Data Protection in the Russian Federation: Overview

by Sergey Medvedev, Gorodissky & Partners, with Practical Law Data Privacy Advisor

Country Q&A | Law stated as of 22-Apr-2020 | Russian Federation

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

This Q&A guide gives a high-level overview of data protection rules and principles, including obligations on the data controller and the consent of data subjects, rights to access personal data or object to its collection, and security requirements. It also covers cookies and spam, data processing by third parties, and the international transfer of data. This Q&A also details the national regulator, its enforcement powers, and sanctions and remedies.

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

Regulation

Legislation

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

General Laws

The main laws affecting personal 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 of July 27, 2006 on Information, Informational Technologies, and the Protection of Information (Information Law).
- Federal Law No. 152-FZ of July 27, 2006 on Personal Data (Personal Data Law).

The principal law in this area, and the primary focus of this Q&A, is the Personal Data Law.

Sectoral Laws

Data protection-specific provisions can also be found in various sectoral laws, for example:

- Federal Law No. 197-FZ of December 31, 2001 Labor Code of the Russian Federation (Labor Code) (Chapter 14).
- Federal Law No. 60-FZ of March 19, 1997, Air Code of Russian Federation (Air Code) (in Russian) (Article 85.1).
- Federal Law No. 323 of November 9, 2011 on the Fundamentals of Protection of the Health of Citizens in the Russian Federation (Health Protection Law) (in Russian).

There are also certain local administrative regulations, recommendations and guidance, and official requirements that regulate personal data collection, storage, and use issued by:

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

Sectoral laws, recommendations and guidance, and other regulations and requirements are 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 impose certain obligations on third parties acting under data operators' instructions and authorization. However, the Federal Law No. 152-FZ of July 27, 2006 on Personal Data (Personal Data Law) imposes liability on data operators and not data processors(Article 6(5), Personal Data Law). 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.

Russian data protection laws do not contain the concepts of data controller and data processor. Instead, the Personal Data Law uses the similar concepts of a data operator and person acting under the data operator's instructions and authorization.

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

- Organizes or carries out (alone or jointly with other persons) the processing of personal data.
- 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 delegate the processing to a third party, subject to the data subject's consent, who will be acting under the data operator's authorization based on a processing agreement, or by operation of a special state or municipal 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?

Data protection laws regulate all personal data processed by data operators, data processors, or third parties. Under the Federal Law No. 152-FZ of July 27, 2006 on Personal Data (Personal Data Law), personal data is any information that directly or indirectly relates to an identified or identifiable data subject (Article 3(1), Personal Data Law).

The Personal Data Law does not distinguish between direct personal data and indirect personal data. Therefore, personal data is considered "direct" or "indirect" depending on the facts of each case. For information on processing personal data, see Question 4.

The Personal Data Law also regulates special categories of personal data, defined to include an individual's:

- Race.
- Nationality.
- Political opinions.
- Religious or philosophical beliefs.
- Health conditions.
- Information about sex life.

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

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

The Personal Data Law also regulates the processing of personal data related to prior convictions (Article 10(3), Personal Data Law) and biometric personal data, which a data operator may process only with data subject consent or under other limited exceptions (Article 11, Personal Data Law).

4. What acts are regulated?

The Federal Law No. 152-FZ of July 27, 2006 on Personal Data (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?

The Federal Law No. 152-FZ of July 27, 2006 on Personal Data (Personal Data Law) does not contain any express provisions regarding its jurisdictional or territorial scope. It is generally presumed that, regardless of where the data operator or data processor is established or located, the Personal Data Law applies to:

- Data processing that occurs in or is targeted at the Russian Federation territory.
- The collection, storage, and use of Russian citizens' personal data.

Under the same principles, for cross-border transfers, the Personal Data Law applies to a certain extent if a Russian citizen either:

- Is a party to a terms of service or user agreement with a foreign data operator.
- Consents to a foreign data operator's collection and use of the citizen's personal data, such as through an online service, such as through an online store.

