Data Protection in the Russian Federation: Overview

by Sergey Medvedev and Stanislav Rumyantsev, Gorodissky & Partners, with Practical Law Data Privacy & Cybersecurity

Please note this resource does not cover legal issues related to the 2022 Ukraine crisis. For resources on these topics, see Russia Sanctions and Related Considerations Toolkit. Data Privacy Advisor subscribers, click here

Country Q&A | Law stated as of 01-Aug-2023 | Russian Federation

A Q&A guide to data protection in the Russian Federation.

This Q&A guide gives a high-level overview of the data protection laws, regulations, and principles in the Russian Federation, including the main obligations and processing requirements for data controllers (operators), data processors, and other third parties. It also covers data subject rights, the supervisory authority's enforcement powers, and potential sanctions and remedies. It briefly covers rules applicable to cookies and spam.

To compare answers across multiple jurisdictions, visit the Data Protection Country Q&A Tool.

This resource does not consider legal developments arising out of and related to the 2022 Ukraine crisis. For resources concerning these topics, see Russia Sanctions and Related Considerations Toolkit.

Regulation

Legislation

1. What national laws regulate the collection, use, and disclosure of personal data?

Data Protection Law

The main law regulating personal data protection and privacy in the Russian Federation, and the primary focus of this Q&A, is Federal Law No. 152-FZ on Personal Data (July 27, 2006) (Personal Data Law).

Other Relevant Laws

Other laws that affect data protection and privacy include:

- The Council of Europe's Strasbourg Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981 (ETS No. 108) (Strasbourg DPC).
- The Constitution of the Russian Federation (Constitution) (Articles 23 and 24).
- Federal Law No. 149-FZ on Information, Informational Technologies, and the Protection of Information (July 27, 2006) (Information Law).
- Federal Law N 572-## on Performing Identification and/or Authentication of Individuals with the Use of Biometrical Personal Data, on Amending Certain Legislative Acts of the Russian Federation and Repealing Certain Provisions of the Legislative Acts of the Russian Federation (December 29, 2022).
- Data protection-specific provisions can also be found in various sectoral laws, for example:
- Federal Law No. 197-FZ on Labor Code of the Russian Federation (December 31, 2001) (Labor Code) (Chapter 14).
- Federal Law No. 60-FZ on Air Code of Russian Federation (March 19, 1997) (Air Code) (in Russian) (Article 85.1).
- Federal Law No. 323 on the Fundamentals of Protection of the Health of Citizens in the Russian Federation (November 9, 2011) (Health Protection Law) (in Russian).
- Federal Law No. 38-FZ on Advertising (March 13, 2006) (Advertising Law). For more on this law, see Country Q&A, Email Marketing Compliance: Russian Federation.
- Federal Law No. 395-1 on Banks and Banking Activities (December 2, 1990) (Banking Law). For more on this law, see Practice Note, Bank Secrecy Laws (Russian Federation).

There are also regulatory acts, recommendations and guidance on various data-related matters issued by the:

- Russian President.
- Russian Government.
- Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor).
- Federal Service for Technical and Export Control (FSTEC).
- Federal Security Service (FSS).

Detailed information about sectoral laws, recommendations and guidance, and other regulations and requirements is outside the scope of this Q&A.

Scope of Legislation

2. To whom do the laws apply?

Data protection laws apply to all data operators and processors (third parties acting on behalf of data operators). Specifically, the Personal Data Law protects "personal data", meaning any information that directly or indirectly concerns a natural person, known as a personal data subject or data subject (Article 3(1), Personal Data Law). For more on the definition of personal data, see Question 3.

The Personal Data Law does not contain the concept of data controller. Instead, it uses the similar concept of a "data operator".

A data operator can be a state or municipal body, a legal entity, or a natural person that both:

- Organizes and/or carries out (alone or jointly with others) the processing of personal data; and
- Determines the purposes of personal data processing, the content of personal data, and the actions (operations) related to personal data.

(Article 3(2), Personal Data Law.)

For more on data processing operations, see Question 4.

A data operator can engage a third party, subject to the data subject's consent, who will be acting under the data operator's instruction based on either a data processing agreement, or state or municipal regulatory act (Article 6(3), Personal Data Law). This Q&A will refer to these third parties as data processors. For more on consent, see Question 9. For more on processing agreements, see Question 17.

3. What personal data does the law regulate?

Under the Personal Data Law, personal data is any information that relates to a directly or indirectly identified or identifiable natural person (data subject) (Article 3(1), Personal Data Law).

For information on processing personal data, see Question 4.

The Personal Data Law also regulates the processing of:

- Special categories of personal data, defined as data that includes an individual's:
  - race;
  - ethnicity;
  - political opinions;
  - religious or philosophical beliefs;
  - statement of health;
  - information about sex life;

- and convictions.

(Article 10(1), (3), Personal Data Law.)

- Biometric personal data, which a data operator can process only with data subject consent or under other limited exceptions (Article 11, Personal Data Law).
- Personal data made publicly available, which means personal data to which the data subject has given an unlimited number of persons access by consenting to processing for further distribution (Article 3(1.1), Personal Data Law, as amended by Federal Law No. 519-FZ on Amendments to Personal Data Law (December 30, 2020) (Federal Law 519) (in Russian)). This type of data encompasses publicly available personal data that individuals provide over the internet, including on social media. Data operators are subject to different consent requirements for processing and transferring this type of data (see Question 9).

For information on processing special categories of personal data, see Question 11.

