ADVANT Beiten

Newsletter Russia

December 2024

Unprecedented increase in liability for personal data leaks

Русская версия

A law increasing administrative liability for personal data leaks was signed on 30 November 2024[1] (No. 420-FZ) (the "**Law**"). The Law will enter into force on **30 May 2025**.

A new article of the **Criminal Code of the Russian Federation** also enters into force on **11 December 2024**. It establishes liability for the illegal use and/or transfer, collection and/or storage of information on computers that contains personal data.

MAIN PARAMETERS OF THE ONSET OF THE NEW ADMINISTRATIVE LIABILITY FOR LEAKS:

- Applicable not only in instances when personal data entered the **public domain illegally**, but also when they were **transferred illegally to a limited number of persons**;

- Applicable only for the actions (inaction) of the data controller which led to the **illegal** transfer of the personal data. Consequently, liability is not established for the accidental transfer of personal data. At the same time, however, it is sometimes difficult to establish whether the transfer was illegal or accidental. For example, in instances when personal data were sent by mistake to another e-mail address, instead of the intended recipient;

- Fines are **differentiated** depending on the **amount** of the "leaked" data and on the specific data categories that were transferred illegally, as well as on whether respective fines **had been imposed previously**;

- As a general rule, administrative liability **is not imposed** on **the general directors** and other officials of private companies for personal data leaks (however, see the note *** in the table below);

- We present in the table below the specific sizes of the fines for companies, depending on the actual circumstances and respective explanations:

<table>
<tr><th></th><th>Regardless of the number of data subjects or identifiers**</th><th>1,000-10,000 data subjects and/or 10,000-100.000 identifiers</th><th>10,000-100,000 data subjects, 100,000-1,000,000 identifiers</th><th>>100,000 data subjects, >1,000,000 identifiers</th></tr>
<tr><td rowspan="2">"Ordinary" personal data</td><td>Initial: RUB 150,000-300,000 ***</td><td>(1) RUB 3-5 million</td><td>(1) RUB 5-10 million</td><td>(1) RUB 10-15 million</td></tr>
<tr><td>Repeat: RUB 300,000-500,000 ***</td><td>(2) 1-3% of annual revenue (but not <RUB 20 million and not >RUB 500 million)</td><td>(2) 1-3% of annual revenue (but not <RUB 20 million and not >RUB 500 million)</td><td>(2) 1-3% annual revenue (but not <RUB 20 million and not >RUB 500 million)</td></tr>
<tr><td rowspan="2">Special personal data categories (including medical data)</td><td>(1) RUB 10-15 million</td><td colspan="3" rowspan="2">* According to the position of Roskomnadzor (the Federal Service for Supervision of Communications, Information Technology and Mass Media), personal data are only considered to be biometric if the specific data are called biometric in a law or regulation.

** Identifier – unique designation of data on an individual in the information system (they may be</td></tr>
<tr><td>(2)**** 1-3% of annual revenue ***** (but not <RUB 25 million and not >RUB 500 million)</td></tr>
</table>

Biometric personal data*	(1) RUB 15-20 million	found, for example, in system logs). *** A fine may also be imposed on *officials* in the amount of RUB 50,000 to RUB 100,000 (initial offence) and from RUB 100,000 to RUB 200,000 (repeated offence). **** Hereinafter (2) implies the commission of an administrative offence by a person subjected to an administrative penalty for a leak (in other words, as a general rule, the commission of an offence in the period after the date of the entry into legal force of a previous judgment on the imposition of an administrative penalty until *one year* has expired since the date of the expiry of the execution of this judgment). ***** Hereinafter, in the case of a *credit institution* – 1-3% of internal funds.
	(2) 1-3% of annual revenue (but not <RUB 25 million and not >RUB 500 million)	

MANDATORY MEASURES TO TAKE IN ORDER TO MITIGATE LIABILITY

At the same time, the Law establishes three criteria which make it possible, if they are all met simultaneously, to reduce the turnover fine to 0.1% (but not <RUB 15 million and not >RUB 50 million) (these criteria must be performed prior to the issue of a respective court judgment):

1) **The costs** incurred on the performance by licensed[2] companies of measures aimed at ensuring **information security** equalled by the data controller, in the three calendar years prior to the identification of the offence, at least **0.1% of annual revenue**.

