p. 8 in the edition of the Federal Law of 14.07.2022 N 266-FZ)

9) processed in cases stipulated by the legislation of the Russian Federation on transport security in order to ensure sustainable and safe functioning of the transport complex, protection of the interests of individuals, society and the state in the sphere of the transport complex from acts of unlawful interference.
(paragraph 9 introduced by the Federal Law of 25.07.2011 N 261-FZ)

3. The notification provided for in paragraph 1 of this Article shall be sent in the form of a document on paper or in the form of an electronic document and shall be signed by an authorised person. The notification shall contain the following information:
(ed. Federal Law of 25.07.2011 N 261-FZ)

1) name (surname, first name, patronymic), address of the operator;

2) the purpose of personal data processing;

3) - 6) ceased to be in force from 1 September 2022. - Federal Law of 14.07.2022 N 266-FZ;

7) description of measures provided for by Articles 18.1 and 19 of this Federal Law, including information on the availability of encryption (cryptographic) means and the names of these means;
(paragraph 7 in the edition of the Federal Law of 25.07.2011 N 261-FZ)

7.1) the surname, first name, patronymic of the natural person or the name of the legal entity responsible for organising the processing of personal data and their contact telephone numbers, postal and e-mail addresses;
(paragraph 7.1 introduced by the Federal Law of 25.07.2011 N 261-FZ)

8) the date of commencement of personal data processing;

9) term or condition for termination of personal data processing;

10) information on the presence or absence of transborder transfer of personal data in the process of their processing;
(paragraph 10 introduced by the Federal Law of 25.07.2011 N 261-FZ)

10.1) information on the location of the database of information containing personal data of citizens of the Russian Federation;
(p. 10.1 introduced by Federal Law of 21.07.2014 N 242-FZ)

10.2) surname, first name, patronymic of a natural person or the name of a legal entity having access to and (or) carrying out on the basis of a contract the processing of personal data contained in state and municipal

information systems;
(item 10.2 introduced by the Federal Law of 14.07.2022 N 266-FZ)

11) information on ensuring the security of personal data in accordance with the requirements for the protection of personal data established by the Government of the Russian Federation.
(paragraph 11 introduced by the Federal Law of 25.07.2011 N 261-FZ)

3.1 When providing the information provided for in paragraph 3 of this Article, for each purpose of personal data processing, the operator shall indicate the categories of personal data, categories of subjects whose personal data are processed, the legal basis of personal data processing, the list of actions with personal data, methods of personal data processing.
(part 3.1 introduced by the Federal Law of 14.07.2022 N 266-FZ)

4. The authorised body for the protection of the rights of personal data subjects shall, within thirty days from the date of receipt of the notification on the processing of personal data, enter the information specified in paragraph 3 of this Article, as well as information on the date of sending the said notification to the register of operators. The information contained in the register of operators, except for the information on the means to ensure the security of personal data during their processing, shall be publicly available.

4.1 The authorised body for the protection of the rights of personal data subjects shall, within thirty days from the date of receipt from the operator of the notification on cessation of personal data processing, exclude the information specified in paragraph 3 of this Article from the register of operators.
(part 4.1 introduced by the Federal Law of 14.07.2022 N 266-FZ)

5. The operator may not be charged with expenses in connection with the examination of the notification on personal data processing by the authorised body for the protection of the rights of personal data subjects, as well as in connection with the entry of information in the register of operators.

6. In case of providing incomplete or unreliable information referred to in paragraph 3 of this Article, the authorised body for the protection of the rights of personal data subjects shall have the right to demand from the operator to clarify the provided information before its entry in the register of operators.

7. In case of changes in the information specified in paragraph 3 of this Article, the operator shall not later than the 15th day of the month following the month in which such changes occurred, shall notify the authorised body for the protection of the rights of personal data subjects of all changes that occurred during the specified period. In case of termination of personal data processing, the operator is obliged to notify the authorised body for the protection of the rights of personal data subjects within ten working days from the date of termination of personal data processing.
(part 7 in the edition of the Federal Law of 14.07.2022 N 266-FZ)

8. The forms of notifications provided for in paragraphs 1, 4.1 and 7 of this Article shall be established by the authorised body for the protection of the rights of personal data subjects.
(part 8 introduced by the Federal Law of 14.07.2022 N 266-FZ)

Article 22.1. Persons responsible for the organisation of personal data processing in organisations

(introduced by Federal Law of 25.07.2011 N 261-FZ)

1 The Operator, which is a legal entity, shall appoint a person responsible for organising the processing of personal data.

2 The person responsible for organising the processing of personal data shall receive instructions directly from and report to the executive body of the organisation that is the operator.

3. the Operator shall be obliged to provide the person responsible for organising the processing of personal data with the information specified in Article 22(3) of this Federal Law.

4. The person responsible for organising the processing of personal data shall, in particular, be obliged to:

1) to exercise internal control over the compliance of the operator and its employees with the Russian Federation legislation on personal data, including requirements to the protection of personal data;

2) bring to the attention of the operator's employees the provisions of the Russian Federation legislation on personal data, local acts on personal data processing, and personal data protection requirements;

3) organise the reception and processing of appeals and requests of personal data subjects or their representatives and (or) exercise control over the reception and processing of such appeals and requests.