When a data operator is not established in the Russian Federation, the Personal Data Law does not require it to designate a local representative to address concerns from data subjects or the supervisory authority.

While the Federal Law No. 242-FZ of July 21, 2014 on Amending Certain Legislative Acts Concerning Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks (Data Localization Law) does not state whether it applies to organizations outside of the Russian Federation, the Federal Service for

Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) issued guidance (in Russian) suggesting that the Data Localization Law applies when an organization outside of Russia purposely directs its activities towards Russia and benefits from those activities. The following list of factors may evidence an organization's targeting of online activities in Russia:

- Primary factors include:
    - using websites registered with a Russian domain name including .ru, .su, and .moscow; and
    - deliberately translating a website by the website operator into Russian, regardless of which domain name the data operator uses, when also accompanied by at least one secondary factor.

- Secondary factors include:
    - allowing payments in Russian rubles;
    - making Russian phone numbers available on the website;
    - displaying Russia-oriented marketing activities, including keyword advertising or banners in Russian with a link to the relevant website;
    - including the possibility of concluding a contract with a Russian resident and delivery of goods or digital content in Russia; and
    - operating the website by the data operator's Russian branch or other local establishment, provided the local establishment's activities are directly linked to the activities performed via the website.

However, even without the above factors, the Data Localization Law will likely still apply if the website has other clear ties to the Russian market.

The Data Localization Law does 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).

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

The Roskomnadzor's guidance 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.

The guidance also notes that certain processing activities do not amount to collection under the Data Localization Law and are outside the scope of the law including:

- Third-party personal data collection that is provided to an operator, for example, if a third party sells its database of contacts. However, Roskomnadzor appears to be reconsidering this interpretation.
- Accidental receipt of personal data such as an unsolicited email from a data subject.

At the same time, data operators should rely on these exceptions with extreme caution. For example, if a data operator updates or supplements the exempt personal data or uses it for a new purpose, the Data Localization Law would then apply. For more on Data Localization Law requirements, see Question 20 and Question 21.

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

The Federal Law No. 152-FZ of July 27, 2006 on Personal Data (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 funds and 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 Federal Law No. 152-FZ of July 27, 2006 on Personal Data (Personal Data Law), a data operator that is processing personal data must notify the Federal Service for Supervision of Communications, Information Technology, and Mass Media (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 and it must contain the following information:

- The data operator's name and address, and the name and contact information of the natural person or legal entity responsible for organizing the processing.
- The purposes of personal data processing.
- The categories of personal data.
- The categories of data subjects whose data is being processed.
- The legal grounds for the processing.
- A list of proposed actions involving the personal data and a general description of the processing methods the data operator will use.
- A description of relevant IT systems and security measures (including encryption).
- The start date of the personal data processing.
- The duration of processing or the conditions for terminating the personal data processing.
- Information on cross-border data transfers.
- The location of the database that will contain the personal data of Russian individuals (see Question 21).

(Article 22(3)(1) to (11), 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 that contained in the notifications it receives. Except for the description of the data operator's IT systems and corresponding security measures, the information in the notification becomes publicly available once included in the register. (Article 22(4), Personal Data Law.) For more on the registry, see Box, Regulator Details.

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

- Is processed only under labor law.
- Has been received by the data operator in connection with a contract with a data subject, provided that the personal data is:
    - not transferred to third parties without the data subject's consent; or
    - used only to perform the contract or to enter into further contracts with the data subject.
- Relates to a certain type of processing by a public association or religious organization acting under the applicable laws, provided that the personal data is not distributed or disclosed to third parties without the data subject's consent.
- Has been made publicly available by the data subject.
- Consists only of the data subject's surname, first name, and patronymic.

- Is necessary for granting the data subject one-time access into the premises where the data operator is located.
- 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.
- Is processed without the use of automated systems under the applicable laws subject to compliance with the data subject's rights.
- Is processed in accordance with the laws and regulations relating to transport security.

