COUNTRY COMPARATIVE GUIDES 2021

The Legal 500 Country Comparative Guides

Russia

DATA PROTECTION & CYBER SECURITY

Contributing firm

Gorodissky & Partners

Stanislav Rumyantsev, Ph.D., CIPP/E

Senior Lawyer | rumyantsevs@gorodissky.com

This country-specific Q&A provides an overview of data protection & cyber security laws and regulations applicable in Russia.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

RUSSIA
DATA PROTECTION & CYBER SECURITY

1. Please provide an overview of the legal and regulatory framework governing privacy in your jurisdiction (e.g., a summary of the key laws, who is covered by them, what sectors, activities or data do they regulate, and who enforces the relevant laws)?

International Treaties

The Russian privacy laws are based on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data established by the Counsel of Europe in 1981 (ETS No.108). This is an international instrument establishing global standards for protecting individuals' privacy and balancing their privacy rights with the concept of free flows of personal data across national borders. In 2018, Russia was among the first signatories to the Protocol Amending the Convention (CETS No.223). The Protocol will enter into force either when it is ratified by all parties to the Convention, or on 11 October 2023 if there are 38 parties to the Protocol at this date. By that time, Russia will have to harmonize its legislation and, among other things, update cross-border transfer rules, data breach notification requirements, data subject rights, etc.

Federal Law "On Personal Data"

The framework act on data protection and privacy is the Federal Law "On Personal Data" dated 27 July 2006 No. 152-ФЗ, as amended (the **"PDL"**). The PDL establishes privacy principles, data subject rights, general data processing and protection requirements, data breach procedures, functions and powers of the data protection authority, and so on. The PDL applies in cases where data operators conduct

- automated data processing including, but not limited to, in the internet; and/or
- non-automated data processing provided that the manner of processing is similar to automated actions (it is possible to search for personal data in a systematized data source and/or access such data according to a pre-defined algorithm).

The term "operator" is a Russian equivalent to an international term "controller". Under art.3(2) of the PDL, the "operator" means the state body, municipal body, legal entity, or natural person which alone or jointly with others organizes and/or conducts the processing of personal data as well as determines the purposes of the personal data processing, scope of personal data to be processed, and actions (operations) conducted with personal data. The data processing includes any action (operation) or set of actions (operations) which is performed on personal data, whether or not by automated means, such as collection, record, systematization, accumulation, storage, clarification (update and change), extraction, use, transfer (distribution, provision, and access), depersonalization, blockage, deletion, and destruction.

Sectoral Laws

Sectoral requirements apply to particular areas of business, types of data subjects, and professional activities. They are established by numerous laws including, among others, the following:

- Labor Code contains detailed requirements on the processing and protection of employee data;
- Federal Law "On information, Information Technologies, and Protection of Information" dated 27 July 2006 No. 149-ФЗ, as amended, prescribes to retain information about web-site users' identity, their conversations, posts, and other online activities;
- Federal Law "On Transport Security" dated 09 February 2007 No. 16-ФЗ, as amended, governs the processing of personal data of passengers, crew members, and transport security officers;
- Federal Law "On Credit Histories" dated 30 December 2004 No.218-ФЗ, as amended,

stipulates how to compose, store, and use credit histories and who may access them;
- Law of the Russian Federation "On Mass Media" dated 27 December 1991 No.2124-1, as amended, restricts certain activities of journalists, such as publishing personal details of underage victims of crimes.

Other Enactments

In some cases, the Russian laws prescribe that the governmental bodies must adopt detailed regulations on personal data matters. Below are several examples:

- Decree of the Government "On Adopting the Regulations on Specifics of Personal Data Processing Conducted Without Automatization Tools" dated 15 September 2008 No.687;
- Decree of the Government "On Adopting Requirements to Protection of Personal Data Processed with Information Systems of Personal Data" dated 01 November 2012 No.1119;
- Decree of the Federal Service for Technical and Export Control of Russia "On Adoption of List and Description of Organizational and Technical Measures for Ensuring Security of Personal Data Processed in Information Systems of Personal Data" dated 18 February 2013 No. 21; and
- Decree of the Federal Security Service of Russia "On Adoption of List and Description of Organizational and Technical Measures for Ensuring Security of Personal Data Processed in Information Systems of Personal Data with the Use of Cryptographic Tools Necessary for Fulfilling Requirements for Personal Data Protection Established for Each Security Level by the Government of the Russian Federation" dated 10 July 2014 No. 378.

