大成 DENTONS

Summer is ending

Key changes to personal data laws in the first half of 2022

August 2022

The new Federal Law No. 266 signed by the president of Russia on July 14, 2022 (the "**Law**"),[1] substantially amends some of the legislative acts governing personal data processing in Russia. Most of the Law's provisions take effect September 1, 2022.

This overview presents the key changes to Russian personal data laws over the first half of 2022 and covers the issues most relevant for personal data operators.

1. New obligations related to security incidents

The Law required personal data operators to notify Roskomnadzor of security incidents that resulted in violation of data subjects' rights. The new obligation applies to cases of transfer (provision, dissemination, accessing) of personal data whether they resulted from wrongdoing or were accidental. Considering the broad definition of "data subjects' rights", many such incidents will fall under the Law.

Pursuant to the Law, this new obligation of the personal data operator arises as soon as a security incident is discovered.

The obligation involves giving Roskomnadzor two notifications: an initial notification within 24 hours with information about the security incident, and subsequent notification within 72 hours with the results of internal investigation of the incident. The details to be included in the notifications are listed in the right column of this page.

Deadline for notification	Information to be included in the notification
24 hours	• About the security incident • About the suspected causes of the violation of data subjects' rights • The anticipated harm to data subjects' rights • Steps taken to control damage done by the security incident • About the person authorized to interact with Roskomnadzor regarding the security incident
72 hours	• The results of internal investigation of the security incident • About people whose actions caused the security incident (if any)

Thus, the personal data operator will have to carry out an internal investigation of the security incident within three days from its discovery. A company must have sufficient resources and implement the respective business processes to meet this deadline.

Information about security incidents will be recorded in a special register. Roskomnadzor will determine how and on what conditions personal data operators work with the register.

Personal data operators will also be required to interact with the state system for detecting, preventing and eliminating the consequences of cyberattacks on Russia's information resources ("**GosSOPKA**").

[1] Federal Law No. 266-FZ of July 14, 2022, on Amending the Federal Law on Personal Data and Certain Legislative Acts of Russia, and Repealing Article 30(14) of the Federal Law on Banks and Banking.

As part of interacting with GosSOPKA, personal data operators must notify the FSB only of security incidents that occurred as a result of wrongdoing. The FSB will approve a procedure for interacting with GosSOPKA.

Liability for security incidents

There is currently no special administrative liability of personal data operators for security incidents: Roskomnadzor considers such cases under Article 13.11(1) of the Russian Code of Administrative Offenses (the so-called general offense). However, the possibility of introducing fines, including turnover fines, for both the incidents themselves and for failing to file notifications of incidents is being discussed.

Important to note:

- Instructions to process personal data (standard forms and concluded contracts) in relation to the interaction process when security incidents occur
- Internal processes and rules for actions for when security incidents occur

2. Application of personal data laws to foreign companies

In recent years, the law enforcement practice on the application of Federal Law No. 152-FZ on Personal Data of July 27, 2006 (the "**Personal Data Law**") to foreign companies that do not have a physical presence in Russia has been narrow. Practice was based on targeting criteria (for more detail, see the overview Personal Data: Ten facts that foreign business in Russia should know). Now the Personal Data Law explicitly states that foreign legal entities will be required to comply with the Law when processing Russian citizens' personal data under a contract or other agreements with those citizens, and on the basis of a consent to process personal data.

The Law has essentially introduced a stricter and broader rule than the previously applied targeting criteria. Roskomnadzor used to highlight compliance with the requirement for "localization" of databases containing Russian citizens' personal data, to publish personal data processing policies and have legal grounds to process data. There are now more requirements: foreign personal data operators will also have to comply with other requirements of the Personal Data Law (e.g., cybersecurity requirements, requirements to the set of policies, and times for responding to data subjects, etc.).

In the context of such broad application of the Personal Data Law, it is notable that special liability for failing to comply with a Roskomnadzor decision prohibiting the collection of Russian citizens' personal data is being introduced. This prohibition is one of the coercive measures under the so-called "Landing Law"[2] that applies to foreign entities conducting activities on the Internet in Russia.

The liability involves an administrative fine of up to RUB 6 million for a first offense and up to RUB 18 million for a repeat offense.