Chapter 5. FEDERAL STATE CONTROL (SUPERVISION) OVER THE PROCESSING OF PERSONAL DATA. LIABILITY FOR VIOLATION OF THE REQUIREMENTS OF THIS FEDERAL LAW

(ed. Federal Law of 11.06.2021 N 170-FZ)

Article 23. Authorised body for the protection of the rights of personal data subjects

1. The authorised body for the protection of the rights of personal data subjects shall be a federal executive authority exercising independently the functions of control and supervision over the compliance of personal data processing with the requirements of the legislation of the Russian Federation in the field of personal data.
(part 1 in the edition of the Federal Law of 14.07.2022 N 266-FZ)

1.1 Retired as of 1 July 2021. - Federal Law of 11.06.2021 N 170-FZ.

2. The authorised body for the protection of the rights of personal data subjects shall consider the personal data subject's appeals on the compliance of the content of personal data and the methods of their processing with the purposes of their processing and shall take the relevant decision.

3. The authorised body for the protection of the rights of personal data subjects shall have the right:

1) to request from individuals or legal entities information necessary for the exercise of its powers and to receive such information free of charge;

2) to carry out verification of the information contained in the notification on personal data processing or to involve other state authorities for such verification within the limits of their authority;

3) to demand from the operator to clarify, block or destroy unreliable or illegally obtained personal data;

3.1) restrict access to information processed in violation of the personal data legislation of the Russian Federation in accordance with the procedure established by the legislation of the Russian Federation;
(item 3.1 introduced by the Federal Law of 21.07.2014 N 242-FZ)

4) to take measures in accordance with the procedure established by the legislation of the Russian Federation to suspend or terminate the processing of personal data carried out in violation of the requirements of this Federal Law;

5) to file lawsuits in court in defence of the rights of personal data subjects, including in defence of the rights of an indefinite number of persons, and to represent the interests of personal data subjects in court;
(ed. Federal Law of 25.07.2011 N 261-FZ)

5.1) send to the federal executive authority authorised in the field of security and the federal executive authority authorised in the field of countering technical intelligence and technical protection of information, as applicable to the scope of their activities, the information specified in paragraph 7 of part 3 of Article 22 of this Federal Law;
(paragraph 5.1 introduced by the Federal Law of 25.07.2011 N 261-FZ)

6) to submit an application to the authority licensing the operator's activity in order to consider the issue of taking measures to suspend or cancel the relevant licence in accordance with the procedure established by the legislation of the Russian Federation, if the condition of the licence to carry out such activity is the prohibition to

transfer personal data to third parties without the consent in writing of the personal data subject;

7) to send to the prosecution authorities, other law enforcement bodies materials for solving the issue of initiating criminal cases on the grounds of offences related to the violation of the rights of personal data subjects, in accordance with the jurisdiction;

8) submit proposals to the Government of the Russian Federation on improvement of the normative legal regulation of the protection of the rights of personal data subjects and personal data processing activities;
(p. 8 in the edition of the Federal Law of 14.07.2022 N 266-FZ)

9) to bring to administrative responsibility persons guilty of violation of this Federal Law.

4. The confidentiality of personal data shall be ensured with regard to the personal data, which became known to the authority authorised to protect the rights of personal data subjects in the course of its activity.

5. The authorised body for the protection of the rights of personal data subjects shall:

1) organise, in accordance with the requirements of this Federal Law and other federal laws, the protection of the rights of personal data subjects;

2) to examine complaints and appeals of citizens or legal entities on issues related to the processing of personal data, as well as to adopt, within its competence, decisions on the results of examination of the said complaints and appeals;

3) maintain a register of operators;

4) to implement measures aimed at improving the protection of the rights of personal data subjects;

5) to take measures to suspend or terminate the processing of personal data in accordance with the procedure established by the legislation of the Russian Federation upon the proposal of the federal executive authority authorised in the field of security, the federal executive authority in the field of state protection or the federal executive authority authorised in the field of countering technical intelligence and technical protection of information;
(ed. Federal Law of 01.07.2017 N 148-FZ)

6) to inform the state authorities, as well as personal data subjects on their appeals or requests on the state of affairs in the field of personal data subjects' rights protection;

7) fulfil other duties stipulated by the legislation of the Russian Federation.

5.1 The authority empowered to protect the rights of personal data subjects shall cooperate with the authorities empowered to protect the rights of personal data subjects in foreign states, in particular the international exchange of information on the protection of the rights of personal data subjects, approve the list of foreign states ensuring adequate protection of the rights of personal data subjects.
(part 5.1 introduced by Federal Law of 25.07.2011 N 261-FZ)

5.2 The rights and obligations of the authority authorised to protect the rights of personal data subjects, established in paragraphs 3 and 4 of this Article, shall be exercised by it directly and cannot be transferred to other public authorities.
(part 5.2 introduced by the Federal Law of 14.07.2022 N 266-FZ)

6. Decisions of the authorised body for the protection of the rights of personal data subjects may be appealed against in court.