Enforcement

Russian courts and several state supervisory bodies enforce the said laws and regulations. The main supervisory body is the Federal Service for Supervision of Communications, Information Technology and Mass Media (***"Roscomnadzor"***) acting as the federal data protection authority of Russia. Roscomnadzor consists of the federal office and more than 70 regional departments located across the country. The supervisory activities of Roscomnadzor are governed by the Decree of the Government "On Adopting the Regulations on Organizing and Performing State Control and Supervision over Personal Data Processing" dated 13 February 2019 No.146.

2. Are there any registration or licensing requirements for entities covered by these laws and, if so, what are the requirements? Are there any exemptions?

There are no registration or licensing requirements. However, the data operators must file a personal data processing notice with Roscomnadzor prior to commencing any processing actions (art.22 of the PDL). The notice should contain a summary of all processing purposes, lawful bases, data categories, data security measures, cross-border transfers, IT systems containing personal data, and other details relevant to a particular operator. The PDL provides for several rare exemptions from the notification requirement but they do not work for the most of active companies doing business in Russia.

3. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

Personal data means any information relating to a directly or indirectly identified or identifiable natural person ("data subject") (art.3(1) of the PDL).

A data category is sensitive if concerns convictions, race, ethnicity, political views, religious or philosophical beliefs, statement of health, or intimacy (art.10 of the PDL).

Biometrical data should mean information about physiological and biological specifics of a human that may be used for establishing their identity, according to a literal interpretation of art.11(1) of the PDL. In its non-binding Explanation published in 2013, Roscomnadzor recommended that operators should consider the said information as biometrical data exclusively in cases where they actually use it for establishing the identity of a data subject.

4. What are the principles related to, the general processing of personal data or PII?

Article 5 of the PDL establishes the following data processing principles:

- Personal data must be processed lawfully and fairly;
- Data processing must be limited to achieving specific, predetermined, and lawful purposes. The data processing incompatible with the

purposes of data collection must be prohibited;
- Integration of databases containing the personal data, which is processed for the purposes incompatible with each other, must be prohibited;
- Only personal data that corresponds to the processing purposes must be subject to processing;
- The content and scope of the processed personal data must correspond to the declared processing purposes. The processed personal data must not be excessive with regard to the declared processing purposes;
- Accuracy and sufficiency of personal data, and, where necessary, its relevance to the data processing purposes must be ensured in the course of the processing. Operators must take the necessary measures, or ensure that they are taken, to delete or adjust incomplete or inaccurate data;
- Personal data must be stored in a form making it possible to identify the data subject no longer than it is required for the data processing purposes, unless a data storage period is set forth by a federal law or an agreement, to which the data subject is a party, beneficiary, or surety. The processed personal data must be destroyed or depersonalized after the processing purposes are achieved or if there is no further need for achieving such purposes, unless otherwise provided for by a federal law.

5. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII and, if so, are there are rules relating to the form, content and administration of such consent?

Consent is one of lawful bases for processing personal data. Data subjects may give consents voluntary, at their own free will, and to their own benefit. Consent must be concrete, informed, and deliberate.

As a rule, data subjects or their representatives may consent to data processing in any manner provided that the data operator must be able to confirm the receipt of such consent (art.9(1) of the PDL).

Russian law provides for several cases where the consent must be granted in writing, namely, the processing of sensitive or biometrical data, cross-border transfers into certain countries, disclosure of employee data to third parties, etc. Under art.9(4) of the PDL, the written consent must contain the following details:

- Surname, first name, patronymic, and address of the data subject and his/her ID document details (number, issuing date and issuing authority);
- Surname, first name, patronymic, and address of the representative of the data subject and his/her ID document details (number, issuing date and issuing authority); and details of the power of attorney or other document confirming the authority of the representative (if the consent is received from the representative of the data subject);
- Company name and address of the data operator;
- Data processing purpose;
- List of processed personal data;
- Company name and address of the data processor;
- List of data processing actions and a general description of the data processing methods;
- Consent term of validity and cancellation procedure;
- Data subject's signature.

Written consent must be executed as a hard-copy document signed with a handwritten signature or an electronic document signed with a digital signature. In practice, there are different views on what type of digital signature should be used because the language of law may be interpreted in several ways.

There are no legal requirements on the administration of consents. Given that data subjects may cancel their consents at any time, it seems reasonable to keep records of the consents.

6. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection?

The processing of conviction records is prohibited except for the cases prescribed by Russian law. For instance, employers may process data about convictions of their employees if the laws prohibit previously convicted persons from holding certain positions (such as school teachers, chief accountants, etc.).

Other categories of sensitive data may be processed on the basis of a written consent, for the performance of a legal obligation, for protecting life, health and other vital interests of data subjects (if it is impossible to obtain

their consent), and in other specific cases.

The Decree of the Government "On Adopting Requirements to Protection of Personal Data Processed with Information Systems of Personal Data" dated 01 November 2012 No.1119 lays down enhanced technical and organizational requirements for IT systems used for processing sensitive data.

7. How do the laws in your jurisdiction address children's personal data or PII?

The PDL does not establish detailed regulations on children's personal data.

According to art.9(6) of the PDL, if a person is incapable, the consent must be received from their legal representative. As follows from the recent case law and the Guidelines for Educational Organizations on the Processing of Personal Data, established by the Letter of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation dated 28 August 2020 № ЛБ-С-074-24059, only parents, guardians, or other legal representatives may consent to the processing of their children's data. The reason is that the minors (i.e. persons under 18) do not have full capability under art. 26 and 28 of the Civil Code except for very specific cases, such as emancipation. The data operator must check the legal representative's powers (art.9(1) of the PDL), but the law does not explain how to do it.

It is possible to process children's data to perform a contract to which a data subject (child) is a party or to conclude such contract at the initiative of a data subject. Under art.28 of the Civil Code, minors from 6 to 13 (inclusively), acting at their own, can enter into petty domestic transactions and transactions aimed at receiving gratuitous benefits as well as spend money provided by their legal representatives or third parties acting upon the legal representatives' permission. In all other cases, the legal representatives act on behalf of their children. Starting from 14 years of age, minors can spend their salaries and other earnings at their own in addition to the above-mentioned transactions (art. 26 of the Civil Code). Such minors can enter into all other transactions upon their legal representatives' permission.

Children's data may be processed for compliance with a legal obligation and in other cases.

8. Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.

The PDL does not apply in the following cases:

- private individuals process personal data solely for their personal and family needs provided that they do not infringe data subjects' rights;
- archival documents containing personal data are stored, collected, registered, or used according to the Russian laws on archiving; and
- processing of personal data classified as a state secret.

9. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

Russian law does not explicitly impose requirements of 'data protection by design' or 'data protection by default', but these concepts are implicit in the PDL.

According to art.19(2) and (4) of the PDL, data operators must implement technical and organizational measures to ensure security of personal data processed with IT systems. Data operator must test the effectiveness of these measures prior to putting an IT system into operation.

Under art.19(1) of the PDL, data operators must implement legal, technical, and organisational measures aimed at protecting personal data against accidental or unlawful access, destruction, alteration, blockage, copy, provision, distribution, or other unlawful actions. This requirement must be observed at all stages of the processing.

10. Are owners or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

Data controllers must adopt privacy policies, internal policies on prevention and detection of privacy violations and elimination of their consequences (art.18.1(1)(2) of

the PDL). Employers must adopt internal policies on the storage and use of employee data, employees' privacy rights and data protection obligations, and data access and transfer rules (art.86-88 of the Labor Code).

There is no explicit requirement to keep records of personal data. In practice, it would be impossible to comply with the PDL without keeping such records.

Under art.18.1(4) fo the PDL, data controllers must demonstrate compliance by presenting their internal documents or in any other manner at the request of Roscomnadzor. That is why a good practice for data operators is to adopt internal policies regulating each and every processing operation and data protection procedure, prepare template consent forms, model contract clauses, and other compliance documents.

11. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

Russian law does not contain such requirements or recommendations. Under art.23(5)(2) of the PDL, Roscomnadzor must react on personal data-related complaints and inquiries of private individuals and legal entities. In addition, data subjects and operators have the right to send inquiries to other state bodies at their choice.

As a rule, state bodies must respond within 30 days from the day of receipt of an inquiry via their official websites, by email or post. Their responses are non-binding, but Russian courts and supervisory authorities usually pay attention to them. Russian law firms often inquire in their own names if their clients wish to know the position of Roscomnadzor on certain matters without disclosing the clients' names.

12. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

The PDL contains the following rules on risk assessments:

- Data operators must evaluate the harm that may be potentially suffered by data subjects in case of breaching the PDL and measure this potential harm against the implemented measures aiming at fulfilling the requirements of the PDL (art.18.1(1)(5) of the PDL). Russian law does not provide for further guidance on how to do it. Hence, data operators perform the evaluations as they see fit.
- Data operators must determine security threats to personal data processed with IT systems (art.19(2)(1) of the PDL). This procedure includes the risk assessment according to the Methodology on Evaluating Information Security Threats (established by the Federal Service for Technical and Export Control of Russia on 05 February 2021).

13. Do the laws in your jurisdiction require appointment of a data protection officer (or other person to be in charge of privacy or data protection at the organization) and what are their legal responsibilities?

Under art.22.1 of the PDL, all data operators that are legal entities must appoint the data protection officer (the ***DPO***). Each data operator may appoint only one officer. The data protection officer is a natural person (employee or external service provider) or legal entity (service provider) that reports directly to the data operator's CEO and bears personal liability for breaching the PDL.

The PDL explicitly establishes the following responsibilities of the DPO:

1. Internal checking of how the data operator and its employees fulfil the Russian privacy laws including the data security requirements;
2. Informing the data operator's employees on the provisions of the Russian privacy laws, internal policies, and data security requirements; and
3. Organizing the receipt and processing of data subjects' inquiries and requests and/or controlling the receipt and processing of such inquiries and requests.

Data operators may impose additional privacy-related responsibilities on their DPOs.

There are no education / special knowledge, experience, conflict-of-interest, or other similar requirements to the role of DPO.

14. Do the laws in your jurisdiction require businesses to providing notice to individuals of their processing activities? If

so, please describe these notice requirements (e.g. posting an online privacy notice).

Data operators must adopt their privacy policies and prepare general descriptions of how they fulfill data protection requirements. Data operators must ensure that their policies and descriptions are available to data subjects 24/7. Where personal data is collected in the internet, data operators must publish their policies and descriptions online and ensure that all users may access them (art.18.1(2) of the PDL).

Upon a data subject's request, data operators must provide the following information (art.14(7) and 18(1) of the PDL):

- confirmation that personal data is actually processed;
- lawful bases and purposes of data processing;
- description of data processing methods;
- name and location of the data operator, information about the persons who have access to personal data or to whom personal data may be disclosed under an agreement with the data operator or under a federal law;
- personal data being processed and relating to the relevant data subject, its source, unless another procedure for such data presentation is provided for by a federal law;
- time periods of data processing, including time periods of its storage;
- procedure on how a data subject may exercise his/her rights established by the Russian laws;
- information on the completed or proposed cross-border data transfer;
- names and addresses of data processors (if any);
- other information as may be prescribed by the Russian laws.

If the data operator receives personal data from anyone other than the data subjects, the data operator must notify the data subjects of the processing purpose, lawful basis, data operator's name and address, and some other details. This rule does not apply if the data subjects have been already informed of the processing and in several other cases.

15. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data and, if so, what are they? (E.g. are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

Under art.6(3) of the PDL, operators may engage data processors upon data subjects' consent. By virtue of law, processors must comply with the principles and data processing rules prescribed by the PDL. Data operators are liable for all actions and omissions of their processors before data subjects. Processors are liable before their data operators.

16. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII or are there any other restrictions relating to the appointment of processors (e.g. due diligence or privacy and security assessments)?

Under art.6(3) and 21 of the PDL, data processing agreements must contain the following mandatory clauses:

- Comprehensive list of actions (operations) to be performed by a data processor
- Data processing purposes
- Non-disclosure (confidentiality) and data security obligations
- Data protection requirements
- Obligations on elimination of data breaches, clarification, blockage, and destruction of data.

Parties may agree additional clauses at their own discretion. Due diligence or privacy and security assessments are not required.

17. Please describe any restrictions on monitoring or profiling in your jurisdiction including the use of tracking technologies such as cookies. How are these terms defined and what restrictions are imposed, if any?

Russian law does not contain any explicit rules about the monitoring or profiling of data subjects. According to the recent case law, web-analytical data (including those collected through cookies) may be regarded as personal data. That is why it is advisable to use cookie banners for obtaining users' consent and ensure compliance of web-analytical services with the PDL.

18. Please describe any laws in your jurisdiction addressing email communication or direct marketing. How are these terms defined and what restrictions are imposed, if any?