4. What acts are regulated?

The Personal Data Law applies to all acts relating to personal data processing, including:

- Collection
- Recording.
- Systematization.
- Accumulation.
- Storage.
- Alteration.
- Retrieval.
- Use.
- Transfer.
- Dissemination.
- Provision.
- Access.
- Depersonalization.
- Blocking.

- Deletion or destruction.

(Article 3(3), Personal Data Law).

The Personal Data Law applies to both automated and non-automated personal data records and mixed data processing activities (Articles 3(3) and (4), Personal Data Law).

5. What is the jurisdictional scope of the rules?

Under the recent amendments to Article 1, the Personal Data Law applies where foreign legal entities and/or natural persons process Russian nationals' personal data on the basis of either agreements concluded with data subjects or their consent.

This rule can be understood to mean that non-Russian data controllers will be obliged to comply with all provisions of the Personal Data Law, including the requirement to process data "with the use of databases located in the territory of the Russian Federation" ("data localisation requirement"). I

It is unclear how foreign controllers with no presence in Russia are expected to learn about the rules applicable to them and how Roscomnadzor might verify their compliance.

6. What are the main exemptions (if any)?

The Personal Data Law does not apply to the following actions:

- Personal data processing by individuals solely for personal and family needs, provided the processing does not infringe data subject rights (Article 1(2)(1), Personal Data Law).
- Organizing the storage, collection, recording, and use of archived documents containing personal data in accordance with the national laws on archive matters (Article (1)(2)(2), Personal Data Law).
- Personal data processing that involves data containing state secrets (Article (1)(2)(4), Personal Data Law).
- Submitting data related to the activities of courts in Russia by the competent authorities, in accordance with the relevant court legislation (Article (1)(2)(5), Personal Data Law).

Notification

7. Is notification or registration with a supervisory authority required before processing data?

Under the Personal Data Law, a data operator (*see Question 2*) must notify Roskomnadzor before it starts to process personal data (Article 22(1), Personal Data Law), subject to limited exceptions.

The data operator can submit the notification on paper or electronically using the Roskomnadzor's website and it must contain the following information:

- The company name of data operator.
- The purposes of personal data processing. For each purpose, the data operator must specify data categories, types of data subjects, lawful basis, and data processing actions and methods.
- A description of privacy compliance and security measures performed by the data operator.
- Information on the protection of IT systems according to the requirements established by the Russian Government.
- The contact information of the DPO.
- The start date of the personal data processing.
- The duration of processing or the conditions for terminating the personal data processing.
- Information on any cross-border data transfers.
- Information on the location of any database containing the personal data of Russian Federation citizens.

(Article 22(3) and (4), Personal Data Law)

Roskomnadzor registers the data operator within 30 days of receiving the notification, assuming the regulator does not have additional questions or inquiries.

Roskomnadzor maintains a register of data operators based on the information contained in the notifications it receives. Except for the security measures performed by data operators, the information in the notification becomes publicly available once included in the register. (Article 22(4), Personal Data Law.)

A data operator may be exempt from the statutory notification requirements and able to process personal data without notification in several rare cases. For example, where the personal data is:

- Included in IT systems that have acquired state computer IT system status under the applicable laws or in state IT systems created for the purposes of state security and public order.
- Processed without the use of automated systems.
- Processed under the laws and regulations relating to transport security.

(Article 22(2), Personal Data Law)

The data operator does not pay any official fee for the notification and registration.

For information on the supervisory authority's notification, registration, or authorization requirements, see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: Russian Federation: Questions 2 and 3.

Main Data Protection Rules and Principles

Main Obligations and Processing Requirements

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

The main obligations imposed on data operators under the Personal Data Law include:

- Complying with the principles for processing personal data, including:
  - collecting and processing personal data fairly and lawfully;
  - limiting personal data collection to only what is necessary for an organization's stated processing purposes;
  - processing personal data only for the purposes for which an organization collects it;
  - maintaining the accuracy of the personal data; and
  - storing personal data only for as long as necessary to fulfill the purposes for which an organization collects it.

  (Article 5, Personal Data Law.)
- When dealing with third-party processors:
  - engaging a processor only on the basis of data subject’s consent unless otherwise prescribed by law (Article 6(3), Personal Data Law);
  - requiring the processor to secure and protect the personal data (Articles 6(3) and 19, Personal Data Law; Regulation No. 1119 of November 1, 2012, of the Government of the Russian Federation On Approval of the Requirements to Personal Data Protection in the course of Its Processing in Personal Data Information Systems (in Russian)); and
  - executing a contract with specific required terms (Article 6(3), Personal Data Law).

For more on data processors, see Question 17.

- Responding to data subjects' requests for information within ten business days (Articles 14(3) and 20, Personal Data Law). For more on data subject rights, see Question 12 and Question 13.
- Informing data subjects of the consequences of failing to provide personal data in response to a mandatory request (Article 18(2), Personal Data Law). For more on data subject information rights, see Question 12.
- Informing data subjects that the data operator has received personal data from sources other than the data subject, unless an exception applies (Article 18(3), Personal Data Law). For more on this notification, see Question 12.
- Taking measures that are necessary and sufficient to ensure compliance with the personal data legislation. Among others, the compliance measures include:
    - appoint a data protection officer (DPO);
    - adopt a privacy policy, register of processing operations (RoPA), and other internal policies on various matters;
    - take legal, organizational, and technical data protection and security measures;
    - perform internal control measures and/or audit the compliance of the data operator with the Personal Data Law and other regulatory acts adopted in line with the Personal Data Law, applicable data security requirements, and the data operator’s privacy policy and internal policies;
    - conduct a data protection impact assessment according to the requirements established by Roskomnadzor;
    - acquaint data operator’s employees participating in the data processing with the personal data legislation including data security requirements, privacy policy, and internal policies, and/or conduct professional training.

