A law has been adopted establishing turnover-based fines for personal data leakages and increasing the existing fines for offences committed during personal data processing

FAO personal data operators

Pepeliaev Group advises of the publication, on 30 November 2024, of Federal Law No. 420-FZ "On amending the Code of Administrative Offences of the Russian Federation" dated 30 November 2024 (the "Law"). The Law will come into force on 30 May 2025.

The key amendments provided for in the Law: are

1. New administrative fines have been established for offences committed during the processing of personal data ("PD"):

- from **RUB 100,000** to **RUB 300,000** for the failure to notify Russian Federal Service for Supervision of Communications, Information Technology and the Mass Media (in Russian, abbreviated to "Roskomnadzor") of the intention to process PD;
- from **RUB 1,000,000** to **RUB 3,000,000** for the failure to notify Roskomnadzor of a leakage of PD;
- from **RUB 3,000,000** to **RUB 20,000,000** for a leakage of PD (in the case of a repeated leakage, turnover-based fines will be applied of 1% to 3% of turnover, but no less than RUB 20,000,000 million and no more than RUB 500,000,000 million);
- from **RUB 500,000** to **RUB 2,000,000** for violating the procedure for processing biometric PD in a common biometric system (CBS) or in another information system;
- for a refusal to enter into an agreement with the consumer in the event that he or she refuses to undergo the identification / authentication procedure with the use of his or her biometric PD from **RUB 200,000** to **RUB 500,000**.

2. Lists of extenuating and aggravating circumstances have been added that are taken into account when a punishment is imposed for a repeat leakage of PD.

3. Fines have been increased for PD being processed in situations that are not provided for in Russian legislation in the field of PD, or for PD being processed

in a manner that is incompatible with the purposes of collecting the PD – from **RUB 150,000** to **RUB 300,000** (for a repeat offence the fine is **RUB 500,000**).

Below are the current amounts of fines (with account being taken of the provisions of the Law) for offences committed during the processing of personal data:

Article of the Russian Code of Administrative Offences	**Elements of the offence**	**Amount of the fine for legal entities**
Breach of general requirements for the processing of PD		
Article 19.7	Failure to provide information to Roskomnadzor or not providing it on a timely basis, or providing incomplete or distorted information.	RUB 3,000 – 5,000
Article 13.11(3)	Failure to publish or otherwise ensure unrestricted access to a policy regarding the processing of PD, and to information about how the requirements for the security of PD are complied with.	RUB 30,000 – 60,000
Article 13.11(4)	Failure to comply with the obligation to provide to the data subject information relating to the processing of his or her PD.	RUB 40,000 – 80,000
Article 13.11(5) (a repeat offence is covered in article 13.11(5.1))	Failure to comply within the timeframes established in legislation with a demand of the subject, their representative or Roskomnadzor to update, block or destroy PD, if the PD is incomplete, obsolete, inaccurate, was received unlawfully or is not necessary for the declared purpose of processing.	RUB 50,000 – 90,000 Repeat offence: RUB 300,000 – 500,000
Article 13.11(6)	The failure of a person, while processing PD without using automated facilities, to fulfil the obligation to ensure that the conditions for safeguarding personal data stored on physical media and preventing any unauthorised access to such data, if such failure has resulted in unlawful or accidental access to	RUB 50,000 – 100,000

	personal data, or in such data being destroyed, altered, blocked, copied, provided, disseminated, or in any other unlawful actions with regard to PD.	
Article 13(11)(1) (a repeat offence is covered in article 13.11(1.1))	Processing PD in situations for which Russian legislation does not provide[1], or if such processing of PD is incompatible with the purposes for collecting the PD.	RUB 60,000 – 100,000 (**RUB 150,000 – RUB 300,000 from 30 May 2024**) Repeat offence: RUB 100,000 – RUB 300,000 (**RUB 300,000 – RUB 500,000 from 30 May 2024**)
Article 13.11(10) (comes into force from **30 May 2025**)	Failure to perform or late performance of the obligation to notify Roskomnazdor of the intention to process PD.	**RUB 100,000 – RUB 300,000 from 30 May 2024**
Article 13.11(2) (a repeat offence is covered in article 13.11(2.1))	Processing PD without a consent in writing in situations when such consent must be received in accordance with legislation or when PD is processed in breach of requirements established by legislation for the content of information included in the consent in writing.	RUB 300,000 – 700,000 Repeat offence: RUB 1,000,000 – 1,500,000
Article 13.11(8) (a repeat offence is covered in article 13.11(9))	Failure to perform, during the collection of PD[2], the obligation to ensure that PD of Russian nationals is recorded, systematised, accumulated, stored, adjusted (updated or modified) or extracted with the use of databases located in the Russian Federation.	RUB 1,000,000 – RUB 6,000,000 Repeat offence: RUB 6,000,000 – RUB 18,000,000

[1] For instance, processing of PD without a justification for such processing, which is provided for in article 6(1) of Federal Law No. 152-FZ dated 27 July 2006 "On personal data".
[2] Including by means of the Internet (in other words, with the help of the website of the company).