Important to note:

- Approach of a foreign company to whether or not the Personal Data Law applies to its activities

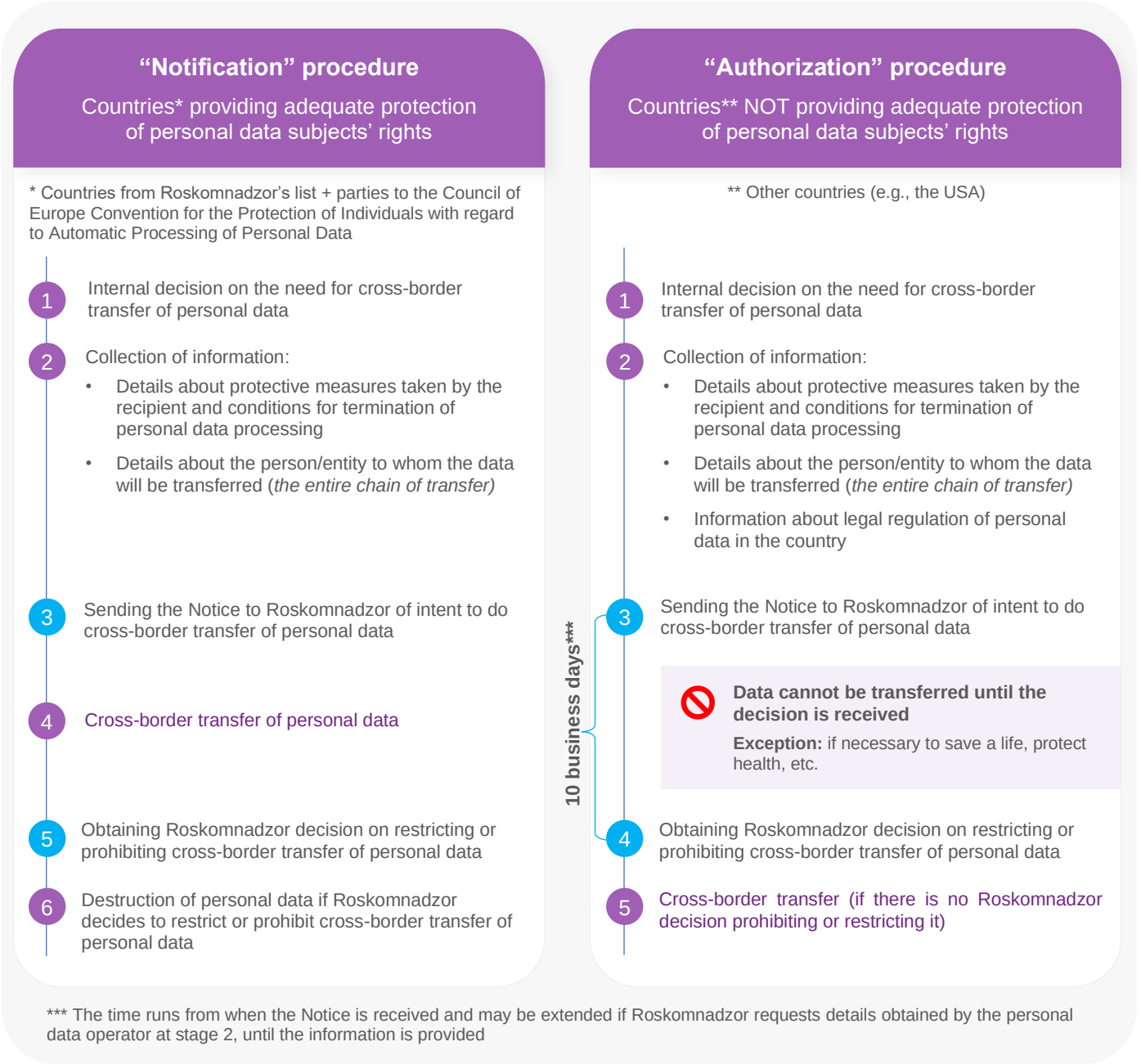
3. New rules for cross-border transfer of personal data

Major amendments have been made to the Personal Data Law relating to cross-border transfer of personal data.

The procedure will remain the same until March 1, 2023: cross-border transfer of personal data to countries that do not provide adequate protection of data subjects' rights (e.g., the USA) is possible in the five cases listed in the Personal Data Law. Special grounds are not required to transfer personal data to countries that provide adequate protection of data subjects' rights (e.g., EU countries).

Starting March 1, 2023, personal data operators will be required to notify Roskomnadzor of their intention to transfer personal data abroad (the "**Notice**"). The Notice will either be a notification or an authorization, depending on which country the data are being transferred to. The diagrams on the next page show the new procedures for cross-border transfer of personal data.

[2] Federal Law No. 236-FZ of July 1, 2021, on the Activities of Foreign Persons on the Internet in Russia.



Once Roskomnadzor examines the Notice it can decide to prohibit or restrict the cross-border transfer of personal data to protect citizens' morality, health, rights, and legitimate interests.