  (Article 18.1(1), Personal Data Law.) Data operators must notify or communicate the DPO's information to the data protection authority, including their name, address, phone number, and email. For more on appointing a DPO, see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: Russian Federation: Questions 4 and 5.
- 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" (Article 18(5), Personal Data Law, as amended by Federal Law No. 242-FZ on Amending Certain Legislative Acts Concerning Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks (July 21, 2014)) (Federal Law 242). For more on localization requirements, see Question 21 and Country Q&A, Data Localization Laws: Russian Federation.
- Notifying Roskomnadzor of the data processing operations, unless an exception applies (Article 22(1), Personal Data Law). For more on notification, see Question 7 and Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: Russian Federation: Questions 2 and 3.
- Blocking access to wrongfully processed personal data after learning of a breach or receiving a notice from the data subject (Article 21(1), Personal Data Law).

9. Is the consent of data subjects required before processing personal data?

In most cases, the Personal Data Law requires the data operator to obtain the data subject's consent before processing their personal data. For circumstances when personal data processing is lawful without consent, see Question 10.

Under the Personal Data Law:

- Unless otherwise provided by law, the data subject's consent can be obtained in any form, including online or electronically. (Article 9(1), Personal Data Law.) Where the law requires the data subject's consent to be given in writing, for example, for biometric data processing, the implied or inferred consent is invalid.
- A data subject can revoke consent. When a data subject revokes consent, a data operator can continue to process the personal data only if the operator has another legal basis for processing the personal data. For the legal bases to process personal data without consent, see Question 10.
- The data operator bears the burden of proof that it obtained the data subject's consent (Article 9(3), Personal Data Law). E-signatures are allowed as evidence of consent if used in accordance with the provisions of the applicable law on digital signatures (Article 9(4), Personal Data Law).
- There is no prescribed or approved form of consent. However, the Personal Data Law specifies the information that must appear in the data subject's written consent:
    - the data subject's full name, address, ID number, such as a passport number, date of issue of the ID, and issuing authority;
    - the data subject's representative's full name, address, ID number, date of issue of the ID and the issuing authority, and details of the power of attorney or other applicable document, if the data subject's representative gave the consent;
    - the data operator's first name, middle name, surname, and address;
    - the purpose of the data processing;
    - a list of personal data the data subject consents to the data operator processing;
    - the first name, middle name, surname, and address of any third party (processor) that is processing the personal data on behalf of the data operator;
    - a list of actions that the data subject consents to the data operator taking in relation to personal data and a general description of the data operator's processing methods;
    - the duration of data subject's consent, and the method of its revocation; and
    - the data subject's signature.

    (Article 9(4)(1) to (9), Personal Data Law.)

The Personal Data Law does not regulate minors. However, a data operator can process the personal data of a data subject who lacks capacity, such as due to mental disorder, with the consent of the data subject's lawful representative (Article 9(6), Personal Data Law).

Separate consent rules govern personal data made publicly available. To process or transfer this data, a data operator must:

- Obtain separate consent and permit the data subject to select which personal data they consent to making publicly available for processing by additional data operators (Article 10.1(1), Personal Data Law, as amended by Federal Law 519. A data subject's silence or inaction never suffices as consent to make personal data publicly available (Article 10.1(8), Personal Data Law).
- Honor any prohibitions on transferring the personal data to an unlimited number of persons or other processing restrictions that the data subject imposes (Article 10.1(9), Personal Data Law).
- Publish information on the existence and nature of any data subject processing restrictions or transfer prohibitions within three days of receiving the data subject's consent (Article 10.1(10), Personal Data Law). This requirement takes effect July 1, 2021 (Article 2, Federal Law 519). Operators can publish this information on their websites, for example as part of a user agreement.
- Not distribute the personal data to other data operators if it is unclear from the data subject's consent:
    - that the data subject permits the data operator to make the personal data publicly available;
    - what processing conditions and restrictions the data subject has imposed; or
    - what personal data categories the data subject has consented to making publicly available for processing by additional data operators.

    Under these circumstances, the data operator that obtained the personal data can process the data itself but cannot distribute the personal data to others (Articles 10.1(4) and (5), Personal Data Law).

Any data operator that distributes or processes personal data made publicly available to an indefinite number of persons by the data subject without providing consent to a data operator is responsible for providing evidence of the processing and subsequent distributions' legality (Article 10.1(2), Personal Data Law).

Data operators can obtain a data subject's consent either directly or through Roskomnadzor's IT system, which will be subject to any rules imposed by the regulator (Articles 10.1(6) and (7), Personal Data Law).

Data subjects can also terminate the processing of their publicly available personal data at any time based on a data operator's failure to comply with these rules (Articles 10.1(12), (13), and (14), Personal Data Law). The termination request serves as a termination of the data subject's consent (Article 10.1(13), Personal Data Law).

These rules do not apply to certain processing by state entities (Articles 10.1(11) and (15), Personal Data Law).