Russian law prescribes that the data operator may contact data subjects for the purpose of direct marketing or political agitation by email or via other communications only upon their prior consent. According to a non-binding guidance of Roscomnadzor, an opt-in consent should be sufficient (art.15(1) of the PDL).

Under art.10 of the Federal Law "On information, Information Technologies, and Protection of Information" dated 27 July 2006 No. 149-ФЗ, messages must contain valid information about the person / entity conducting the mailing. This person / entity must ensure that the addressee may withdraw from the mailing at any time (e.g. add an opt-out link to each message).

In is prohibited to use autodial systems for direct marketing by phone. A human should choose whom to call (art.18 of the Federal Law "On Advertising" dated 13 March 2006 No. 38-ФЗ).

19. Please describe any laws in your jurisdiction addressing biometrics, such as facial recognition. How are these terms defined and what restrictions are imposed, if any?

Under art.11 of the PDL, biometric data may be processed on the basis of a written consent with several exceptions (e.g. the processing of biometrics for border control purposes).

There are sectoral requirements and regulations according to which Russian banks and state authorities compose the unified biometric system for identifying bank clients.

The Decree of the Government "On Adopting Requirements to Protection of Personal Data Processed with Information Systems of Personal Data" dated 01 November 2012 No.1119 prescribes enhanced technical and organizational requirements for IT systems used for processing biometrical data. The Government also established requirements to data media containing biometrical data and their use and storage by data operators.

20. Is the transfer of personal data or PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does cross-border transfer of personal data or PII require notification to or authorization form a regulator?)

Article 12 of the PDL states that it is permitted to freely transfer personal data from Russia only into countries "ensuring an adequate level of protection of data subjects' rights". They are UK, France, Germany, Ireland, and all other parties to the Convention of the Council of Europe for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108). In addition, Roscomnadzor adopted adequacy decisions with regard to Singapore, South Korea, Japan, Australia, and some other countries.

Cross-border transfers into the rest of the world (including US, India, or China) are possible based on a derogation. The most practical derogations are a written consent or performance of a contract concluded with a data subject. There is no requirement to obtain an authorization from Roscomnadzor.

According to Art.18(5) of the PDL, data operators are obliged, under several exceptions, "to ensure recording, systemization, accumulation, storage, clarification (update, change) and extraction of personal data of Russian Federation nationals with the use of databases located in the territory of the Russian Federation when collecting this personal data in any manner, including via the Internet". In simple terms, it is illegal to collect personal data originated from Russian nationals, directly upload, and process it on a non-Russian server without involving a database installed on a Russia-based server. This requirement cannot be obviated even with a data subject's written consent.

21. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

Article 19 of the PDL provides for the following data security obligations:

- determine and identify all security risks relating to the personal data processing in IT systems;
- assume necessary technical and organisational measures in order to ensure security of the personal data processed in IT systems as necessary for complying with the

data security requirements according to the security levels established by the Government;
- use information security tools compliant with Russian standards;
- inspect efficiency of the implemented personal data security measures prior to putting IT systems into operation;
- keep records of all physical data media;
- identify unauthorised access to personal data and assume appropriate measures;
- restore personal data which was modified or destroyed as a result of unauthorised access;
- establish access rules with regard to personal data processed in IT systems and ensure registering and recording all actions performed with personal data in IT systems; and
- supervise over the implementation of data security measures and the observance of the security levels established by the Government.

22. Do the laws in your jurisdiction address security breaches and, if so, how does the law define "security breach"?

The PDL does not contain the term "security breach". However, art.19 of the PDL requires that data operators must implement necessary measures aiming at protecting personal data against accidental or unlawful access, destruction, alteration, blockage, copy, provision, distribution, or other unlawful actions.

23. Does your jurisdiction impose specific security requirements on certain sectors or industries (e.g. telecoms, infrastructure)?

Among others, there are specific security requirements for facilities belonging to critical information infrastructure of Russia. These facilities include IT systems, networks and automated control systems used in healthcare, financial, chemical, nuclear, telecom, military, energy, and several other industries.

24. Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?

Data operators must not report security breaches except for the case described below.

Under art.21 of the PDL, data operators must conduct an internal check upon an inquiry made by data subjects (their representatives) or Roscomnadzor. If data operators reveal unlawful data processing, they must suppress it, eliminate the violation (or destroy the relevant data), and report on the elimination of violations to data subjects or Roscomnadzor depending on who submitted the inquiry. If Roscomnadzor forwarded a data subject's inquiry to the data operator, then the data operator must report to both of them.

25. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cyber-crime, such as the payment of ransoms in ransomware attacks?

The Russian Criminal Code establishes liability for developing, using, and spreading viruses, hacking, and several other cyber-crimes.

There are no specific laws on cyber-crimes.

26. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

Russia does not have a separate cybersecurity regulator.

27. Do the laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of the rights, how they are exercised, what exceptions exist and any other relevant details.

Data subjects have the following rights:

- Right to receive information about the processing of personal data;
- Right to demand for clarifying, blocking, or destroying personal data in cases where such data is incomplete, outdated, incorrect, illegally received, or such data is unnecessary for the declared processing purpose;
- Right to submit complaints about actions

(omission) of the data operator to competent authorities and bring a legal action;
- Right to defend data subjects' rights and legitimate interests, including the compensation of damages and/or moral damage, in court or according to other procedures established by the applicable law;
- Other rights established by the applicable law.

Data subjects may exercise their rights by contacting data operators, complaining to Roscomnadzor and other supervisory authorities, and/or bringing a court action.

28. Are individual data privacy rights exercisable through the judicial system or enforced by a regulator or both?

Both. Under art.23 of the PDL, Roscomnadzor must react on data subjects' complaints. In certain cases, Roscomnadzor may give binding orders to data operators and inspect their activities. Roscomnadzor has the power to represent data subjects before court or go to court in the interests of public.

Data subjects may sue data operators as described in Q29.

29. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

A data subject may bring a lawsuit against the data operator if the data subject believes that their rights are infringed. A data subject has no right to litigate in the interests of public. Class actions are possible.

30. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data privacy laws? Is actual damage required or is injury of feelings sufficient?

Data subjects may claim for monetary damages (if they suffered an actual damage as a result of data operator's unlawful actions or omission) or moral harm compensation (if they suffered from an injury of feelings). The amount of damages / compensation must be determined by court on a case-by-case basis.

31. How are the laws governing privacy and data protection enforced?

Breaches of Russian law can be revealed during a regular or extraordinary inspection by Roscomnadzor. In addition, Roscomnadzor has the power to monitor activities of the data operators without any interaction with them.

Roscomnadzor has the power to initiate administrative offence cases against data operators and their managers and bring them to court for the final resolution (see Q32). Certain privacy-related cases may be initiated and resolved by other supervisory authorities.

In rare cases (e.g. unlawful access to electronic information (hacking)), illegal operations with personal data may entail criminal liability. According to the Criminal Code, only natural persons may be sentenced to criminal punishments.

On the ground of a court act, Roscomnadzor has the power to suppress access to a website in the whole territory of Russia if the website contains illegally processed personal data. According to the recent case law, Roscomnadzor extensively applies the suppression for websites if they are anyhow involved in illegal processing of data.

32. What is the range of fines and penalties for violation of these laws?

The Code for Administrative Offences provides for several types of offences directly or indirectly relating to the data privacy compliance. If they are discovered, separate administrative liability may be imposed on the data operator itself (acting as a legal entity) and/or its responsible managers (usually, the DPO and/or the CEO). The law-enforcement bodies have the authority to decide at their own discretion which person(s) – a responsible manager, the data operator, or both – is/are to be accused of an administrative offence depending on the circumstances of the case.

The highest fines are established for the breach of the personal data localization requirement (see Q20). First-time breach entails a fine up to RUB 6 000 000 (approx. USD 78 000) on a legal entity and/or up to RUB 200 000 (approx. USD 2 600) on the legal entity's responsible managers. Repeated breach leads to a fine up to RUB 18 000 000 (approx. USD 234 000) on a legal entity and/or up to RUB 800 000 (approx. USD 10 400) on the responsible managers (art.13.11(8) and (9) of the Code for Administrative Offences). Fines for other violations are lower (max. RUB 500 000 that is approx. USD 6 500). According to the recent case law, a fine may be imposed either per violation, or per each episode of a violation, e.g. multiplied on the number of affected data subjects.

33. Can personal data or PII owners/controller appeal to the courts against orders of the regulators?

Data operators may appeal to the courts against orders of the regulators. In most cases, this can be done within 3 months from the day when the data operator became aware of a possible infringement of its rights and legal interests by a regulator's order.

Contributors

Stanislav Rumyantsev, Ph.D., CIPP/E
Senior Lawyer
rumyantsevs@gorodissky.com