STONEBRIDGE LEGAL

STRICTER PENALTIES FOR PERSONAL DATA BREACHES

3 December 2024

On 30 November 2024, the President of the Russian Federation signed draft laws No. 502113-8 (amendments to the Criminal Code of the Russian Federation – the ***RF CC***)[1] and No. 502104-8 (amendments to the Administrative Offences Code – the ***AOC***)[2], which were officially published on the same day. These documents, inter alia, toughen the liability of business and management for violation of personal data processing rules.

The amendments to the RF CC will come into force on 10 December 2024, while the amendments to the AOC will only come into force after the 180-day transition period is over (i.e., on 30 May 2025). Nevertheless, the amendments to the AOC are of particular interest to businesses as they significantly increase fines for personal data processing violations.

AMENDMENTS TO THE AOC

The draft law both introduces new offences and changes the liability for existing offences.

1. New fines

The fines have been increased significantly for "general" personal data processing offences (i.e., if processing in cases not provided for by the legislation or processing incompatible with the purposes of personal data collection – part 1 and 1.1 of Article 13.11 of the AOC). Below is a comparative analysis of these amendments.

Article 13.11 of the AOC	Description	Actual fine (RUB)	New fine (RUB)
Part 1 (initial violation)	Officials	from 10,000 to 20,000	from 50,000 to 100,000
	Legal entities	from 60,000 to 100,000	from 150,000 to 300,000
Part 1.1 (repeated violation)	Officials	from 20,000 to 50,000	from 100,000 to 200,000
	Legal entities	from 100,000 to 300,000	from 300,000 to 500,000

2. New elements of offence

The draft law introduces new elements of an offence, which can be divided into the following:

a. failure to notify the Federal Service for Supervision of Communications, Information Technology and the Media (***Roskomnadzor***);
b. actions related to *unauthorised personal data transfer* (*provision, distribution, access*) (***personal data leakage***); and
c. violating the procedure or rules for personal data processing.

[1] https://sozd.duma.gov.ru/bill/502113-8
[2] https://sozd.duma.gov.ru/bill/502104-8#bh_histras

We do not specify the fine amount for state or municipal bodies' representatives or non-profit organisations.

Violations for failure to notify Roskomnadzor

Article 13.11 of the AOC adds new offences as parts 10 and 11, which provide for penalties for failure to notify Roskomnadzor and notification at short notice:

- of the intention to process personal data; and
- of cases of unauthorised or accidental personal data leakage resulting in the infringement of personal data owners' rights.

The following fines are imposed on legal entities for these violations:

- from RUB 100,000 to RUB 300,000; or
- from RUB 1,000,000 to RUB 3,000,000, respectively.

Violations related to personal data leakages

New administrative penalties for personal data leakages and identifiers of individuals deserve special attention. The latter may include individual data such as numbers, or numerical, alphabetical or other unique designations of information about an individual. An operator's actions or omissions resulting in unauthorised personal data leakages will be considered an offence.

Depending on the volume and categories of illegally transferred data, fines for legal entities may reach **RUB 20 million**. In case of repeated violations related to data leakage, negotiable fines **of 1% to 3% of the personal data operator's annual revenue**, but **not less than RUB 20 million** and **not more than RUB 500 million** are envisaged.

However, a fine may be imposed below the minimum threshold only if the following conditions are simultaneously met:

- the legal entity has invested significantly into information security (not less than 0.1% of the aggregate annual revenue or lending institution equity for the previous 3 years);
- an additional requirement is that the operator itself has an appropriate licence in the field of encryption (cryptography) or technical protection of confidential information, or that the business engages a licensed organisation to ensure its information security;
- the legal entity has documentary proof of compliance with the legal requirements for personal data processing in its information systems over the previous 12 months; and
- there are no aggravations such as continued wrongdoing and/or repeated violations stipulated by parts 1–11 of Article 13.11 of the AOC (including new rules on failure to notify Roskomnadzor of personal data processing and/or leakage) and/or Articles 13.6 and 13.12 of the AOC (on violations of encryption use and information protection rules).

The reduced administrative penalty is also limited and amounts to 1/10 of the minimum administrative fine, but not less than RUB 15 million and not more than RUB 50 million.

Personal data processing offences

Companies which violate the procedure or technological rules for processing biometric personal data for the identification and authentication of individuals may be subject to fines of up to RUB 2 million. Managers of such companies may be fined up to RUB 1 million for the same violations.

Inter alia, a fine of up to RUB 500,000 may be imposed on a legal entity for refusing to conclude, execute, amend or terminate a contract with a consumer if it relates to the consumer's refusal to be identified or authenticated using his or her biometric data. A fine of up to RUB 100,000 may be imposed on a company's official for the same offence.

AMENDMENTS TO THE RF CC

The RF CC introduces a new Article 272.1 establishing liability for illegal actions with illegally obtained computer information containing personal data. In addition to the general rules, special corpus delicti with corresponding stricter penalties are provided for, such as:

- actions with regard to personal data of minors, special categories of biometric personal data;
- self-interested actions that cause major damage committed by a group of persons by prior conspiracy or with the use of official position;
- actions related to the transborder transfer of personal data or transborder movement of data carriers containing them; and
- actions that result in grave consequences or actions that were committed by an organised group.

A separate penalty exists for the creation, and/or ensuring the operation, of a resource designed to carry out illegal operations with personal data obtained illegally.

These offences may result in penalties of up to 10 years' imprisonment. The exception is when personal data is processed by individuals for personal or family needs.

OUR SUGGESTIONS AND RECOMMENDATIONS

- Despite the long period of discussion of the draft laws, their provisions may give rise to ambiguous interpretations by the authorities and business representatives. In particular, in order to issue fines below the minimum values, the methods of calculating the operator's investments (expenses) are ambiguous: it is required to take a weighted average of the annual cumulative revenue for the previous three-year period or to take into account the total cumulative revenue for all three years. There is also no unambiguous position as to what documents should confirm the fact of compliance with the legal requirements.

- We recommend starting preparation for an internal audit on information security and the proper processing of personal data in advance as it is advisable to conduct such an audit taking into account the new requirements that will come into force upon completion of the 180-day transition period. Taking into account the scope of changes introduced into the legislation, based on the audit results it will be necessary to update the existing local normative acts, policies, instructions and other documents on the processing and protection of personal data. In some cases it may be necessary to adjust technological business processes, as well as data management methods and techniques.

- In some cases it may be advisable to obtain licences in the field of encryption (cryptography) and technical protection of confidential information in order to reduce the risk of prosecution.

STONEBRIDGE LEGAL

T: +7 495 785 30 00
E: marketing@stonebridgelegal.ru

14/2 Kadashevskaya nab.
Moscow 119017 Russia