LinkedIn blocking in Russia: first practical implementation of new data retention law

18.11.2016

Content:

LEGAL STRATEGY CLUB, LLC

P.O. Box, Russia, 105064
Moscow, Susalniy N, per.,
build 17-5

info@legalstr.com
www.legalstr.com

I. Case details

On November 10, 2016 the Moscow City Court (the court of second instance) confirmed the decision of the Tagansky district court (first instance) to block access to the website of LinkedIn on the territory of the Russian Federation.

Roskomnadzor (the country's telecom supervising body) brought charges against LinkedIn with regard to collection of personal data of unregistered Internet users in absence of their consent (article. 6 (1) of the Russian Law on Personal Data) and failure to store Russian users personal data within the country's territory (article18 (5) of the Law on Personal Data).

The legal ground for such charges and further blocking was failure of the company to comply with some provisions of the newly amended Russian laws "On information, information technologies and information protection", "On Telecommunications" and the Code of Administrative Offences (CAO).

According to new amendments to these laws, a company, which website is registered as an organizer of the dissemination of information, shall, store in the territory of the Russian Federation within six months all information containing data details of Russian citizens, as well as information about the facts of reception, transmission, delivery and (or) processing of voice information, written text, images, sounds, or other electronic messages of Internet users.

Practically these requirements mean that a foreign company which targets cooperation with Russian citizens and receives their personal data and details via internet communication, it must have physical servers and technical IT facilities in the territory of Russian Federation in order to keep the personal data inside the country. Moreover, if such company collects and/or receives data of website-unregistered Russian citizens it must make sure that it is happening with the consent of such users.

The case Roskomnadzor vs LinkedIn shows that the supervising body may practically target a broad number of companies over alleged data protection violations. It also become clear that from now on Roskomnadzor has surely included IP addresses information and dada processed by cookies as information falling under the broad definition of "personal data details".

II. Recommendations

Those foreign companies already cooperating or aiming to cooperate with Russian entities and citizens are recommended first of all to ensure that they comply with the data protection rules and to adapt their data protection and storage policies so that they would follow the Russian regulations. The next step could be considering a lease of servers and IT facilities in Russia, to ensure de facto storage of the date in the territory of the country.

Certainly implementation of such recommendations may cause some difficulties for foreign companies, especially given that the technical implementation of these recommendations is complicated and requires additional financing and adjustment of budgeting plans.

It could be that LinkedIn case becomes a singe case, before concretization of certain Russian data protection provisions. Indeed, if similar cases would be filed to court under the effective data protection regulations there would be a risk that all foreign companies targeting auditory in Russia, including such as Facebook, Microsoft, Apple, Visa, etc., would be forced to suspend their activity in Russian internet segment.

***