ALRUD

Newsletter

Regulation in the field of personal data: what to expect in 2023?

December 23, 2022

Dear Ladies and Gentlemen!

We would like to inform you about the upcoming changes in the regulation of personal data which will take effect in 2023. The mentioned changes comprise:

- New order of planned state inspections over personal data processing in 2023;
- Changes in cross-border data transfer;
- Assessment of harm that may be caused to personal data subjects in case of violation of personal data legislation;
- New forms of notifications on personal data processing;
- The procedure for destruction of personal data.

New rules for cross-border data transfers

New rules for cross-border data transfer will come into force on March 1, 2023. If you plan to transfer personal data abroad from March 1, 2023, you will have to submit a respective notification to the Russian DPA ("**Roskomnadzor**").

Depending on "adequacy" of personal data protection in the country to the territory of which data is to be transferred, you will be able to start transferring data immediately after submitting the notification, or 10 days after its consideration by Roskomnadzor. Read more about the latest changes related to cross-border transfer of personal data in our newsletter by clicking here.

Partial moratorium on planned audits of Roskomnadzor in 2023

In March 2022 a moratorium on scheduled state audits was declared, including the sphere of personal data. Such moratorium is valid until December 31, 2022.

On October 1, 2022, the Government approved extension of the partial moratorium on planned inspections in 2023. Next year, planned inspections by government agencies will only be allowed in relation to objects of control classified as extremely high and high risk.

As for Roskomnadzor's state control over personal data processing, planned inspections in 2023 can be implemented by the regulator with respect to data controllers that have committed violations in the following areas and under the following conditions[1]:

[1] The criteria for assessment of risk category are defined in Annex 1 to the Regulation on Federal State Control of Personal Data Processing (Decree of the Government of the Russian Federation of 29.06.2021 N 1046). Criteria for the extremely high risk category are not defined in the area of personal data processing. Criteria for the **high risk** category are specified.

Consequences of violation of personal data legislation	Type of violation of personal data legislation
Issuance of an order / demand to eliminate the violation / warning to prevent the violation within the last 2 years ***AND / OR*** Bringing to administrative liability within 3 years preceding the date of the decision to classify the activity of the supervised entity as a risk category	Processing of sensitive data and (or) biometric personal data
	Collection of personal data, including via the Internet, performed with the use of databases located outside the Russian Federation
	Cross-border data transfer to "inadequate" jurisdictions
	Transfer of depersonalized personal data to third parties
	Processing of personal data for purposes other than stated at the stage of data collection
	Illegal processing of personal data of minors
	Processing of personal data in information systems containing personal data of more than 20000 data subjects
	Collection of personal data, including via the Internet, performed with the use of foreign software and services

In other cases, companies are exempt from planned state audits. At the same time, Roskomnadzor can make a preventive visit to an organization, regardless of its degree of risk.

According to the court practice, monitoring compliance with localization requirements in relation to collection of personal data in the Internet is not regarded as a measure of state control. Thus, the moratorium also does not restrict Roskomnadzor to request information from data controllers on their compliance with localization requirements when collecting personal data in the Internet.

There are also expected regulatory changes which provide:

- Roskomnadzor's power to initiate proceedings for certain violations of personal data processing without conducting control measures in relation to data controller[2];
- the possibility of Roskomnadzor's unscheduled inspections in 2023 in case of leaks of databases with personal data[3].

Updated list of countries with adequate personal data protection

Roskomnadzor updated the list of countries with adequate personal data protection for the purposes of cross-border data transfer. The new list will come into force on March 1, 2023.

Now the list includes both the list of countries that are party to **Convention 108** and the list of countries considered as adequate that are not party to Convention 108.

Earlier, the list of countries that are not parties to Convention 108 consisted of 29 jurisdictions. Now it has been expanded by the regulator to 34 jurisdictions. China, India, Thailand, Cote d'Ivoire and the Kyrgyz Republic are recognized as "adequate countries" for the purposes of cross-border transfer of personal data.

[2] The Bill No. 181342-7 "On Amendments to the Code of Administrative Offences of the Russian Federation".
[3] Draft Government Decree "On Amendments to Certain Acts of the Government of the Russian Federation".

Below is a complete list of countries that provide adequate personal data protection:

Transfer to such countries can be carried out immediately after the filing of a **notification** on cross-border data transfer to Roskomnadzor

"Adequate" jurisdictions - countries party to Convention 108:

- Austria
- Argentina
- Bosnia and Herzegovina
- Burkina Faso
- Luxembourg
- Hungary
- Uruguay
- Greece
- Georgia
- Ireland
- Italy
- Andorra
- Liechtenstein
- Monaco
- Belgium
- Malta
- Moldova
- Poland
- San Marino
- Northern Macedonia
- Senegal
- Serbia
- Slovenia
- Croatia
- Romania
- Slovakia
- United Kingdom
- Tunisia
- Turkey
- Ukraine
- Germany
- Finland
- France
- Montenegro
- Czech Republic
- Switzerland
- Estonia

"Adequate" jurisdictions – countries not being party to Convention 108:

- Australia
- Gabon
- Israel
- Qatar
- Canada
- Kyrgyzstan
- China
- Thailand
- Malaysia
- Mongolia
- Bangladesh
- New Zealand
- Angola
- Belarus
- Benin
- Zambia
- India
- Kazakhstan
- Costa Rica
- South Korea
- Ivory Coast
- Mali
- Niger
- Peru
- Singapore
- Tajikistan
- Uzbekistan
- Chad
- Vietnam
- Togo
- Brazil
- Nigeria
- South Africa
- Japan

Transfers to countries that are not included in the list of "adequate" jurisdictions above (e.g., the U.S., Chile, etc.) can be carried out after the 10-day period for Roskomnadzor to consider a **notification** on cross-border data transfer has expired.