(Article 22(2)(1) to (9), Personal Data Law.)

Notification and registration do not require the data operator to pay any official fee.

For information on individual notification requirements, see Question 12.

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 Federal Law No. 152-FZ of July 27, 2006 on Personal Data (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.)

- Responding to data subjects' requests for information within 30 days (Articles 18(1) and 20, Personal Data Law). For more on data subject rights, see Question 13 and Question 14.
- 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 notification, 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 data subject notification, see Question 12.
- Defining the categories of personal data, the purposes of data processing, and the duration of processing, if the data operator collected the personal data from a source other than the data subject, unless there is an exception (Article 18(3), Personal Data Law).
- Obtaining the data subject's consent before processing their personal data unless an exception applies. For more on consent, see Question 9 and Question 10.
- Taking measures that are necessary and sufficient to ensure proper personal data processing including:
    - appointing a data protection officer;
    - adopting a data protection policy and other required documents;
    - conducting audits to check compliance with the Personal Data Law and impact assessments following data breach incidents; and
    - training employees on compliance with the Personal Data Law.

  (Article 18.1(1), Personal Data Law.)
- When processing personal data, taking other appropriate security measures, especially legal, technical, and organizational measures to prevent unauthorized or unlawful data processing (Article 19(1), Personal Data Law).
- Using and storing personal data on storage systems and media with technology that protects against illegal or accidental access, dissemination, modification, or copying (Article 19(10), Personal Data Law).
- Locating the data center or data server in the territory of Russia, if the data operator collects and processes personal data of Russian individuals (Article 2, Federal Law No. 242-FZ of July 21, 2014 on Amending Certain Legislative Acts Concerning Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks (Data Localization Law); Article 18(5), Personal Data Law). For more on localization requirements, see Question 21.
- Notifying the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) to register before processing personal data, unless an exception applies (Article 22(1), Personal Data Law). For more on notification, see Question 7.
- Blocking or restricting 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, Federal Law No. 152-FZ of July 27, 2006 on Personal Data (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.

The data subject's consent must be specific, informed, and wilful. 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, practitioners typically find that implied or inferred consent is invalid.

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).

A data subject may revoke consent. When a data subject revokes consent, a data operator may continue to process the personal data only if the operator would otherwise be permitted to process the personal data without consent. For the legal bases to process personal data without consent, see Question 10.

The data operator has the burden of proof to establish that it obtained the data subject's consent (Article 9(3), Personal Data Law).

There is no prescribed or approved form of consent. However, the Personal Data Protection Act specifies the information that must appear in the data subject's written consent:

- The data subject's first name, middle name, surname, address, ID number, such as a passport number, date of issue of the ID, and issuing authority.
- The data subject's representative's first name, middle name, surname, 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 that is processing the personal data under the data operator's authorization.
- 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.

- 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 may 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).

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

Under Federal Law No. 152-FZ of July 27, 2006 on Personal Data (Personal Data Law), a data operator may process personal data without the data subject's consent when data processing is required to:

- Achieve objectives defined by an international treaty or under Russian law.
- Further certain judicial purposes.
- Perform certain powers by the federal authorities for state and municipal services.
- Execute an agreement either:
  - with the data subject; or
  - where the data subject is the beneficiary or guarantor.
- Protect the data subject's life, health, or other vital interests.
- Exercise 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.
- Pursue professional journalistic, media, scientific, literary, or other creative activities, provided there are no breaches of the data subject's rights and freedoms.
- Further statistical or other scientific purposes, provided the relevant personal data has been anonymized (depersonalized).
- Provide access to data that the data subject has made publicly available.
- Comply with applicable law that calls for mandatory publication or disclosure.

(Article 6(1)(1) to (11), Personal Data Law.)

Special Rules

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

Under the Federal Law No. 152-FZ of July 27, 2006 on Personal Data (Personal Data Law), sensitive data refers to any information that relates to nationality, racial or ethnic origin, political opinions, religious or philosophical beliefs, or the state of a person's health or sex life (Article 10(1), Personal Data Law).

