

Newsletter

Fines for violations of personal data processing have been increased dramatically

December 19, 2024

Dear Ladies and Gentlemen!

We would like to draw your attention to the adoption of several significant pieces of legislation that are designed to enhance administrative liability and introduce new criminal offences in the context of personal data processing.

Increased fines for data breaches and failure to notify Roskomnadzor



On November 30, 2024, the President of the Russian Federation signed Federal Law No. 420-FZ, which tightens administrative liability for personal data breaches ("**420-FZ**").

Furthermore, the 420-FZ introduces additional administrative offences and increases fines for existing offences as set out in Article 13.11 of the Code of Administrative Offences of the Russian Federation ("**the CAO RF**").

Offence	Fine amount for legal entities and individual entrepreneurs ¹ , RUB
New offences of Article 13.11 of the CAO RF	
Action (inaction) resulting in unlawful transfer (provision, distribution, or access) of personal data (" data breach ") <i>Parts 12-14 of Article 13.11 of the CAO RF</i>	
<ul style="list-style-type: none"> from 1,000 to 10,000 personal data subjects and/or from 10,000 to 100,000 identifiers² 	from 3 mln to 5 mln
<ul style="list-style-type: none"> from 10,000 to 100,000 personal data subjects and/or from 100,000 to 1,000,000 identifiers 	from 5 mln to 10 mln
<ul style="list-style-type: none"> more than 100,000 personal data subjects and/or more than 1,000,000 identifiers 	from 10 mln to 15 mln
Repeated data breach , if an individual has been held to account under Parts 12-15 or 16-18 of Article 13.11 of the CAO RF <i>Part 15 of Article 13.11 of the CAO RF</i>	from 1 to 3% of annual income, but no less than 20 mln and no more than 500 mln
Data breach of sensitive personal data <i>Part 16 of Article 13.11 of the CAO RF</i>	from 10 mln to 15 mln

¹ Please be advised that in accordance with Parts 1.1 and 8-18 of Article 13.11 of the CAO RF, **individual entrepreneurs are held liable as legal entities**. However, the elements of offences under Parts 10-18 of the CAO RF **do not extend liability to officials of non-governmental organizations**.

² An identifier is a unique designation of information about an individual contained in the controller's personal data information system and related to such person.

Offence	Fine amount for legal entities and individual entrepreneurs ¹ , RUB
Data breach of biometric personal data <i>Part 17 of Article 13.11 of the CAO RF</i>	<i>* regardless of the number of personal data subjects whose personal data was leaked</i> from 15 mln to 20 mln <i>* regardless of the number of personal data subjects whose personal data was leaked</i>
Repeated data breach of sensitive personal data or biometric personal data , if an individual has been held liable under Parts 12-18 <i>Part 18 of Article 13.11 of the CAO RF</i>	from 1 to 3% of annual income, but no less than 25 mln and no more than 500 mln
Failure to notify and/or late notification of Roskomnadzor about data breach <i>Part 11 of Article 13.11 of the CAO RF</i>	from 1 mln to 3 mln
Failure to notify and/or late notification of Roskomnadzor about the intention to process personal data <i>Part 10 of Article 13.11 of the CAO RF</i>	from 100,000 to 300,000
New fines under Article 13.11 of the CAO RF	
Unlawful personal data processing / personal data processing incompatible with the purposes of its collection <i>Part 1 of Article 13.11 of the CAO RF</i>	from 150,000 to 300,000 <u>Repeated offence:</u> from 300,000 to 500,000

Mitigating and aggravating circumstances for repeated data breaches under Parts 15 and 18 of Article 13.11 of the CAO RF

Mitigating and aggravating circumstances are separately fixed for repeated data breaches in the specified offences.

Mitigating circumstances

The possibility of reducing an administrative fine below the lower threshold for these offences is introduced. The fine will be calculated as a percentage of gross revenue/company's funds, up to 0.1% of gross revenue/company's funds, but not less than 15 and not more than 50 million rubles. The following conditions must be met **simultaneously**:

- (A) The annual expenditure on information security measures over a three-year period equates to a minimum of 0.1% of gross revenue/company's funds.
 It is also important that contractors **involved in the project** must possess the appropriate license for TPCI³ or a license for MCPI⁴. If the appropriate licenses are available, implementation of these measures by the controller is possible independently. However, a license is not required for the purpose of maintenance of the MCPI for their own needs.
- (B) Conducting an audit to confirm compliance with data protection requirements for

³ FSTEC license for the technical protection of confidential information in accordance with clause 1, part 1, article 12 of the Federal Law "On Licensing of Certain Types of Activities".