10. If consent is not given, on what other grounds (if any) can processing be justified?

Under the Personal Data Law, a data operator can process personal data without the data subject's consent when data processing:

- Achieves objectives defined by an international treaty or under Russian Federation law.
- Furthers certain judicial purposes.
- Furthers court enforcement purposes.
- Performs certain powers by the federal authorities for state and municipal services.
- Concludes an agreement at the initiative of a data subject and/or executes an agreement either:
    - with the data subject; or
    - where the data subject is the beneficiary or guarantor.
- Protects the data subject's life, health, or other vital interests.
- Exercises the data operator's or third parties' rights and interests, or to further public purposes, provided there are no breaches of the data subject's rights and freedoms.
- Pursues professional journalistic, media, scientific, literary, or other creative activities, provided there are no breaches of the data subject's rights and freedoms.
- Furthers statistical or other scientific purposes, provided the relevant personal data has been depersonalized.
- Process depersonalized data for the purposes established by Russian law.
- Comply with applicable law that calls for mandatory publication or disclosure.

(Article 6(1)(2) to (11), Personal Data Law, as amended by Federal Law 519).

Special Rules

11. Do special rules apply for certain types of personal data, such as sensitive data?

Under the Personal Data Law, special categories of data refers to any information that relates to racial or ethnic origin, political opinions, religious or philosophical beliefs, convictions, or the state of a person's health or sex life (Article 10, Personal Data Law).

A data operator can process special categories of data only if:

- The data subject provided written consent to the data processing (for more on consent, see Question 9).
- The sensitive data is personal data made publicly available and the data operator complies with the rules governing processing and transferring that type of data (for more on these requirements, see Question 9).

- An international treaty on re-admission, for example, an immigrant's return to the country, requires the processing.
- It performs the processing in connection with the population census.
- It performs the processing under the relevant laws on social support, employment, pensions, insurance, or citizenship.
- It needs to process the personal data to protect the data subject's or another individual's life, health, or vital interests, and it is impossible to obtain consent.
- A professional who is engaged in various medical activities for certain medical purposes carries out the processing and is subject to medical confidentiality.
- Public societies or religious organizations process their members' personal data for the purposes defined by their articles of incorporation, provided they do not transfer the personal data to third parties without the data subject's written consent.
- It needs to process the personal data to establish or enforce the data subject's or a third party's rights, or to administer justice.
- The processing is consistent with Russian Federation legislation on state defense, security, anti-terrorism, transport safety, anti-corruption, law enforcement, execution, criminal investigation, or prosecution.
- Prosecutors' offices process the personal data in the context of special prosecution enforcement.
- State authorities, municipal agencies, or other organizations process the personal data for child adoption or foster care purposes.
- The processing complies with legislation on citizenship.

(Article 10(2)(1) to (10), Personal Data Law, as amended by Federal Law 519).

State and municipal bodies can process data about an individual's prior convictions consistent with the authority granted to them by applicable law (Article 10(3), Personal Data Law).

A data operator must immediately stop processing sensitive personal data when the reasons for the processing no longer exists (Article 10(4), Personal Data Law).

Data operators face more stringent requirements to process biometric data, which they can process only with the data subject's written consent unless:

- An international treaty on re-admission, for example, an immigrant's return to the country, requires it.
- The processing is consistent with Russian Federation legislation on state defense, security, anti-terrorism, transport safety, anti-corruption, law enforcement, execution, criminal investigation, prosecution, or citizenship.

(Article 11, Personal Data Law.)

For information on processing non-sensitive data, see Question 9 and Question 10.

Rights of Individuals

12. What information rights do data subjects have?

Under the Personal Data Law, a data operator must provide written notice to data subjects if the operator:

- Collects personal data from a data subject and the data subjects requests the following information:
    - 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 can 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, and its source, unless another procedure for such data presentation is provided for by a federal law;
    - time periods of data processing, including periods of its storage;
    - procedure on how a data subject can exercise their rights established by the Russian laws;
    - information on the completed or proposed cross-border data transfer;
    - names and addresses of data processors (if any);
    - information about performing compliance measures;
    - other information as may be prescribed by the Russian laws.

    (Article 14(7), Personal Data Law Decree.)
- Uses automated means of processing for decision-making (Article 16(3), Personal Data Law). When using automated processing for decision-making, the data operator must:
    - explain the decision-making procedure;
    - provide the data subject an opportunity to object to the decision;
    - explain how the data subject can protect their rights and legitimate interests relating to the processing; and
    - explain the legal consequences of the decision-making.

    (Article 16(3), Personal Data Law.)

- Received the data subject's personal data from a third party (Article 18(3), Personal Data Law). Unless an exception applies, when a data operator receives a data subject's personal data from a source other than the data subject, before processing the data, the operator must inform the data subject of:
    - the data operator's name or the name of the data operator's representative, and their addresses;
    - the personal data processing's purpose and legal basis;
    - list of personal data;
    - the proposed personal data users;
    - the data subject's rights (for more on these rights, see Question 13; and
    - the personal data's source.

    (Article 18(3)(1) to (5), Personal Data Law.)

    A data operator is not obliged to provide this information if:
    - the data operator has already informed the data subject that their personal data is being processed;
    - the data operator received the personal data under a federal law or in connection with performing a contract with or for the benefit of the data subject;
    - the data subject provided consent to another data operator to make the personal data publicly available and both the original data operator and the recipient data operator comply with the rules governing processing and transferring that type of data (for more on these requirements, see Question 9);
    - the data operator processes the personal data to pursue professional journalistic, media, scientific, literary, or other creative activities, provided there are no breaches of the data subject's rights and freedoms; or
    - providing the data subject with the information would otherwise infringe third parties' rights and lawful interests.

    (Article 18(4)(1) to (5), Personal Data Law, as amended by Federal Law 519).