A data operator may process sensitive data only if:

- The data subject provided written consent to the data processing.
- The data subject made their personal data publicly available.
- An international treaty on re-admission, for example, immigrants' 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 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 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.)

State and municipal bodies may 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 may process only with the data subject's written consent unless:

- An international treaty on re-admission (for example, immigrants' return to the country) requires it.
- The processing is consistent with Russian legislation on state defense, security, anti-terrorism, transport safety, anti-corruption, law enforcement, execution, criminal investigation, prosecution, 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 should be provided to data subjects at the point of collection of the personal data?

Under Federal Law No. 152-FZ of July 27, 2006 on Personal Data (Personal Data Law) and the Regulation on the Particulars of Personal Data Processing Performed Without the Use of Automated Means approved by the Decree of the Government of the Russian Federation No. 687 of September 15, 2008) (in Russian) (Personal Data Law Decree), a data operator must provide written notice to data subjects if the operator:

- Uses non-automated means to process the personal data (Sections 7(a) and 8(a), (Personal Data Law Decree)). If the data operator processes personal data using non-automated means, the data operator must advise data subjects in writing of:
    - the data operator's name and address;
    - the data subject's name and address;
    - the purpose for data processing;
    - the term of data processing;
    - a description of data processing methods and personal data uses; and
    - the source of the personal data.

(Sections 7(a) and 8(a), 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; and
  - explain how the data subject may protect their rights and legitimate interests relating to the processing.

  (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;
  - 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 obligated 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 has made the personal data publicly available, or the data operator received the personal data from a source open to the public;
  - 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.)

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 Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) issued non-binding guidance (in Russian) for data operators on drafting privacy and data protection policies that comply with the Personal Data Law. In practice, Roskomnadzor considers whether data operators follow the guidance when conducting compliance investigations.

13. What other specific rights are granted to data subjects?

Under Federal Law No. 152-FZ of July 27, 2006 on Personal Data (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 of the data processing by the data operator.
- The legal grounds and purposes of data processing.
- The methods and purposes of data processing used by the data operator.
- The data operator's name and location, and information on the persons (except for employees) who have access to the personal data or to whom personal data may be disclosed under the agreement with the data operator or under the law.
- How a data subject may exercise their rights under the Personal Data Law. For more on these rights, see Question 12, Question 13, and Question 14.
- The duration of data processing, including the duration of storage of personal data.
- Information on any completed or prospective cross-border data transfers.
- The name and address of anyone processing the data on the data operator's behalf.
- Other information provided by the Personal Data Protection Act and other laws.

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

Data subject has the right to:

- Data access, correction, modification, and deletion (Article 14, Personal Data Law).
- Object to direct marketing (Article 15(1), 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).

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

- Incomplete.
- Out of date.
- Inaccurate.
- Unlawfully obtained.
- Not necessary for the declared or claimed purposes of data processing.

(Article 14(1), Personal Data Law.)

Data operators have:

- Thirty days to grant or deny a data subject's access request (Article 20(1) and (2), Personal Data Law).
- Seven working days to respond to the data subject's deletion or modification requests (Article 20(3), Personal Data 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 Federal Law No. 152-FZ of July 27, 2006 on Personal Data (Personal Data Law), a data operator must take necessary and sufficient protective security measures to protect personal data. These measures include the following:

- Appointing a data protection officer.
- Adopting a privacy and data protection policy and other documents, including corporate orders and rules, intended to prevent and detect breaches and violations of the Personal Data Law.
- Implementing other relevant legal, organizational, and technical security measures.
- Performing internal assessments and audits to ensure compliance with the Personal Data Law and the data operator's internal policies.
- Evaluating harm caused to data subjects in the event of a breach.
- Training employees on the relevant provisions of the Personal Data Law and internal data protection policies.