⁴ FSS license for the provision of services in the field of cryptographic information protection in accordance with clause 5, part 1, article 12 of the Federal Law "On Licensing of Certain Types of Activities".

processing in information systems within 12 months prior to the data breach.

In practice, this will require companies to conduct annual audits of their personal data information system ("information system").

- (C) The absence of aggravating circumstances as set out in Parts 15 and 18 of Article 13.11 of the CAO RF.

In addition, other offences in the field of personal data, including "primary" breaches, will be subject to general mitigating circumstances. Furthermore, should the circumstances permit, companies may request that the court impose a fine below the minimum amount or issue a warning instead of a fine.



In the meantime, we cannot rule out the possibility of courts considering the aforementioned circumstances when determining whether to reduce liability, both for "primary" breaches and for other offences under Article 13.11 of the CAO RF. Over time, such circumstances may become a standard of good faith for the companies.

Aggravating circumstances

The following circumstances will serve to burden liability for such offences:

- (A) Continuation of a wrongful activity despite a formal request from a state authority to cease such an activity.

The 420-FZ does not clarify what constitutes a continuation of a wrongful activity in the event of personal data breaches. It may be assumed that this means the continuation of a wrongful transfer or failure to take measures to eliminate the causes of breach and prevent consequences. However, the latter actions are not formally qualifying for offences under Parts 15 and Part 18 of Article 13.11 of the CAO RF.

- (B) An individual that
 - has already been held liable under Parts 1-11 of Article 13.11 and/or Article 13.6, Article 13.12 of the CAO RF, and
 - at the time of rendering the decision on breaches, the individual is considered to have been subjected to administrative punishment for past offences (Article 4.6 of the CAO RF).

Cancellation of "discounts"

Please note that the previously valid discount of 50% for the payment of a fine for an offence under Article 13.11 of the CAO RF, identified during state or municipal control, is no longer applicable.

Consequently, for any offences under Article 13.11 of the CAO RF, legal entities will be required to pay the full amount of an imposed fine.

Change of jurisdiction for Article 13.11 of the CAO RF

The jurisdiction of the offences under Article 13.11 of the CAO RF will be attributed to arbitration courts. Please note that previously, these cases were considered by magistrates.

The change of venue is a positive development for companies, as the specialization of judges in Arbitrazh courts is more aligned with the needs of business, and such courts are better equipped to handle the specific details of the cases they consider.

Other developments

Furthermore, the 420-FZ introduces new offences related to violations of biometric personal data processing in the Unified Biometric System ("UBS") and other information systems:

Offence	Fine amount, RUB
Failure to comply with the established procedure for processing biometric personal data in the UBS and other information systems <i>Part 2 of Article 13.11³ of the CAO RF</i>	Officials – from 100,000 to 300,000 Legal entities – from 500,000 to 1 mln

Offence	Fine amount, RUB
<p>The failure to implement organizational and technical measures to ensure the security of biometric personal data in the UBS and other information systems.</p> <p><i>Part 3 of Article 13.11³ of the CAO RF</i></p>	<p>Officials – from 300,000 to 500,000</p> <p>Legal entities – from 1 mln to 1.5 mln</p>
<p>Processing of biometric personal data without accreditation</p> <p><i>Part 4 of Article 13.11³ of the CAO RF</i></p>	<p>Officials – from 500,000 to 1 mln</p> <p>Legal entities – from 1 mln to 2 mln</p>
<p>The refusal to conclude, execute, amend or terminate a contract with a consumer in connection with the consumer's refusal to undergo identification and/or authentication using the consumer's biometric personal data</p> <p><i>Article 14.8 of the CAO RF</i></p>	<p>Officials – from 50,000 to 100,000</p> <p>Legal entities – from 200,000 to 500,000</p>

Furthermore, a general limitation has been set for **credit institutions** regarding the amount of administrative penalties in accordance with the CAO RF. This amount of penalties **must not exceed 3%** of the credit institution's funds.