2) A company has to hand supporting documentation which confirms its compliance with the requirements on the protection of personal data during their processing in information systems. Such requirements are established, in particular, in Resolution No. 1119 of the Russian Government dated 1 November 2012 and include at the very least such measures as a) the organisation of a **security regime to protect the premises** where the information system is located, preventing the possibility of the uncontrolled penetration or presence in these premises of individuals who have no right of access to these premises; b) the **safeguarding** of personal data **media**; c) the approval by the director of the data controller of a document **listing the individuals** who require access to the personal data being processed in the information system in

order to perform their employment duties; d) the use of **information security tools** which have passed procedures introduced to assess their compliance with the requirements of Russian law on information security, *inter alia*, when the application of such tools is required to neutralise existing threats. An **audit report** on privacy matters could serve as a document which confirms compliance with requirements. In accordance with the Law, the audit should be conducted **at least once every 12 months**.

3) There are no **aggravating circumstances** such as (a) continuing unlawful behaviour, notwithstanding the demand of the competent authorities to cease and desist, or (b) fines imposed previously[3] on the company for a violation of Russian personal data legislation or information protection rules (including fines for the failure to notify Roskomnadzor of personal data processing).

If turnover fines are imposed, an aggravating circumstance would include, *inter alia*, an administrative offence in the form of the failure to notify Roskomnadzor of the leak (the initial notice on the leak must be e-mailed to Roskomnadzor within 24 hours of discovering of the incident). In addition, any failure to notify Roskomnadzor will now constitute a separate administrative offence – a respective fine of at least RUB 1 million is established for companies.

RECOMMENDATIONS

In light of the above, we recommend that companies-data controllers (including foreign companies doing business in Russia, *inter alia*, online) take the following steps, amongst others, **over the next six months**:

1) Russian companies or the representatives/branches of foreign companies should send, if they have not already done so, a **notice** on personal data processing to Roskomnadzor. The Law also establishes the imposition of fines on the company of up to RUB 300,000, if the data controller does not perform its obligation to send notices.

2) Conduct a mandatory personal data **audit** in order to identify and eliminate any possible instances of non-compliance.

3) Deliver mandatory **training** on the protection of personal data for employees, as the human factor remains one of the key reasons for leaks.

4) Sign personal data processing **assignments** (data controller-data processor agreements) according to the form established by the personal data law, first and foremost, with all cloud and other providers that have been ordered to process significant volumes of personal data or sensitive personal data categories.

5) Issue **powers of attorney** to authorised representatives for interaction with Roskomnadzor and courts in case of leaks.

We would be delighted to assist you with the performance of personal data audits, the delivery of respective training courses and the preparation of the necessary documents.

[1] Under the Russian personal data law, personal data leaks are understood to mean the illegal or accidental transfer of (the provision, dissemination of, granting of access to) personal data which led to the infringement of the rights of personal data subjects.

[2] A contractor or the data controller must have a licence authorising the development, production and dissemination of encryption (cryptographic) tools or authorising activity aimed at the technical protection of confidential information.

[3] When at the time of the commission of the offence (at the time when a court issued the respective judgment) a person is deemed to have been subjected to an administrative penalty (see the note **** in the table above).

Kind regards,

Andrey Slepov
Partner
Andrey.Slepov@advant-beiten.com

Imprint
This publication is issued by Beiten Burkhardt Rechtsanwaltsgesellschaft mbH
Ganghoferstrasse 33, 80339 Munich, Germany
Registered under HR B 155350 at the Regional Court Munich / VAT Reg. No.: DE811218811
For more information see:
www.advant-beiten.com/en/imprint