Thus, if you plan to transfer data after March 1, 2023, you should assess your risks and take preparations now, especially if the transfers involve jurisdictions such as the United States.

Approved requirements for the assessment of harm that may be caused to personal data subjects

Data controllers shall perform an assessment of the harm that may be caused to personal data subjects in case of a violation of personal data legislation.

The requirements defined by Roskomnadzor for such an assessment will come into force on March 1, 2023[4].

Damage assessment is carried out by a DPO or a special commission appointed by a data controller. The results of harm assessment shall be formalized by a harm assessment act.

A data controller, as part of a harm assessment, determines one of the degrees of harm that may be caused to the subject of personal data in case of violation of personal data legislation, as listed below:

<table>
<tr><th>High harm</th><th>Medium harm</th><th>Low harm</th></tr>
<tr><td>Processing of biometric personal data
(except for cases provided by law)</td><td>Dissemination of personal data
(except for cases provided by law)</td><td rowspan="3">Maintenance of publicly accessible sources of personal data, formed in accordance with the legislation on personal data</td></tr>
<tr><td>Processing of sensitive personal data
(except for cases provided by law)</td><td>Processing of personal data for additional purposes other than the original purpose</td></tr>
<tr><td>Processing of personal data of minors for conclusion and/or performance of contracts (except for cases provided by law)</td><td>Direct marketing using databases owned by another data controllers</td></tr>
<tr><td>Anonymization of personal data
(except for processing for statistical or other research purposes)</td><td>Obtaining a data subject consent in the Internet via functionality of a website which does not involve further identification and/or authentication of the data subject</td><td rowspan="3">Appointment as a DPO of a person who is not a full-time employee of the company (i.e. "external DPO")</td></tr>
<tr><td>Assignment of processing to a foreign data processor</td><td rowspan="2">Processing of personal data which involves obtaining consent containing a provision on the right to carry out the processing to a certain or indefinite number of persons for incompatible purposes</td></tr>
<tr><td>Collection of personal data using databases located outside Russia</td></tr>
</table>

New forms of notifications on personal data processing

Roskomnadzor has adopted new notification forms[5]:

- On the intention to process personal data;
- On changes in a previously submitted notification on the intention to process personal data;
- On termination of personal data processing.

When submitting a notification on the intention to process personal data, a data controller shall determine and provide for each purpose:

- Legal basis;
- Category of data subjects;
- Categories of processed personal data;
- Types and means of processing.

[4] Order of Roskomnadzor of 27.10.2022 № 178 "On approval of the Requirements for the assessment of harm that may be caused to personal data subjects in case of violations of the Federal Law" On Personal Data".
[5] Order of Roskomnadzor of October 28, 2022 № 180 "On approval of forms of notices of intent to process personal data, on changes in information contained in the notice of intent to process personal data, on the termination of the processing of personal data".

As before, a data controller shall also provide information on implemented data security measures; information about the presence/absence of cross-border transfer; location of a database with personal data; and contact information of a DPO.

In the case of termination of processing, a notification must specify the reason for termination (e.g. liquidation of the organization, revocation of the license, expiration of the processing period).

The new forms must be used if a respective notification is to be filed after December 26, 2022. If a notification was filed before that date, there is no need to resubmit the new forms.

Requirements for destruction of personal data

Personal data legislation does not establish specific methods or methodology for the destruction of personal data, and a data controller on its own determines such a procedure, including by establishing it in internal documents.

Requirements on confirmation of data destruction approved by Roskomnadzor will come into effect on March 1, 2023[6].

The Regulator establishes requirements for the form and content of documents confirming the destruction of personal data.

The destruction of personal data, depending on the method of processing of such personal data, will be confirmed by the following documents:

- In case of non-automated processing of personal data - an act of destruction of personal data;
- In case of automated processing of personal data / "mixed" processing of personal data - an act of destruction of personal data and an extract from the logbook of events in the information system of personal data.

Recommendations for compliance with the new regulation

Data controllers shall assess the compliance of their personal data processing processes with future regulatory requirements in the short terms, including:

- Analyze cross-border data flows to ensure compliance with cross-border data transfer rules, depending on the "adequacy" of the jurisdiction to which the data is to be transferred;
- Update internal documents to the new requirements for harm assessment and destruction of personal data.

We hope that the information provided herein will be useful for you. If any of your colleagues would also like to receive our newsletters, please let us know by sending us his/her email address in response to this message. If you would like to learn more about our Data protection and Cybersecurity practice, please let us know in reply to this email. We will be glad to provide you with our materials.

Note: Please be aware that all information provided in this letter was taken from open sources. Neither ALRUD Law Firm, nor the author of this letter, bear any liability for consequences of any decisions made in reliance upon this information.

[6] Order of Roskomnadzor of October 28, 2022 No. 179 "On approval of the requirements for confirmation of the destruction of personal data".

If you have any questions,
please, do not hesitate
to contact ALRUD Partner

Sincerely,
ALRUD Law Firm

Maria Ostashenko

Partner

Commercial, Intellectual Property, Data Protection and Cybersecurity

E: mostashenko@alrud.com