The Personal Data Law also requires data operators to:

- Make privacy and data protection policies freely available for any interested person.
- Publish the privacy and data protection policies online if they collect personal data online, by phone, or using other telecommunication networks.

(Article 18.1(2), Personal Data Law.)

On July 31, 2017, an advisory body for Roskomnadzor issued non-binding guidance (in Russian) for data operators on drafting privacy and data protection policies that comply with the Personal Data Law.

13. Other than information rights, what other specific rights are granted to data subjects?

Under the Personal Data Law, the data subject has the right to access the data the data operator is processing and the right to receive information related to data processing on their request, including:

- 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 can 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 and 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 can exercise their rights established by the Russian laws.
- Information on the completed or proposed cross-border data transfer.
- Names and addresses of data processors (if any).
- Information about performing compliance measures.
- Other information as may be prescribed by the Russian laws.

(Article 14(7)(1) to (10), Personal Data Law.)

A data subject has the right to:

- Data access, correction, modification, and deletion (Article 14, Personal Data Law).
- Object to direct marketing (Article 15(2), Personal Data Law).
- Object to decisions being made solely on the basis of automated data processing (Article 16, Personal Data Law).
- Complain about the data operator's actions or omissions and claim compensation for losses, including moral damages (Article 17, Personal Data Law).
- Exercise other rights established by the Russian laws.

Data subjects can request the deletion of their personal data if the data is:

- Incomplete.
- Out of date.
- Inaccurate.

- Unlawfully obtained.

(Article 21, Personal Data Law.)

Data subjects also have the right to prohibit or restrict the data operator from transferring personal data made publicly available to an unlimited number of persons (Article 10.1(9), Personal Data Law, as amended by Federal Law 519) For more on the rules governing this type of data, see Question 9).

In addition to the Personal Data Law, Federal Law No. 264-FZ on Amending the Information Law (July 13, 2015) (in Russian) amended the Information Law to require search engine operators that use online advertisements targeting customers within the Russian Federation to remove search listing information on individuals when the information is:

- Shared in violation of Russian Federation law.
- False, outdated, or no longer relevant.

(Article 10.3, Information Law.)

14. Do data subjects have a right to request the deletion of their data?

See Question 13.

Security Requirements

15. What security requirements are imposed in relation to personal data?

Under the Personal Data Law, a data operator must take the necessary legal, organizational, and technical measures to protect personal data against any unauthorized, illegal, or accidental access, destruction, modification, blocking, copying, provision, or distribution, as well as against any other unauthorized actions.

A data operator must secure personal data by:

- Locating security threats in the relevant IT systems while processing personal data.
- Protecting IT systems used for the personal data processing according to the security requirements (security levels) established by the Russian Government.

- Assessing security measures' effectiveness before implementation.
- Recording any computer media that contains personal data.
- Applying certified data security tools.
- Detecting unauthorized access to personal data.
- Restoring personal data that has been modified or destroyed due to unauthorized access.
- Adopting rules governing:
    - access to personal data being processed in the relevant IT systems; and
    - registration and recording of all actions related to personal data in the relevant IT systems.
- Exercising control over security measures regarding personal data.

(Article 19(2)(1) to (9), Personal Data Law.)

Biometric data is also subject to specific additional security requirements set by Resolution No. 512 of July 6, 2008 of the Government of the Russian Federation on Approval of the Requirements for Material Carriers of Biometric Personal Data and Technologies for Storing Such Data Outside of Information Systems of Personal Data.

For more on security requirements in the Russian Federation, including under the Information Law) various sectoral laws, see Practice Note, Information Security Considerations (Russian Federation).

16. Is there a requirement to notify data subjects or the supervisory authority about personal data security breaches?

The data operators must notify Roscomnadzor if they become aware of a data leak affecting data subjects' rights. There should be two consecutive notices.

The first notice must be submitted within 24 hours. This notice must contain details about the incident, its alleged reasons, the potential harm to data subjects, elimination measures and the operator's contact person.

The second notice must contain internal investigation results and information about persons (if any) whose actions caused the leak. This notice must be submitted within 72 hours of becoming aware of the data leak. Hence, the operator must investigate the leak within 72 hours, but the Personal Data Law does not contain any rules on the investigation.

(Article 21(3.1), Personal Data Law.)

For more information on responding to cyber incidents including data breaches, as well as specific requirements for high-risk sectors or facilities, see Practice Note, Cyber Incident Response and Data Breach Notification (Russian Federation).

Processing by Third Parties

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

The Personal Data Law requires data processors to comply with the basic principles and processing rules under the Personal Data Law (Article 6(3), Personal Data Law). For more on these principles, see Question 8.

Data operators can engage third-party data processors on the basis of data subjects' consent (Article 6(3), Personal Data Law).

The Personal Data Law requires data operators to execute written contracts with third-party data processors to ensure the security and confidentiality of the personal data in the data processor's possession. The contract must include, among other things:

- A list of actions that the third party will perform.
- The purpose of the processing.
- IT security requirements.
- The third party's obligation to keep personal data confidential and secure, and otherwise comply with the Personal Data Law.
- Full list of processed data categories.
- Audit undertakings and data breach reporting procedures.
- The processor's obligations to fulfil the data localization requirement and perform various compliance measures.

(Article 6(3), Personal Data Law.)

Third-party data processors face contractual liability for violations of the Personal Data Law while data operators remain liable for these third parties' acts or omissions before data subjects. If the data processor is a non-Russian person or entity, both the processor and data operator are liable for third parties' acts or omissions before data subjects (Article 6(5) and (6), Personal Data Law).