7. The authorised body for the protection of the rights of personal data subjects shall annually send a report on its activities to the President of the Russian Federation, the Government of the Russian Federation and the Federal Assembly of the Russian Federation. The said report shall be published in mass media.

8. The financing of the authorised body for the protection of the rights of personal data subjects shall be carried out at the expense of the federal budget.

9. An advisory council shall be established within the authority empowered to protect the rights of personal data subjects, on a voluntary basis, whose formation and activity procedure shall be determined by the authority empowered to protect the rights of personal data subjects.

10. In order to record information on incidents provided for in paragraph 3.1 of Article 21 of this Federal Law, the authorised body for the protection of the rights of personal data subjects shall keep a register of personal data incidents, shall determine the procedure and conditions of interaction with operators within the maintenance of the said register.
(part 10 introduced by the Federal Law of 14.07.2022 N 266-FZ)

11. Information on computer incidents resulting in unlawful or accidental transfer (provision, dissemination, access) of personal data shall be transmitted to the federal executive authority authorised in the field of security and the authorised body for the protection of the rights of personal data subjects in accordance with the procedure established jointly by the federal executive authority authorised in the field of security and the authorised body for the protection of the rights of personal data subjects.
(part 11 introduced by the Federal Law of 14.07.2022 N 266-FZ)

Article 23.1. Federal state control (supervision) over personal data processing

(introduced by the Federal Law of 11.06.2021 N 170-FZ)

1. Federal state control (supervision) over the processing of personal data shall be exercised by the federal executive authority exercising the functions of control (supervision) over the compliance of personal data processing with the requirements of the legislation of the Russian Federation in the field of personal data.

2. The subject of federal state control (supervision) over the processing of personal data is compliance by operators with mandatory requirements in the field of personal data established by this Federal Law and other regulatory legal acts of the Russian Federation adopted in accordance with it.

3. Federal state control (supervision) over the processing of personal data is carried out in accordance with the Federal Law of 31 July 2020 N 248-FZ "On State Control (Supervision) and Municipal Control in the Russian Federation" (except for control (supervisory) activities carried out without interaction with the controlled person).

4. Information about infliction of harm (damage) or threat of infliction of harm (damage) to legally protected values, revealed in the course of conducting activities without interaction with the controlled person, shall be the basis for making a decision to conduct a control (supervisory) activity in accordance with Article 60 of the Federal Law dated 31 July 2020 N 248-FZ "On State Control (Supervision) and Municipal Control in the Russian Federation".

5. Regulations on federal state control (supervision) over the processing of personal data, including the procedure for organisation and implementation of control (supervisory) activities conducted without interaction with the controlled person, shall be approved by the Government of the Russian Federation.

Article 24. Liability for violation of the requirements of this Federal Law

(1) Persons guilty of violating the requirements of this Federal Law shall bear the liability provided for by the legislation of the Russian Federation.
(ed. Federal Law of 25.07.2011 N 261-FZ)

2. Moral damage caused to the subject of personal data due to violation of his/her rights, violation of the rules of personal data processing established by this Federal Law, as well as requirements to personal data protection established in accordance with this Federal Law, shall be compensated in accordance with the legislation of the Russian Federation. Compensation for moral damage shall be made regardless of compensation for property damage and losses incurred by the subject of personal data.
(part 2 introduced by Federal Law of 25.07.2011 N 261-FZ)

Chapter 6. FINAL PROVISIONS

Article 25. Final provisions

1. This Federal Law shall come into force one hundred and eighty days after the day of its official publication.

2. After the date of entry into force of this Federal Law, the processing of personal data included in personal data information systems before the date of its entry into force shall be carried out in accordance with this Federal Law.

2.1 Operators who processed personal data before 1 July 2011 are obliged to submit to the authorized body for the protection of the rights of personal data subjects the information specified in paragraphs 5, 7.1, 10 and 11 of Part 3 of Article 22 of this Federal Law not later than 1 January 2013.
(part 2.1 introduced by the Federal Law of 25.07.2011 N 261-FZ)

3. Repealed. - Federal Law of 25.07.2011 N 261-FZ.

4. Operators who carry out processing of personal data before the date of entry into force of this Federal Law and continue to carry out such processing after the date of its entry into force, shall be obliged to send to the authorised body for the protection of the rights of personal data subjects, except in cases provided for by paragraph 2 of Article 22 of this Federal Law, the notification provided for by paragraph 3 of Article 22 of this Federal Law, not later than 1 January 2008.

5. Relations related to the processing of personal data carried out by state bodies, legal entities, individuals in the provision of state and municipal services, execution of state and municipal functions in the constituent entity of the Russian Federation - the city of federal significance Moscow, shall be regulated by this Federal Law, unless otherwise provided for by the Federal Law "On peculiarities of regulation of certain legal relations in connection with the annexation to the constituent entity of the Russian Federation - the city of federal significance Moscow".
(part 5 introduced by the Federal Law of 05.04.2013 N 43-FZ)

President
Russian Federation
VLADIMIR PUTIN

Moscow, Kremlin

27 July 2006.

N 152-FZ

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)