Personal Data Regulation in Russia: Roskomnadzor Update

2 April 2019

Two recent developments in Roskomnadzor's enforcement practice are of note to companies that need to interact with Roskomnadzor. First, in early 2019, Roskomnadzor[1] initiated proceedings against Twitter and Facebook for failure to comply with personal data localization requirements in respect of their Russian users. Second, in February 2019, changes were introduced to the way Roskomnadzor exercises control over personal data processing.

Debevoise & Plimpton

Facebook and Twitter. As of 1 September 2015, Russian Personal Data Law[2] requires operators of personal data to ensure that the recording, systematization, accumulation, storage, specification (updating, amendment) and extraction of personal data of Russian citizens are performed through databases located in Russia. Failure to comply may result in the personal data operator being included in the Register of Violators of the Rights of Personal Data Subjects (the "Register") and access to the website of such violator being blocked.

According to Roskomnadzor statistics, since this requirement came into effect, Roskomnadzor has conducted more than 3,000 scheduled audits and 200 unscheduled audits and more than 4,500 monitoring operations and has identified violations of the personal data localization requirement in not more than 1% of cases.[3] Roskomnadzor has audited companies, branches and representative offices registered in Russia, including subsidiaries of foreign companies[4] and foreign companies with no Russian presence but activities directed at Russia.[5] When auditing foreign companies, Roskomnadzor requested information on their compliance with the Russian personal data legislation.[6] Depending on the response and a confirmation of localization issued by

---

1 The Federal Service for Oversight of Communications, Information Technologies and Mass Media ("Roskomnadzor").

2 Federal Law No. 152-FZ on Personal Data dated 27 July 2006 (the "Personal Data Law").

3 https://rkn.gov.ru/news/rsoc/news49466.htm; https://rkn.gov.ru/plan-and-reports/reports/p449/.

4 For example, in early 2019, Roskomnadzor conducted an audit of Russian subsidiaries of Burger King, Proctor & Gamble and Apple that have databases in Russia.

5 The criteria for determining whether the activities are directed at Russia are available at https://digital.gov.ru/ru/personaldata/.

6 Pursuant to Article 23(3)(1) of the Personal Data Law.

the entity that, according to the operator's answer or Roskomnadzor's research, provides technical facilities for hosting databases of such foreign companies in Russia, Roskomnadzor either determined that there was no violation or brought legal proceedings.[7]

The most prominent example of a breach of localization requirements and its consequences was that of the professional social network LinkedIn. In 2016, LinkedIn was blocked in Russia after Roskomnadzor brought action against it for failure to comply with the localization requirements and to obtain required consents for personal data processing.[8] LinkedIn disputed that it was subject to Russian localization requirements.

Unlike LinkedIn, Twitter and Facebook were in regular communication with Roskomnadzor long before the latter commenced its audit in December 2018.[9] When the audit started, Roskomnadzor requested information on the status of personal data localization. Having received no confirmation of such localization or a plan for its implementation in Facebook's and Twitter's responses, Roskomnadzor initiated administrative proceedings against Twitter and Facebook for failure to provide adequate information in response to Roskomnadzor's requests.[10]

Notably, despite Twitter and Facebook not having localized the data in Russia for more than three years since this requirement became effective, Roskomnadzor did not seek to block them, as in the case of LinkedIn. Instead, Roskomnadzor initiated proceedings to hold the companies administratively liable. Such administrative liability can result in fines of RUB 3,000 to RUB 5,000 (approx. USD 45-80) for each instance of failure to provide adequate responses to Roskomnadzor's requests.[11] Though the fines do not prevent Roskomnadzor from blocking Twitter or Facebook in the event of continued noncompliance, so far there has not been any indication that Roskomnadzor intends to do so. The Head of Roskomnadzor, Alexander Zharov, stated that the Service is not contemplating blocking Facebook.[12]

The difference in Roskomnadzor's approach towards Facebook and Twitter and that towards LinkedIn may be driven by the former maintaining a dialogue with

---

7 *See The Action Plan Upon the Receipt of Information Regarding the Personal Data Operators in Foreign Jurisdictions*, available at https://rkn.gov.ru/news/rsoc/news34576.htm.

8 The details of the LinkedIn case are available here.

9 https://tass.ru/obschestvo/3852614.

10 Article 19.7 of the Administrative Offences Code of the Russian Federation.

11 The decision on whether the companies will be held liable on this ground must be issued by the magistrate judges within one month after accepting the case for hearing. Hearings on the Twitter and Facebook cases have been postponed twice and will be held on 5 April 2019.

12 https://www.interfax.ru/russia/642923.

Roskomnadzor, as well as the social and political impact if they were blocked in Russia, given the prevalence of Facebook and Twitter use.

New rules for conducting audits of personal data operators. On 23 February 2019, the amended rules for conducting audits of personal data operators by Roskomnadzor[13] came into effect. The amendments are aimed to extend Roskomnadzor's authority and increase the scrutiny of processing of personal data. Among other things, they include:

- **New grounds for conducting unscheduled audits**. Roskomnadzor may now conduct unscheduled audits of personal data operators upon approval of the public prosecutor:
  - based on the results of "control activities without direct contact with the operators" (i.e., monitoring of information posted by the operator on the Internet and in mass media and analysis of information provided by the operator or obtained by Roskomnadzor on its own); and
  - based on petitions of individuals about breaches of their rights by the personal data operator.

An unscheduled audit may also be conducted on the basis of previously existing grounds, such as upon the instruction of the President or government of Russia, upon a request of the public prosecutor or on the basis of failure to comply with Roskomnadzor's orders.

- **More scheduled audits for certain operators**. As before the amendments, scheduled audits generally are conducted every three years. But now Roskomnadzor also has the authority to audit the following operators every two years:
  - operators involved in cross-border transfer of personal data to jurisdictions that are viewed as not providing an adequate level of personal data protection (including the United States and China);
  - operators that process personal data on behalf of a foreign state, a foreign legal entity or an individual that is not registered in Russia;
  - operators that process personal data in the state information systems;

[13] Decree of the Government of the Russian Federation No. 146 on Approval of the Rules for Organizing and Exercising State Control and Oversight of Personal Data Processing dated 13 February 2019 (the "Rules").

- operators that collect biometric and certain other special types of personal data (e.g., that relating to race or ethnic origin, political views, health, criminal convictions, etc.).

- **Reduced time for conducting unscheduled audits**. Previously, the period for conducting scheduled and unscheduled audits was 20 days, with a possible extension for another 20 days. The amendments have reduced the period for conducting unscheduled audits to 10 days, with a possible extension for no more than 10 days. The period for conducting scheduled audits has not changed. As a result of this amendment, Roskomnadzor is likely to conduct audits more quickly, but it may require operators to provide voluminous information within a shorter period of time.

- **Remediation periods**. Roskomnadzor must now indicate in its compliance order a time period no longer than six months during which the personal data operator must remediate any breaches that were identified. No maximum remediation periods were previously specified, meaning that the companies will now have less time to implement the remediation steps that Roskomnadzor requires.

* * *

Please do not hesitate to contact us with any questions.

LONDON

Jane Shvets
jshvets@debevoise.com

MOSCOW

Anna V. Maximenko
avmaximenko@debevoise.com

Elena Klutchareva
emklutchareva@debevoise.com