PD leakages		
Article 13.11(11) (comes into force from **30 May 2025**)	Failure to perform or late performance of the obligation to notify Roskomnazdor of a leakage of PD that has been identified.	**RUB 1,000,000 – RUB 3,000,000 from 30 May 2025**
Article 13.11(12) (comes into force from **30 May 2025**)	Actions (an omission) that have (has) resulted in a leakage of PD of 1,000 to 10,000 subjects[3] and/or of 10,000 to 100,000 identifiers[4].	**RUB 3,000,000 – RUB 5,000,000 from 30 May 2025**
Article 13.11(13) (comes into force from **30 May 2025**)	Actions (an omission) that have (has) resulted in a leakage of PD of 10,000 to 100,000 subjects and/or of 100,000 to 1,000,000 identifiers.	**RUB 5,000,000 – RUB 10,000,000 from 30 May 2025**
Article 13.11(14) (comes into force from **30 May 2025**)	Actions (an omission) that have (has) resulted in a leakage of PD of more than 100,000 subjects and/or of more than 1,000,000 identifiers.	**RUB 10,000,000 – RUB 15,000,000 from 30 May 2025**
Article 13.11(16) (comes into force from **30 May 2025**)	Actions (an omission) of the operator that have (has) resulted in a leakage of special categories of PD[5].	**RUB 10,000,000 – RUB 15,000,000 from 30 May 2025**
Article 13.11(17) (comes into force from **30 May 2025**)	Actions of the operator that have resulted in a leakage of biometric PD[6].	**RUB 15,000,000 – RUB 20,000,000 from 30 May 2025**
Article 13.11(15) (comes into force from **30 May 2025**)	Repeat leakage of PD.	**From 1% to 3% of the total amount of revenue per calendar year, but no less than RUB 20,000,000 and no more than RUB 500,000,000**

[3] In the event of a leakage of PD of less than 1,000 subjects (and less than 10,000 identifiers) the company may be held liable under article 13.11(1) of the Russian Code of Administrative Offences.
[4] An identifier is a unique mark of the information about an individual that is contained in the operator's information system and pertains to such individual.
[5] Special categories of PD include PD regarding racial and national identity, political views, religious or philosophical beliefs, state of health, intimate life and criminal record.
[6] Biometric PD means information that characterises physiological and biological features of a human being and allows for the person's identity to be established.

		starting from 30 May 2025
Article 13.11(18) (comes into force from **30 May 2025**)	Leakage of special categories of PD or of biometric PD, if such leakage is of a repeat nature.	**From 1% to 3% of the total amount of revenue per calendar year, but no less than RUB 25,000,000 and no more than RUB 500,000,000 starting from 30 May 2025**
Breach of requirements for the protection of PD		
Article 13.12(6)	Breach of requirements for the protection of information as established by federal laws and other items of legislation adopted in connection with them.	RUB 10,000 – RUB 15,000
Article 13.12(2)	Use of non-certified information systems, databases and data banks, as well as means of protection of information if they are subject to compulsory certification.	RUB 20,000 – RUB 25,000 + confiscation of uncertified means of protection of information
Article 13.6(1)	Use in communications networks of uncertified means of communication or uncertified coding (cryptographic) tools during the transfer of messages in the Internet if legislation provides for their compulsory certification.	RUB 60,000 – RUB 300,000 + confiscation of uncertified cryptographic tools
Breach of requirements for the protection of PD[7]		
Article 14.8(8) (comes into force from **30 May 2025**)	A refusal to enter / perform / amend / terminate a contract with a consumer if he or she refuses to undergo the identification and/or authentication procedure using his or her biometric PD	**RUB 200,000 – RUB 500,000 from 30 May 2025**
Article 13.11(3)	The publication and updating, in cases determined by federal laws, of biometric	RUB 500,000 – RUB 1,000,000

[7] Article 13.11.3 of the Code of Administrative Offences focuses on non-compliance with Federal Law No. 572-FZ dated 29 December 2022 "On identifying and/or authenticating individuals using biometric personal data, on amending certain legislative instruments of the Russian Federation and on repealing certain provisions of legislative instruments of the Russian Federation". In this situation biometric PD includes an image of an individual's face made with photo and video equipment and a voice recording made with sound recording equipment (pursuant to Resolution No. 408 of the Russian Government dated 1 April 2024).