Entry into force

The amendments to the CAO RF will enter into force **on May 30, 2025** – 180 days after the official publication of the 420-FZ.

Criminal liability for unlawful personal data trafficking and data breaches



On November 30, 2024, the President of the Russian Federation also signed Federal Law No. 421-FZ, which introduces new criminal offences in the Russian Criminal Code ("the CC RF") relating to the illicit trafficking of personal data and the unauthorized disclosure of such data ("**421-FZ**"):

Examples of offences under Article 272.1 of the CC RF⁵ Punishment

Unlawful use and/or transfer (provision, distribution, or access), collection and/or storage of computer information containing personal data obtained through unlawful access to the means of its processing or storage, other interference in its functioning, or by other unlawful means⁶

Part 1 of Article 272.1 of the CC RF

- fine of up to 300,000 RUB or in the amount of other income for the period up to 1 year
 - or compulsory labour for up to 4 years
 - imprisonment for up to 4 years
- If it involves **the cross-border transfer** of personal data or **cross-border movement of personal data carrier**⁷:
- imprisonment for up to 8 years + fine of up to 2 mln RUB / in the amount of other income for the period up to 3 years + deprivation of the right to hold certain positions / engage in certain activities for up to 4 years

⁵ The processing of personal data by individuals exclusively for personal and family needs is not subject to the provisions set out in Article 272.1 of the CC RF.

⁶ In certain cases, stricter liability is imposed, such as in cases where these criminal acts are perpetrated using sensitive categories of personal data, biometric personal data, or personal data of minors.

⁷ The cross-border movement of personal data carrier is defined as the importation to the territory of the Russian Federation and/or exportation from the territory of the Russian Federation of machine-readable carrier (including magnetic and electronic) on which information is recorded and stored.

The creation and/or maintenance of an information resource (on the Internet, an information system or software) for the purpose of facilitating the deliberate storage, transfer (distribution, provision, access) of computer information obtained illegally.

Part 6 of Article 272.1 of the CC RF






fine of up to 700,000 RUB or in the amount of other income for the period up to 2 years with deprivation of the right to hold certain positions / engage in certain activities +

- or compulsory labour for up to 5 years; or
- imprisonment for up to 5 years

The amendments to the CC RF entered into force on December 11, 2024 – 10 days after the official publication of the 421-FZ.

Recommendations for compliance with the new regulation

The data controllers have 6 months to assess the current compliance of personal data processing and prepare for changes, in particular:

-  • The objective is to **audit the processes of processing personal data, paying close attention to their information system**, and to implement the necessary measures in the field of information security. It is essential to document the audit results and develop a plan for conducting annual audits of information system. Furthermore, regular training sessions for employees on working with personal data must be conducted and documented.
-  • It is not too late to develop and implement **an internal procedure for responding to personal data breaches** in the company (taking into account the requirements for notifying Roskomnadzor of such incidents and informing the subjects as well). In the event of a breach, one shall apply these measures, which may then be held as **a circumstance mitigating**
-  • It is important to review contracts and agreements with third-party organisations involved in the processing of personal data. This should include both controllers and processors. It is essential to ensure that the controller is aware of any personal data breaches and that the necessary information security measures are in place.
-  • The objective is to update **the local regulations** in the field of information security and to inform employees about them.
-  • Please notify Roskomnadzor of any processing of personal data that has not been previously disclosed
- Legalize the ongoing **cross-border transfer of personal data**.

We hope that you will find the information provided herein useful. If any of your colleagues would also like to receive our newsletters, please kindly send them the [link](#) to the electronic subscription form. If you would like to learn more about our [Data Protection and Cybersecurity](#), please let us know by replying 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 based on analysis of the publicly available information as well as on our understanding and interpretation of the legislation and law enforcement practice. Neither ALRUD Law Firm nor authors of this letter bear any liability for consequences of any decisions made in reliance upon this information.

If you have any questions,
please contact ALRUD
Partner

Sincerely,
ALRUD Law Firm



Maria Ostashenko

Partner

Commercial, Intellectual Property, Data
Protection and Cybersecurity

E: mostashenko@alrud.com