(Article 18.1(1)(1) to (6); 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 in the course of processing personal data.
- Processing personal data in specific IT systems that employ appropriate protections for personal data and have passed assessment procedures.
- Assessing security measures' effectiveness before implementation.
- Recording any computer media that contains personal data.
- Applying different certified methods of protection of personal data (including encryption).
- 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 subject to specific additional security requirements, including those set by the 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.

16. Is there a requirement to notify personal data security breaches to data subjects or the national regulator?

There is generally no legal requirement to report data breaches to data subjects or to the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor).

After locating or detecting unauthorized processing of personal data, Federal Law No. 152-FZ of July 27, 2006 on Personal Data (Personal Data Law) requires data operators (or the relevant authorized person) to terminate the personal data processing within three business days. If the data operator cannot remedy the unlawful data processing, it must destroy the personal data within ten business days. Following the termination of processing or personal data destruction, the data operator must notify the data subject or their representative.

If Roskomnadzor made the termination or destruction request, the data operator must send the corresponding notification to the Roskomnadzor. (Article 21(3), 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 Federal Law No. 152-FZ of July 27, 2006 on Personal Data (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 engaging third-party data processors under the Personal Data Law must obtain data subject consent to disclose the personal data unless an exception applies (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.
- The third party's obligation to keep personal data confidential and secure, and otherwise comply with the Personal Data Law.

(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 all acts or omissions of these third parties (Article 6(5), Personal Data Law).

Data processors must also:

- Keep personal data confidential (Article 7, Personal Data Law).
- Protect personal data against loss, misuse, modification, unauthorized or accidental access or disclosure, alteration, or destruction.
- Provide the level of protection for the personal data that the Personal Data Law requires.

(Articles 6(3) and 19; 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).)

Personal data transfers within and outside the Russian Federation must satisfy the same general requirements. For more on personal data transfers, see Question 20.

Electronic Communications

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

The Federal Law No. 152-FZ of July 27, 2006 on Personal Data (Personal Data Law) does not define "cookies." There are no official guidelines from the Federal Service for Supervision of Communications, Information Technology, and Mass Media (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.

A person distributing information must provide the addressee with the explicit option of rejecting the information when using a method that allows for addressee's identification, including when sending regular postal messages and electronic messages (Article 10(3), Federal Law No. 149-FZ of July 27, 2006 on Information, Informational

Technologies, and the Protection of Information). Therefore, it is generally presumed that all types of cookies require the data subject's opt-in consent in the absence of more specific legislation or guidance on this point.

19. What requirements are imposed on the sending of unsolicited electronic commercial communications (spam)?

Unsolicited electronic commercial communications (spam) are not allowed in Russia. A sender may 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, Federal Law No. 38-FZ of March 13, 2006 on Advertising.)

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 Federal Law No. 152-FZ of July 27, 2006 on Personal Data (Personal Data Law) regulates cross-border data transfers. Before making an international transfer, data operators must ensure that the receiving country provides an adequate level of protection for data subject rights unless an exception applies (Article 12(1), Personal Data Law). Countries that provide an adequate level of protection include:

- All countries that are signatories to the Strasbourg Convention (Article 12(1), Personal Data Law).
- Countries included on the official list (in Russian) maintained by the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor), which includes Australia, Argentina, Canada, Israel, Mexico, and New Zealand, among others.

International data transfers to any jurisdiction with the adequate protection level are not subject to any restriction and do not require any specific authorization.

Cross-border transfers of personal data to countries that do not provide a level of adequate protection are permitted only if the:

- The data operator has obtained the data subject's written consent.

- An international treaty to which the Russian Federation is a party permits the cross-border data transfer.
- The cross-border data transfer is allowed under applicable laws as necessary for the purposes of:
    - protecting the Russian constitutional system;
    - protecting the national state defense and state security; or
    - securing the maintenance of the Russian transportation system, and protecting the interests of individuals, society and the state in the transportation sector from illegal intrusion.
- The cross-border data transfer is needed to perform a contract to which the data subject is a party.
- The cross-border data transfer is required to protect the data subject's life, health, or other vital interests and it is impossible to obtain their prior consent in writing.