Electronic Communications

18. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

The Personal Data Law does not define "cookies." There are no official guidelines from Roskomnadzor or other state agencies on the use, application, or distribution of cookies. However, Roskomandzor has recently started to apply general data protection principles to cookies and other online identifiers in practice. Therefore, preparing and publishing cookie-policies is becoming more popular.

19. What rules regulate sending commercial or direct marketing communications?

The Personal Data Law requires organizations to obtain the data subject's consent before processing personal data for the purposes of email communications promoting goods, works, or services. The data subject can revoke or withdraw consent at any time. (Article 15, Personal Data Law.) For more on consent, see Question 9.

Under the Advertising Law, a sender can send electronic commercial communications only with the addressee's prior consent and must immediately stop sending on the recipient's request. Failure to comply with these requirements can lead to different types of liability, including administrative liability. (Articles 18(1) and 38, Advertising Law.)

For information on the Advertising Law, see Country Q&A, Email Marketing Compliance: Russian Federation.

International Transfer of Data

Transfer of Data Outside the Jurisdiction

20. What rules regulate the transfer of data outside your jurisdiction?

Article 12 of the Personal Data Law regulates cross-border data transfers. The data exporter performs a transfer impact assessment (TIA) before conducting a cross-border transfer for the first time. This TIA will cover the subsequent transfers unless their conditions (for example, data importer, destination country, purpose, data categories) are changed.

During the TIA, the data exporter must assess how the data importer "ensures personal data confidentiality and security in the course of processing" based on the information received from the importer (Article 12(5), Personal Data Law). The Personal

Data Law establishes no assessment criteria or methodology. Consequently, the exporter must decide how to perform and document the TIA.

The data exporter must perform a TIA in all cases and for all destination countries with rare exceptions not applicable to business purposes. If there is an adequacy decision regarding the destination country, performing a TIA will not include the examination of the laws of that country. There are adequacy decisions in respect of all signatories to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and some other countries shortlisted by Roskomnadzor, for example:

- China;
- Singapore;
- Japan;
- South Korea;
- Israel; and
- Canada.

For the purpose of TIA, the data exporter must receive from the data importer the following information:

- The data importer's full name, postal address, phone number and email address.
- A description of how the data importer protects personal data to be received from the exporter (data protection measures) and under what conditions the data processing will be terminated.
- A general description of the privacy laws in the data importer's jurisdiction if there is no adequacy decision in respect of the destination country.

The exporter must disclose the information received from the data importer at the request of Roscomnadzor.

The data exporter must notify Roscomnadzor before conducting a cross-border transfer. The notice must contain the:

- Exporter's company name and address, date and number of the previously filed data processing notice (this is a general notice describing all data processing operations and security measures to be filed by everyone who processes personal data within Russia).
- Name of the DPO phone number, postal address and email address.
- Lawful basis and purpose of the cross-border transfer and further data processing.
- Data categories.
- Types of data subjects.
- Destination countries.
- Date of completing the TIA.

(Article 12(4), Personal Data Law.)

A notice must be filed before performing a cross-border transfer for the first time. The notice covers subsequent transfers until the details specified therein become outdated.

If there is an adequacy decision regarding the destination country, personal data can be transferred as soon as the exporter files the relevant cross-border transfer notice.

If there is no adequacy decision, the exporter must not conduct a cross-border transfer until Roskomandzor reviews the relevant cross-border transfer notice. As a rule, the exporter must wait for ten business days from filing the notice.

Roscomnadzor has the power to restrict or prohibit a cross-border transfer for protecting morality, citizens' health or rights and legal interests within ten business days of receiving the relevant cross-border transfer notice.

At the request of competent state authorities, Roscomnadzor has the power to restrict or prohibit a cross-border transfer in several cases related to the public security and interests. In such cases, a cross-border transfer can be suppressed any time (even once the ten-day period has expired).

If a cross-border transfer is restricted or prohibited, the data exporter must stop the relevant cross-border transfer and ensure that the data importer destroyed previously received data (Article 12(14), Personal Data Law).

The Personal Data Law does not require a separate international data transfer agreement. Parties can set rules governing personal data transfers by incorporating a special provision into the primary agreement between the parties or by including an addendum to that existing agreement.

The Personal Data Law does not recognize the concept of standard contractual clauses (SCCs), binding corporate rules (BCRs), or approved codes of conduct. For more on cross-border data transfers, see Practice Note, Cross-Border Personal Data Transfers (Russian Federation).

21. Is there a requirement to store any type of personal data inside the jurisdiction?

Federal Law 242 amended the Personal Data Law and the Information Law mainly by:

- Requiring all data operators, when collecting personal data, to ensure that any recording, systematization, accumulation, storage, change, or extraction of Russian citizens' personal data occurs in data centers located in the Russian Federation territory. This means that it is illegal to collect personal data of Russian nationals, directly upload, and process it on a non-Russian server without involving a database installed on a Russia-based server (Article 18(5), Personal Data Law).
- Introducing a mechanism for Roskomnadzor to block websites and online resources that illegally process Russian citizens' personal data (Article 15.5, Information Law).

Practitioners understand these requirements to prohibit data operators from storing Russian citizens' personal data outside of the Russian Federation without first storing the data within Russian territory. Therefore, local and foreign data operators must process or organize the processing of Russian citizens' personal data within the Russian Federation in the first place, subject to compliance with other general requirements of the Personal Data Law.