The Notice can be filed in hard copy or electronically. There is no special approved form. The Notice will need to contain the following information:

- About the personal data operator and **notice of intent to process personal data**
- About the data protection officer
- The legal ground and purpose of the cross-border transfer and further processing of personal data
- The categories and list of personal data to be transferred
- The categories of data subjects
- The list of countries where the personal data will be transferred
- The date of the personal data operator's audit of recipients' compliance with confidentiality and security obligations regarding data processing

When the Law was being considered in Russia's State Duma, Roskomnadzor explained that personal data operators will have to send a Notice once for each country to which personal data will be transferred. But the Law does not directly imply this interpretation, so it

is advisable to wait for further Roskomnadzor guidance on this issue.

In addition, there are now more grounds for restricting or prohibiting cross-border transfer of personal data. They include, for example, protecting Russia's economic and financial interests, and Russia's sovereignty, security, territorial integrity and other interests internationally. These restrictions and bans may be imposed as stipulated by the Russian government and if there is a submission from a government authority competent in the relevant area.

Personal data operators that transferred personal data abroad prior to September 1, 2022, and will continue to do so after that date are required to file a Notice not later than March 1, 2023.

Important to note:

- Cases and specifics of cross-border transfer of personal data at the company
- Whether a notice of intent to process personal data has been filed with Roskomnadzor

4. New requirements for the instruction to process personal data

When another company is involved in processing personal data, for example, to provide accounting services or IT support, the instruction to process personal data must be in writing. The Law has expanded the list of requirements to the contents of the instruction. For example, now it must contain the list of personal data, the obligation to comply with the personal data localization requirement, provisions on interaction with and notification of the operator regarding security incidents, etc.

The Law states that if a foreign legal entity is instructed to process personal data, that entity is liable to data subjects together with the personal data operator. It can be concluded from this rule that the foreign legal entity and the data operator will share liability depending on their specific actions that harmed the data subject.

Important to note:

- Instructions to process personal data (standard forms and concluded contracts) for new provisions that must be included in them

5. Change in the rules for notifying of intent to process personal data

5.1. More cases requiring notification of intent to process personal data

Companies processing personal data, including branches and representative offices, must generally notify Roskomnadzor when they start processing personal data. The Personal Data Law has been amended to considerably limit the number of cases in which a personal data operator does not have to notify Roskomnadzor, for example, if:

- The personal data are being processed in government information systems
- The personal data are being processed without using automation
- The personal data are being processed under transportation safety laws

So, most operators will now be required to notify Roskomnadzor.

5.2. The notice of intent to process personal data must be detailed

Personal data operators used to be required to list details including the following in a notice: the categories of personal data and data subjects, the legal grounds for processing, the list of actions and methods of processing personal data. The Law has updated this obligation. Now these details must be given for each processing purpose.

5.3. New deadline for notifying of changes in personal data processing

The Law gives personal data operators more time to notify Roskomnadzor of a change of details contained in a notice of intent to process personal data.

Operators must now notify Roskomnadzor of changes by the 15th day of the month after the month in which the changes occurred.

Important to note:

- Whether a notice of intent to process personal data has been filed with Roskomnadzor

6. Restriction on personal data collection

6.1. Collection of consumers' personal data

Amendments made to Russian Law No. 2300-1 on Consumer Protection of February 7, 1992 (the "**Consumer Protection Law**")[3] introduced the concept of "unacceptable contract terms." They also specify a number of conditions that are considered by default as infringing consumers' rights. The conditions include, for example: the seller's right to unilaterally refuse to perform an obligation; limitation of the consumer's right to choose the venue for disputes, and exclusion or limitation of the seller's liability for nonperformance or improper performance of an obligation when not provided for by law.

At the same time, according to the amendments made to the Consumer Protection Law, the seller (provider, marketplace owner) may not refuse to enter into, perform, amend or terminate a contract with a consumer because the latter refuses to provide their personal data, unless:

- The personal data must be provided by law
- The personal data are directly related to performance of the contract with the consumer (e.g., when the consumer's address is needed to deliver the product)

Consumers have the right to demand clarification as to why the contract cannot be entered into, amended or terminated without providing personal data, and the legal grounds for this.

Starting September 1, 2022, legal entities could face an administrative fine of up to RUB 50,000[4] for failing to follow the rules for such refusal.

6.2. Collection of biometric personal data

A number of legislative restrictions and bans have been introduced on the processing of biometric personal data since 2020. This trend continues with the Personal Data Law gaining the rule that provision of biometric personal data cannot be mandatory. The only exceptions to this rule are when biometric personal data are processed on legal grounds other than the data subject's consent.

