ALRUD

Newsletter

Stricter liability for personal data processing

December 28, 2023

Dear Ladies and Gentlemen,

We would like to inform you about significant legislative initiatives that impose increased administrative liability for violations of personal data processing, as well as criminal liability for unlawful personal data trafficking and data breaches.

Increased fines for data breaches and failure to notify DPA

On 4 December 2023, a bill was submitted to the State Duma[1] which increases liability for personal data breaches.

The bill also proposes supplementing the Code of Administrative Offences of the Russian Federation (the "**CAO RF**") with other administrative offences and increasing the number of fines for administrative offences previously prescribed by the CAO RF:

Administrative offence	**Fines for legal entities[2]**	
Action (inaction) resulting in the unlawful transfer (provision, distribution, or access) of personal data ("**data breach**")	Number of personal data subjects and/or identifiers[3]	Fine amount
	• from 1,000 to 10,000 personal data subjects and/or • from 10,000 to 100,000 identifiers	from 3 mln to 5 mln RUB
	• 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 RUB
	• more than 100,000 personal data subjects and/or • more than 1,000,000 identifiers	from 10 mln to 15 mln RUB
	Repeated data breach: from 0.1% to 3% of annual income, but no less than 15 mln RUB and no more than 500 mln RUB	

[1] Bill No. 502104–8 "On Amending the CAO RF".

[2] Please note the bill stipulates that individual entrepreneurs are subject to administrative liability as legal entities for the new offences, as well as for data localization offences of the CAO RF. Meanwhile, it does not envisage liability for officials of non-governmental organizations.

[3] Subject to the number of personal data subjects whose data has been leaked and/or the number of the leaked unique information indicators about the individuals necessary to identify them ("**identifier**").

Administrative offence	Fines for legal entities[2]
Data breach of **sensitive personal data**[4]	from 10 mln to 15 mln RUB Repeated data breach: from 0.1% to 3% of annual income, but no less than 20 mln RUB and no more than 500 mln RUB
Failure to notify DPA ("**Roskomnadzor**") **about a data breach**	from 1 mln to 3 mln RUB
Failure to notify Roskomnadzor **about the intention to process personal data**	from 100,000 to 300,000 RUB
Unlawful personal data processing / personal data processing **inconsistent with the purposes of its collection**	from 150,000 to 300,000 RUB Repeated offence: from 300,000 to 500,000 RUB

As of now, the bill is pending consideration by the State Duma in the first reading. The text of the bill is expected to be further elaborated on by the second reading.

If passed, the amendments to the CAO RF would come into force within 30 days after its official publication.

Criminal liability for unlawful personal data trafficking and data breaches

A bill introducing new offences in the Criminal Code of the Russian Federation (the "**CC RF**") for crimes related to illegal personal data trafficking and data breaches has also been submitted to the State Duma[5]:

Offence[6]	Punishment
Article 272.1 of the CC RF Unlawful use and/or transfer, collection, 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 means[7]	• fine of up to 700,000 RUB • or forced labour for up to 4 years • or imprisonment for up to 4 years If the crime has caused grave consequences[8]: • fine of 3 mln RUB / other income for a period of up to 4 years + deprivation of the right to hold certain offices or engage in certain activities for up to 5 years

The bill also imposes criminal liability for the creation and/or operation of information resources,

[4] Regardless of the number of personal data subjects whose personal data was leaked and/or the number of identifiers leaked. Please also note that the bill does not impose liability for data breaches of biometric personal data.

[5] Bill No. 502113-8 "On Amending the CC RF".

[6] Personal data processing by individuals solely for personal and family needs does not fall within the scope of Article 272.1 of the CC RF.

[7] In separate cases, stricter liability is imposed, e.g., if the criminal acts are committed with the use of sensitive data and biometric personal data, involve cross-border transfer of unlawfully obtained computer information containing personal data or cross-border transfer of media containing such computer information.

[8] **Grave consequences** include, inter alia, the temporary suspension or disruption of data controller's activity, disruption of the integrity of information systems with personal data, or distribution of computer information containing personal data to an unlimited number of third parties.

information systems, or software that aim to unlawfully store or transfer computer information containing personal data.

As of now, the bill is pending consideration by the State Duma in the first reading.

Violations of biometric personal data processing and collection of written consent

The Russian Parliament has passed the law[9] imposing administrative liability for violations of the placement of biometric personal data in the Unified Biometric System ("**UBS**").

In addition, the law significantly increases the number of administrative fines for personal data processing without the written consent required by law.

Offence	Fine amount for legal entities
Article 13.11.3 of the CAO RF Placement and updating of biometric personal data in the UBS by banks, multifunctional centres, and other organizations in violation of the requirements specified by law	from 500,000 to 1 mln RUB
Article 13.11 (2 – 2.1) of the CAO RF Personal data processing without written consent in cases where it is collected by law	from 300,000 to 700,000 RUB Repeated offence: from 1 mln to 1.5 mln RUB

Provisions of the law will come into force on 23 December 2023.

Recommendations for compliance with future regulations

Data controllers should already be evaluating the compliance of personal data processing processes with the future regulatory requirements, namely:

- Conduct an internal audit of personal data processing processes and implement the measures needed to ensure compliance with the requirements of the laws on personal data and information security

- Develop and introduce an internal procedure for responding to personal data breaches at the company, taking into account the requirements of notifying Roskomnadzor about such data breaches

- Revise contracts/agreements with third-party organizations involved in personal data processing to ensure that there is an obligation to notify the data controller about data breaches, as well as an obligation to comply with certain information security standards

- Update corporate documents concerning information security and inform employees about them

- File a notification with Roskomnadzor about personal data processing, if not done before
- Revise written consent templates and, if necessary, update templates and ensure the collection of the necessary written consentsfrom data subjects

[9] Federal Law of 12.12.2023 No. 589-FZ "On Amending the Code of the Russian Federation on Administrative Offences"

We hope that you will find the information provided herein useful. If any of your colleagues would also like to receive our newsletters, please 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.

NB: Please note that all information was taken from open sources. Neither ALRUD, nor the author of this letter, is responsible for any consequences that arise as a result of making decisions based on this letter.

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