In general, the localization requirements do not:

- Prohibit access from abroad to servers, IT systems, databases, or data centers that are located within the Russian territory.
- Impose any special restrictions on the subsequent transfers, including cross-border transfers, of Russian citizens' personal data.

The localization requirements do not apply to the cases specified in Article 6(1), paragraphs 2, 3, 4, and 8 of the Personal Data Law which include processing:

- Required to achieve the purposes established by an international agreement or statute to fulfill a data operator's obligation under Russian law (Article 6(2), Personal Data Law).
- Performed for law enforcement purposes (Article 6(3), Personal Data Law).
- Performed by government agencies while providing public services (Article 6(4), Personal Data Law).
- For journalism, the mass media, or other scientific, literary, or creative activities, if the processing does not violate individuals' privacy rights (Article 6(8), Personal Data Law).

(Article 18(5), Personal Data Law.)

The Ministry of Digital Development, Communications, and Mass Media issued guidance (in Russian) further clarified that the localization requirements also do not apply to the activities of Russian and foreign air carriers and those acting on their behalf when processing the personal data of passengers traveling for the purposes of booking and issuing air tickets, baggage tickets, and other transportation documents.

However, data operators should rely on these exceptions with extreme caution, as Roskomnadzor has not adopted the guidance. For example, if a data operator updates or supplements the exempt personal data or uses it for a new purpose, the localization requirements will then apply. For more on localization requirements, see Question 20 and Country Q&A, Data Localization Laws: Russian Federation.

In practice, Roskomnadzor has already issued several significant fines for violations of the Data Localization Law , including on Facebook and Twitter for failing to comply with data localization requirements and on LinkedIn (in Russian) for refusing to transfer personal data of Russian individuals to Russian territory. LinkedIn was ultimately blocked from operating in the Russian Federation as a result of its non-compliance.

Data Transfer Agreements

22. Are data transfer agreements contemplated or in use? Has the supervisory authority approved any standard forms or precedents for cross-border transfers?

The Personal Data Law neither requires data operators to sign data transfer agreements, nor specifically regulates them. However, data transfer agreements are widely used in practice, especially when foreign parties or third-party operators are involved. Many data operators enter into these agreements with recipients located in and outside of the Russian Federation to prevent unauthorized disclosure or public distribution of personal data by recipients as required by law (Article 7, Personal Data Law).

Roskomnadzor has not adopted a standard form of data transfer agreement. Therefore, data operators must draft a suitable data transfer agreement in accordance with the specific data processing circumstances and confidentiality principles under basic contractual principles.

23. For cross-border transfers, is a data transfer agreement sufficient, by itself, to legitimize transfer?

See *Question 22*.

For more on cross-border data transfers, see Practice Note, Cross-Border Personal Data Transfers (Russian Federation).

24. Must the relevant supervisory authority approve the data transfer agreement for cross-border transfers?

The Personal Data Law does not require Roskomnadzor to approve or register data transfer agreements. For more on the rules regulating transfers, see Question 20.

Enforcement and Sanctions

25. What are the enforcement powers of the supervisory authority?

Roskomnadzor has certain enforcement powers including:

- Sending out requests to individuals and legal entities and obtaining necessary information on personal data processing.

- Carrying out inspections and checking the information contained in notifications on the processing of personal data and cross-border transfers submitted by data operators or engaging with other state agencies for this specific purpose.
- Rectifying, blocking, or destroying false or illegally obtained personal data.
- Limiting access to data that is processed in violation of the Personal Data Law; see Question 21.
- Suspending or terminating personal data processing that was initiated in violation of the Personal Data Law.
- Bringing civil actions before the competent courts to protect data subjects' rights and representing their interests before the trial.
- Submitting materials to the Prosecutor's Office and other law enforcement agencies for the purposes of commencement of criminal cases for data breaches.
- Issuing binding orders and bringing guilty parties to administrative liability.

(Article 23(3), Personal Data Law.)

26. What are the sanctions and remedies for non-compliance with data protection laws?

In the Russian Federation, non-compliance with data protection laws is generally punishable with:

- Civil lawsuits, including moral damages recoveries.
- Administrative sanctions, such as administrative fines and measures.
- Criminal sanctions, such as imprisonment.

The data protection laws have been enforced quite heavily in recent years, and data subjects have sent many complaints to Roskomnadzor. There has also been a growing number of appeals by data operators against Roskomnadzor orders and decisions imposing different sanctions on data operators and blocking their internet resources. As a result, national case law and court practice relating to sanctions for non-compliance with the data protection laws continues to evolve rapidly. Blocking platforms and websites remain the most serious concern and available sanction for online businesses and e-commerce platforms.

Amendments to relevant data protection laws and the Russian Code of Administrative Offenses came into force on February 24, 2021 that substantially increased the administrative sanctions for violations of data protection laws (Federal Law No. 19-FZ on Amendments to the Code of Administrative Offenses (February 24, 2021) (in Russian)).

Data protection violations have been categorized into the following types of privacy and data protection violations, which are now subject to the following administrative fines unless the offense constitutes a crime:

- Personal data processing in cases not provided by applicable laws and personal data processing incompatible with the processing purposes:

- company officers and government officials: RUB10,000 to RUB20,000; or
- companies: RUB60,000 to RUB100,000.

(Article 13.11(1), Code of Administrative Offenses.)

Repeated offenses can result in fines ranging from RUB100,000 to RUB300,000 for companies (Article 13.11(1.1), Code of Administrative Offenses).