(starting from **30 May 2025** this will be article 13.11.3(1))	PD in a CBS[8] with a breach of requirements established by legislation.	
Article 13.11.3(2) (comes into force from **30 May 2025**)	Breach of the procedure for processing biometric PD in the CBS, procedure for processing biometric PD, vectors of CBS in information systems of organisations that have undergone accreditation and perform authentication based on biometric PD of individuals or requirements for information technologies and technical means that are intended for the processing of biometric PD, vectors of the CBS with a view to performing identification and/or authentication.	**RUB 500,000 – RUB 1,000,000 from 30 May 2025**
Article 13.11.3(3) (comes into force from **30 May 2025**)	The failure to apply organisational and technical measures to ensure the safety of biometric PD when it is processed in a CBS, when the CBS interacts with other information systems or when organisational and technical measures are taken to ensure safety of biometric PD when it is processed in other information systems where authentication is performed with the use of individuals' PD.	**RUB 1,000,000 – RUB 1,500,000 from 30 May 2025**
Article 13.11.3(4) (comes into force from **30 May 2025**)	Processing of biometric PD, vectors of the CBS for the authentication of individuals in information systems of companies that do not have accreditation or whose accreditation has been suspended or terminated.	**RUB 1,000,000 – RUB 2,000,000 from 30 May 2025**

What to think about and what to do

1. Conduct an audit of PD processing procedures.

2. Determine the legal, organisational and technical measures that are necessary to safeguard PD from being accessed unlawfully or accidentally, from being destroyed, modified, blocked, copied, provided, or distributed as well as from other unlawful actions with respect to PD. Ensure that all necessary measures are taken.

[8] CBS means a common biometric system.

3. Develop a full set of local regulations governing the processing and protection of PD.

4. Develop the necessary forms of consents to the processing of PD, if written consents must be obtained.

5. Ensure that biometric PD and special categories of PD are processed in a proper manner.

6. Formalise orders for/agreements with third parties to have personal data processed.

For groups of companies: for each purpose of PD processing determine a specific operator of PD (a specific legal entity) and the full range of third parties inside the group to whom the PD is transferred and formalise the necessary documents.

7. Publish the PD Processing Policy and other documents on the company's website.

8. When collecting PD, ensure that PD of Russian nationals is recorded, systematised, accumulated, stored, adjusted (updated or modified) or extracted with the use of databases located in the Russian Federation.

9. Notify Roskomnadzor of the intention to process PD and of the intention to perform a cross-border transfer of PD.

10. Regularly hold training in the field of personal data for the company's employees as an efficient measure to prevent any data leakage.

Help from your adviser

The lawyers of Pepeliaev Group would be happy to provide comprehensive legal support to companies.

Pepeliaev Group provides the following types of services:

1. conducting an audit of PD processing;
2. devising a roadmap to bring a client's activity in line with the requirements of legislation on PD;
3. devising the full set of local regulations that govern the processing and protection of PD;
4. ensuring that PD of different categories of PD subjects (applicants, employees, former employees, clients, contracting parties) is processed lawfully;
5. selecting the optimal way to obtain consent to the processing of PD, including advising on methods of obtaining a data subject's written consent;
6. auditing the client's website in terms of whether it complies with the requirements of legislation on PD and drafting documents in the field of PD for the client's website;

7. advising on issues of personal data processing within the scope of interactions with third parties (including, drafting all necessary documents);
8. analysing information systems of PD that are used, advising on how to perform localisation requirements for databases;
9. drafting notifications to Roskomnadzor;
10. providing one-time consultations on any issues associated with the processing of personal data;
11. DPO - legal support on a subscription basis at favourable rates;
12. devising and holding training in the field of personal data for the client's employees;
13. providing support to clients in cases of leakages of personal data on a round-the-clock basis.

Contact details

Nikolay Solodovnikov
Partner

Tel.: +7 (495) 767 00 07
n.solodovnikov@pgplaw.ru

Polina Bardina
Head of Digital Group

Tel.: +7 (495) 767 00 07
p.bardina@pgplaw.ru

Nataliya Balekina
Associate

Tel.: +7 (495) 767 00 07
n.balekina@pgplaw.ru