

BIRCH LEGAL

Legal alert

Roskomnadzor published requirements for assessment of data breach impact and data destruction

On 29 November 2022 as a follow-up to amendments introduced in July of 2022 to the Federal Law “On Personal Data” (the “**Personal Data Law**”), The Federal Service for Supervision of Communications, Information Technology and Mass Media (“**Roskomnadzor**”) published clarifications regarding:

1

requirements for the procedure for assessing the impact of a data breach (Order of Roskomnadzor dated 27 October 2022 No. 178 “On approval of the requirements for assessing the harm that may be caused to personal data subjects in case of violation of the Federal Law “On Personal Data”)

2

requirements for the procedure for confirming the fact of the destruction of personal data (Order of Roskomnadzor dated 28 October 2022 No. 179 “On approval of the requirements for confirming the destruction of personal data”)

The clarifications published and summarized below will come into effect **on 1 March 2023 and will be valid until 1 March 2029**.



Impact assessment of data breach

It shall be noted that in accordance with the amendments to the Personal Data Law adopted in July 2022, information on the assessment of a data breach’s impact and the harm caused by it must be reflected in the form of a notification of the fact of unlawful or accidental transfer of personal data that shall be sent to Roskomnadzor within 24 hours from the moment a security incident is detected.

In accordance with the clarifications of Roskomnadzor, the corresponding harm assessment:

- Must be carried out by the person responsible for the processing of personal data or by a specially formed commission.
- The degree of harm caused is assigned according to the assessment. The degree of harm is assessed differently depending on:
 - categories of subjects and the number of subjects whose data is processed
 - consistence and categories of personal data
 - list of actions with personal data (presence / absence of cross-border data transmission)
 - method of processing personal data
 - the number of third parties entrusted with the processing of personal data subjects' personal data
- There are only 3 categories of degrees of harm that can be caused as a result of violating the Personal Data Law, listed on the next page.

High

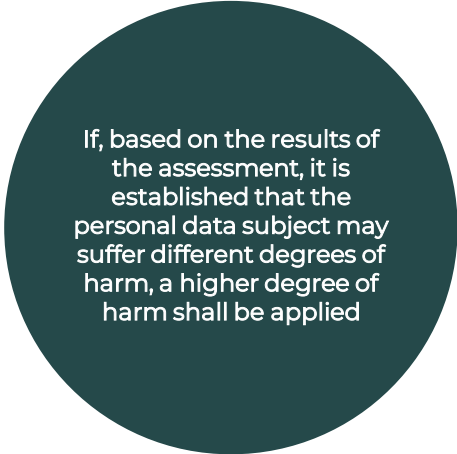
- processing biometric personal data used by the operator to identify the personal data subject
- processing special categories of personal data relating to race, nationality, political opinions, religious or philosophical beliefs, health status, private life, criminal record
- processing personal data of minors for the performance of an agreement to which a minor is a party or beneficiary or guarantor, as well as to conclude an agreement on the initiative of a minor or an agreement under which a minor will be a beneficiary or guarantor in cases not provided for by the legislation of the Russian Federation
- depersonalization of personal data, including for the purpose of conducting assessment (scoring) studies, providing services for predicting the behavior of consumers of goods and services, as well as other studies
- instructions to a foreign person (foreign persons) to process personal data of citizens of the Russian Federation
- collection of personal data using databases located outside the Russian Federation

Medium

- distribution of personal data on the official website of the operator, as well as the provision of personal data to an unlimited circle of persons
- processing personal data for additional purposes other than the original purpose of collection
- promotion of goods, works, services on the market by making direct contacts with a potential consumer using personal data bases owned by another operator
- obtaining consent to the processing of personal data through the implementation on the official website of functionality that does not entail further identification and (or) authentication of the personal data subject
- carrying out activities for the processing of personal data, which involves obtaining consent to the processing of personal data, containing provisions for granting the right to process personal data to a certain and (or) indefinite circle of persons for incompatible purposes

Low

- maintaining public sources of personal data, formed in accordance with Article 8 of the Personal Data Law
- appointing a person, who is not a full-time employee of the operator, as responsible for the processing of personal data



If, based on the results of the assessment, it is established that the personal data subject may suffer different degrees of harm, a higher degree of harm shall be applied

The results of the impact assessment are reflected in the **Impact Assessment Certificate**, which can be issued both as a paper and as an electronic document signed with an electronic signature containing the following mandatory elements:

- name or full name and address of the operator
- date of issue of the certificate
- the date of the impact assessment
- full name, position of the persons who conducted the impact assessment, as well as their signature
- degree of harm



Destruction of personal data

In accordance with the current Personal Data Law, the right to destroy data is one of the basic rights of the personal data subject (clause 1, article 14).

In addition, regardless of the request of the data subject, personal data is subject to destruction in the following cases:

detection of unlawful processing of personal data when it is impossible to ensure the legality of processing

achieving the purpose of processing personal data

In accordance with the clarifications of Roskomnadzor dated 29 November 2022, depending on the method used for processing personal data, confirmation of the destruction of personal data must be expressed:

1

in the form of the Destruction Certificate of personal data (if the processing is carried out without the use of automation tools)

2


in the form of the Destruction Certificate of personal data and uploading data from the event log to the personal data information system (if processing is carried out with the use of automation)

Destruction Certificate

- name (legal entity) or full name (individual) and address of the operator
- name (legal entity) or full name (individual), address of persons processing personal data of the personal data subject on behalf of the operator (if the processing was instructed to such a person)
- name of the subject or other information relating to a specific individual whose personal data was destroyed
- full names, positions of the persons who destroyed the personal data of the personal data subject, as well as their signatures
- list of categories of destroyed personal data
- the name of the destroyed physical carrier containing personal data with the indication of precise quantity of sheets in relation to each physical carrier (in the case of processing personal data without the use of automation)
- the name of the personal data information system from which personal data was destroyed (if processing personal data carried out without the use of automation)
- method of destruction of personal data
- the reason for the destruction of personal data
- date of destruction of personal data of the personal data subject

Uploaded data from the log file

- name of the subject or other information relating to a specific individual whose personal data was destroyed
- list of categories of destroyed personal data
- the name of the personal data information system from which the personal data of the personal data subject were destroyed
- the reason for the destruction of personal data
- date of destruction of personal data of the personal data subject



The Destruction Certificate and the uploaded data from the log are subject to storage for 3 years from the date of destruction of personal data

The requirements for the uploaded data are not strict. If the data system used by the operator does not allow all the information indicated above to be uploaded, the missing data may be additionally reflected in the Destruction Certificate.

The Destruction Certificate can be issued both as paper and as an electronic document signed with an electronic signature.

For further information please contact



Ksenia Petrovets
Senior Associate

M: +7 921 090 8942
ksenia.petrovets@birchlegal.ru



Anna Lapshina
Senior Associate

M: +7 964 771 4655
anna.lapshina@birchlegal.ru



Victor Mukhin
Associate

M: +7 921 747 5194
victor.mukhin@birchlegal.ru

Subscribe to our
Telegram channel



birchlegal.ru

© BIRCH LEGAL 2022. All rights reserved. BIRCH LEGAL LLC's Taxpayer Identification Number (INN) is 7703618107. The information provided in this legal alert may not be considered as professional advice or legal services and is not advice related to a specific situation. This information is intended for the general review of the users in relation to issues that may be of interest to them. BIRCH LEGAL is not liable for incomplete information.