The Personal Data Law now also explicitly states that a personal data operator cannot deny a data subject service for refusing to provide their biometric data and/or consent to process their data, unless the consent is required by law.

Important to note:

- Processes for collecting consumers' personal data and grounds / reasons for collecting the data

7. Updated requirements for inhouse documentation of personal data operators

7.1. Obligation to maintain the register of personal data processing activities

The Law has required personal data operators to issue inhouse policies detailing their personal data processing activities. The Law has essentially introduced a "light" version of the so-called register of personal data processing activities as a mandatory document. Keeping that document was one of the practices personal data operators followed even before the Law was adopted. The Law states that personal data operators must provide the following information in the inhouse policy for each data processing purpose:

- The categories and list of personal data to be processed
- The categories of personal data subjects whose data are processed
- How personal data are processed and how long they are stored
- How personal data are destroyed

7.2. Requirements for publishing personal data processing policies

According to the Law, if personal data are collected using the Internet, then the policy must be published not just on the site, but also on the relevant webpages where the personal data are collected. We believe that it should also be acceptable to display an active hyperlink to the policy (for example, as a pop-up window or a redirect to a special page).

[3] Federal Law No. 135-FZ of May 1, 2022, on Amending Article 16 of the Russian Law on Consumer Protection.

[4] Federal Law No. 145-FZ of May 28, 2022, on Amending Article 14.8 of the Russian Code of Administrative Offenses.

7.3. Restriction of practices in the field of personal data processing not provided for by law

The Personal Data Law now has a provision that an operator's documents relating to personal data processing cannot contain provisions restricting data subjects' rights and give operators powers and obligations not provided for by Russian law.

The latter restriction needs to be further clarified by Roskomnadzor. That's because it's unclear whether this restriction covers cases where, according to another jurisdiction, the personal data operator is also required to meet foreign regulatory requirements applicable to it (e.g., the requirements of the General Data Protection Regulation (GDPR)).

Important to note:

- Inhouse documentation about personal data processing
- Whether site/app contains the personal data processing policy on each page where the personal data are collected

8. Changes in times for interaction with personal data subjects and Roskomnadzor

The amendments to the Personal Data Law have made the time for personal data operators to contact data subjects and Roskomnadzor three times shorter. Personal data operators will have to take the following actions within 10 business days (depending on which request was received):

- Reply to a data subject's request for information about the processing of their personal data
- Notify the data subject that it has personal data relating to the data subject and give the data subject the opportunity to review the data
- Reply to a Roskomnadzor request

The time can be extended by not more than five business days if the personal data operator advises the data subject or Roskomnadzor, respectively, of the reason for the extension.

The Personal Data Law has also introduced the principle that the form of the reply to a data subject's request for information about the processing of their personal data must be identical. By default, it should be given in the same form as the request.

Important to note:

- Internal processes of the company regarding communications with Roskomnadzor and data subjects

9. Additional criteria for personal data processing consent validity

Whether a consent was valid was previously determined using the following formula: the consent must be concrete, informed and conscious. The Law has now added that the consent must also be specific and unambiguous. However, these additional criteria are value judgments and must be assessed on a case-by-case basis. But at this stage it can be concluded that the consent must be more detailed and definite.

Important to note:

- Current consent forms in terms of meeting criteria of being specific and unambiguous

10. Active steps of personal data subjects are now required

The Personal Data Law now includes a provision that a contract made with a data subject cannot contain provisions allowing it to be made through the data subject's inaction. This is meant to stop such practices as end user agreements including personal data processing provisions to which a user agrees by "continuing to use the site."

Important to note:

- User documentation (agreements, banners, terms of use, etc.)

Enactment of the Law

September 1, 2022

All of the Law's provisions go into effect, other than those listed below.

March 1, 2023

The provisions described in sections 3 and 5.3 of this overview go into effect, plus a number of other minor changes.

A Notice must be filed by March 1, 2023, if cross-border transfer of personal data was done prior to September 1, 2022, and is ongoing.

Contacts

Victor Naumov

Saint Petersburg Managing Partner, PhD in Law

Dentons

T +7 812 325 84 44

victor.naumov@dentons.com

Vladislav Arkhipov

Counsel, Russia IP, IT and Telecommunications practice, PhD in Law

Dentons

T +7 812 325 84 44

vladislav.arkhipov@dentons.com

Kseniia Smirnova

Senior Associate, Russia IP, IT and Telecommunications practice

Dentons

T +7 812 325 84 44

kseniia.smirnova@dentons.com

Alexander Kotov

Junior Associate, Russia IP, IT and Telecommunications practice

Dentons

T +7 812 325 84 44

alexander.kotov@dentons.com