- Personal data processing carried out without the data subject's written consent in cases where such consent is necessary, or with a written consent that does not meet mandatory requirements:
  - company officers and government officials: RUB20,000 to RUB40,000; or
  - companies: RUB30,000 to RUB150,000.

(Article 13.11(2), Code of Administrative Offenses.)

Repeated offenses can result in fines ranging from RUB300,000 to RUB500,000 for companies (Article 13.11(2.1), Code of Administrative Offenses).

- Failure to publish or provide access to a privacy policy or information on requirements for personal data protection:
  - company officers and government officials: RUB6,000 to RUB12,000; or
  - companies: RUB30,000 to RUB60,000.

(Article 13.11(3), Code of Administrative Offenses.)

- Failure to provide a data subject information on the processing of their personal data:
  - company officers and government officials: RUB8,000 to RUB12,000; or
  - companies: RUB40,000 to RUB80,000.

(Article 13.11(4), Code of Administrative Offenses.)

- Failure to satisfy within the prescribed time limit a request for personal data clarification, blocking or destruction, in cases where personal data is incomplete, outdated, imprecise, illegitimately received, or unnecessary for the announced purpose of data:
  - company officers and government officials: RUB8,000 to RUB20,000; or
  - companies: RUB50,000 to RUB90,000.

(Article 13.11(5), Code of Administrative Offenses.) Repeated offenses can result in fines ranging from RUB300,000 to RUB500,000 for companies (Article 13.11(5.1), Code of Administrative Offenses).

- Failure to comply with security requirements while storing tangible media containing personal data, and unauthorized access that results in illegitimate or accidental access to personal data or its destruction, modification, blocking, copying, submission, or dissemination:

- company officers and government officials: RUB8,000 to RUB20,000; or
- companies: RUB50,000 to RUB100,000.

(Article 13.11(6), Code of Administrative Offenses.)

- Failure of a state or municipal authority to meet the obligation to anonymize personal data or to comply with the anonymization methods or requirements:
  - RUB6,000 to RUB12,000.

(Article 13.11(7), Code of Administrative Offenses.)

- Failure to comply with data localization requirements:
  - company officers and government officials: RUB100,000 to RUB200,000; or
  - companies: RUB1,000,000 to RUB6,000,000.

(Article 13.11(8), Code of Administrative Offenses.)

- Repeated failure to comply with data localization requirements:
  - company officers and government officials: RUB500,000 to RUB800,000; or
  - companies: RUB6,000,000 to RUB18,000,000.

(Article 13.11(9), Code of Administrative Offenses.)

If Roskomnadzor investigates and identifies any data breach, it is empowered to:

- Initiate an administrative offense case.
- Prepare the administrative offense report against the infringer.
- Bring the administrative case to court.

The Russian authorities announced new fines (a percentage of the operator's turnover) for data leakages. However, the relevant bill had not been published at the time of writing.

Regulator Details

Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor)

W https://eng.rkn.gov.ru

W http://rkn.gov.ru/personal-data/register (personal data processing registry)

Main areas of responsibility. Supervision of legitimate data processing, accepting notifications, registering and maintaining the register of data operators, carrying out inspections and enforcement, and adopting official regulations and guidelines. The website is available in English and Russian.

Contributor Profile

Sergey Medvedev, PhD, LLM, Partner

Gorodissky & Partners
T +7 (495) 937 6116

F +7 (495) 937 6104

E medvedevs@gorodissky.ru

W www.gorodissky.com

Professional qualifications. Russia, Lawyer, 2005; Software Attorney, 2013; Trademark Attorney, 2014; Design Attorney, 2015.

Areas of practice. IP and IT; data protection and privacy, internet and e-commerce; media and entertainment; unfair competition and false advertising; dispute resolution and litigation; anti-counterfeiting and anti-piracy; IP/IT transactions and restructurings; and IP/IT due diligence and audits.

Stanislav Rumyantsev, PhD, Senior Lawyer

Gorodissky & Partners
T +7 (495) 937 6116

F +7 (495) 937 6104

E rumyantsevs@gorodissky.com

W www.gorodissky.com

Professional qualifications. PhD, CIPP/E.

Areas of practice. Data privacy and protection; e-commerce and marketing; domain names, websites and digital content; IT-outsourcing projects, development and implementation of information systems and cloud solutions; software development and distribution networks; know-how and protection of trade secrets; legal due diligence in

the IP, IT and Data Privacy fields; IP transactions, mergers and acquisitions in IT sector; dispute resolution and litigation; copyright, trademarks and IP management.

END OF DOCUMENT

RESOURCE HISTORY

Law stated date updated following periodic maintenance.

This document has been reviewed by the author as part of its periodic maintenance to ensure it reflects the current law and market practice on 1 August 2023.

Review Completed on June 23, 2022.

We reviewed this document on June 23, 2022 to ensure it reflects the most current law and market practice. We did not make any substantive changes to the document.

Review Completed June 10, 2021.

We reviewed this document on June 10, 2021 to ensure it reflects the most current law and market practice. We have revised this resource to include Federal Law No. 519-FZ on Amendments to Personal Data Law (December 30, 2020) (in Russian) which took effect March 1, 2021, and amends Federal Law No. 152-FZ on Personal Data (July 27, 2006) (Personal Data Law), and Federal Law No. 511-FZ on Amendments to the Code of Administrative Offenses (December 30, 2020) (in Russian).

Review Completed April 22, 2020.

We reviewed this document on April 22, 2020 to ensure it reflects the most current law and market practice. We did not make any substantive changes to the document.