(Article 12(4), 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 appropriate safeguards for cross-border transfers such as standard contractual clauses (SCCs), binding corporate rules (BCRs), or approved codes of conduct. Typically, companies acting as data operators will:

- Confirm whether the receiving country provides an adequate level of data protection before transferring any personal data abroad.
- Obtain written consent from the respective data subjects, if required.
- Execute international data transfer or confidentiality agreements with third-party recipients, such as foreign data operators.

Following these steps, companies will proceed with cross-border data transfers in accordance with their applicable internal corporate rules, orders, or policies.

In addition to the Personal Data Law, Roskomnadzor has issued comments and a set of FAQs (in Russian) stating that data operators may make cross-border personal data transfers if the data operator both:

- Complies with Article 12 of the Personal Data Law.
- Stores a primary copy of the database containing Russian citizens' personal data, collected in Russia, in the Russian territory, including any subsequent updates and additions to that personal data. For more on localization requirements, see Question 21.

The guidance also indicated that any cross-border personal data transfer must be consistent with the stated or claimed purpose of data processing. After the purpose is achieved, the data processing must be terminated or stopped.

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

21. Is there a requirement to store (certain types of) personal data inside the jurisdiction?

On July 21, 2014, the President of the Russian Federation signed Federal Law No. 242-FZ of July 21, 2014 on Amending Certain Legislative Acts Concerning Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks (Data Localization Law), which became effective on September 1, 2015.

The Data Localization Law amends the Federal Law No. 152-FZ of July 27, 2006 on Personal Data (Personal Data Law) mainly by introducing:

- New obligations for data operators on collecting, storing, and processing Russian citizens' personal data.
- A new mechanism for the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) to block websites and online resources that illegally process Russian citizens' personal data.

Specifically, the Data Localization Law requires all data operators to ensure that any recording, systematization, accumulation, storage, change, or extraction of Russian citizens' personal data occurs in data centers located in Russian Federation territory. This means that any Russian citizens' personal data that data operators collect must be stored in servers, IT systems, databases, or data centers located in Russia. (Article 2, Data Localization Law.)

Although the Data Localization Law does not expressly state it, practitioners understand the law to prohibit data operators from storing Russian citizens' personal data outside of the Russian Federation without first storing the data within Russian territory. Therefore, all 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 Data Localization Law does not:

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

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 noncompliance. Facebook and Twitter have appealed the lower court decisions.

Data Transfer Agreements

22. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

Federal Law No. 152-FZ of July 27, 2006 on Personal Data (Personal Data Law) does not specifically regulate data transfer agreements, but they are widely used in practice, especially when foreign parties or third-party operators are involved.

The Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) has not adopted a standard form of data transfer agreement. Therefore, data operators must draft any data transfer agreement in accordance with the specific data processing circumstances and confidentiality principles under basic contractual principles.

23. Is a data transfer agreement sufficient to legitimize transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

Under Federal Law No. 152-FZ of July 27, 2006 on Personal Data (Personal Data Law), a data transfer agreement is generally sufficient to legitimize international personal data transfers to countries that do not provide an adequate level of protection if the data subject's consent is expressly stated in, or attached to, the agreement. In certain exceptional instances, data transfer agreements will be executed as trilateral contracts. Transfers to countries with adequate data protection do not require data subject's consent in addition to the data transfer agreement. For more on the rules regulating transfers, see Question 20.

The data operator also must notify the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) about its right to make the cross-border data transfer when it notifies the regulator for registration purposes. For more on the notification and registration requirements, see Question 7.

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

24. Does the relevant national regulator need to approve the data transfer agreement?

The Federal Law No. 152-FZ of July 27, 2006 on Personal Data (Personal Data Law) does not require the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) to approve or register data transfer agreements. The data operator and third party must execute a written data transfer agreement that contains certain confidentiality and other obligations to be effective and enforceable. For more on the rules regulating transfers, see Question 20.

Enforcement and Sanctions

25. What are the enforcement powers of the national regulator?

The Federal Service for Supervision of Communications, Information Technology, and Mass Media (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 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 Federal Law No. 152-FZ of July 27, 2006 on Personal Data (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.
- Filing petitions with the Federal Service for Technical and Export Control (FSTEC), the Federal Security Service (FSS), and other state agencies to suspend or cancel relevant licences.
- 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 Russia, non-compliance with data protection laws can be generally punishable with:

- Civil sanctions, such as moral damages.
- Administrative sanctions, such as administrative fines.
- Criminal sanctions, such as imprisonment.

Russian data protection laws have been enforced quite heavily in recent years, and data subjects have sent many complaints to the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor). There has also been a growing number of appeals by data operators against the orders and decisions of Roskomnadzor 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 Russian 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 on Administrative Offenses came into force on July 1, 2017 that substantially increased the administrative sanctions for violations of data protection laws. 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:
    - a warning in place of a fine;
    - individuals: RUB1,000 to RUB3,000;
    - individual entrepreneurs: RUB5,000 to RUB10,000;
    - company officers and government officials: RUB5,000 to RUB10,000; or
    - companies: RUB30,000 to RUB50,000.

    (Article 13.11(1), Code on 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:
    - individuals: RUB3,000 to RUB5,000;
    - individual entrepreneurs: RUB10,000 to RUB20,000;

- company officers and government officials: RUB10,000 to RUB20,000; or
- companies: RUB15,000 to RUB75,000.

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

- Failure to publish or provide access to a privacy policy or information on requirements for personal data protection:
  - a warning in place of a fine;
  - individuals: RUB700 to RUB1,500;
  - individual entrepreneurs: RUB5,000 to RUB10,000;
  - company officers and government officials: RUB3,000 to RUB6,000; or
  - companies: RUB15,000 to RUB30,000.

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

- Failure to provide a data subject information on the processing of their personal data:
  - a warning in place of a fine;
  - individuals: RUB1,000 to RUB2,000;
  - individual entrepreneurs: RUB10,000 to RUB15,000;
  - company officers and government officials: RUB4,000 to RUB6,000; or
  - companies: RUB20,000 to RUB40,000.

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

- Failure to satisfy within the prescribed time limit a request on 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:
  - a warning in place of a fine;
  - individuals: RUB1,000 to RUB2,000;
  - individual entrepreneurs: RUB10,000 to RUB20,000;
  - company officers and government officials: RUB4,000 to RUB10,000; or
  - companies: RUB25,000 to RUB45,000.

(Article 13.11(5), Code on 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:
    - individuals: RUB700 to RUB2,000;
    - individual entrepreneurs: RUB10,000 to RUB20,000;
    - company officers and government officials: RUB4,000 to RUB10,000; or
    - companies: RUB25,000 to RUB50,000.

    (Article 13.11(6), Code on 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:
    - a warning in place of a fine; or
    - RUB3,000 to RUB6,000.

    (Article 13.11(7), Code on Administrative Offenses.)
- Failure to comply with data localization requirements:
    - individuals: RUB30,000 to RUB50,000;
    - company officers and government officials: RUB100,000 to RUB200,000; or
    - companies: RUB1,000,000 to RUB6,000,000.

    (Article 13.11(8), Code on Administrative Offenses.)
- Repeated failure to comply with data localization requirements:
    - individuals: RUB50,000 to RUB100,000;
    - company officers and government officials: RUB500,000 to RUB800,000; or
    - companies: RUB6,000,000 to RUB18,000,000.

    (Article 13.11(9), Code on 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.

Roskomnadzor has also announced its intention (in Russian) to impose administrative liability for the illegal acquisition of personal data, and will introduce legislation in 2020 affording it that authority. Roskomnadzor's primary enforcement concern at present is compliance with data localization requirements.

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; IP/IT due diligence and audits.

Languages. Russian, English, French

END OF DOCUMENT

