

Databases that are used to process personal data of Russian citizens must be physically located in Russia starting September 1, 2016

In July 2014 Russia enacted Federal Law No. 242-FZ which introduced new requirements for storage of personal data of Russian citizens (the "**Amendment**"). The Amendment will become effective September 1, 2016. The purpose of the Amendment is two-fold.

First, it amends Federal Law No. 152-FZ "On Personal Data" dated July 27, 2006 (the "**Personal Data Law**") by introducing new obligations with regard to the storage of Russian citizens' personal data.

Secondly, it amends Federal Law No. 149-FZ "On Information, Information Technology and Protection of Information" dated July 27, 2006 (the "**Information Law**") by introducing a mechanism for the regulator, i.e. the Federal Service for Supervision of Communications, Information Technology and Mass Media (the "**RKN**"), to block websites that process personal data of Russian citizens in violation of the Russian data protection laws.

Interestingly, the initial aim of the Amendment was to improve protection of privacy of Russian Internet-users. In particular, as follows from the explanatory note to the Amendment, which referred to Case C-131/12 adopted by the Court of Justice of the European Union on May 13, 2014 ('*right to be forgotten*'), the Amendment '*would introduce an opportunity for such users to demand IT-companies to delete their personal data published on third parties' websites from the web browsers' search results*'. However, the consequences of the Amendment appear to be more far-reaching than initially stated.

The Amendment addresses the obligations of "*personal data operators*" and "*information system operators*", which pursuant to the Personal Data Law and the Information Law may include foreign entities, public bodies or individuals that process personal data of Russian citizens. It should be noted that "personal data" under Russia law has an extremely broad definition:

personal data – any information relating to an individual who is directly or indirectly identified or identifiable (personal data owner).

Therefore new Russian data storage requirements on their face apply to all legal entities and individuals involved in the processing of personal data of Russian citizens, including foreign legal entities that are not represented in any way whatsoever within Russia.

There are no exemptions provided in the Amendment as to particular types of business of operators (e.g. tourism, transportation, e-commerce, banks, telecommunication, IT-companies etc.) or particular kinds of personal data i.e. ordinary (name, date of birth, address, sex etc.), sensitive (race, ethnic origin, views, state of health, private life) or biometric (fingerprints, eye or hair colour etc.).

Obligation to Use Russian Data Centers

Pursuant to the wording of the Amendment law, the operators will have to "*ensure recording, systematization, accumulation, storage, change and extraction of personal data of Russian citizens with the use of data centers located on the territory of the Russian Federation in the course of collecting personal data including via the Internet*". In other words, personal data of Russian citizens processed by operators must be stored in data centers located in Russia.

Operators are exempt from the above obligation, i.e. they are allowed to store personal data of Russian citizens in foreign data centers, if such processing is required:

- to achieve goals prescribed by an international treaty or other Russian laws and necessary for the operators to perform their functions, authorities and obligations imposed on them by Russian laws;
- for the administration of justice or enforcement proceedings;
- for the provision of public/municipal services by the Russian state and municipal authorities, local government authorities and entities; and
- to implement a journalist's professional activity and (or) the legitimate activities of the mass media or scientific, literary and creative activities.

Notice to the RKN

Generally operators must file notification with the RKN if they intend to process personal data subject to number of exceptions, e.g. processing of personal data of employees or of contracting party etc. This notification requirement has always been there and applied to wide range of commercial companies. However, it was generally not complied with by foreign companies which had no presence in Russia due to absence of effective monitoring and enforcement tools and effective sanctions for non-compliance. The Amendment, however, imposes an obligation on operators to notify the RKN on the exact location of data centers where Russian data is or will be stored.

Therefore, failure to give such notice to the RKN may constitute a breach of the Personal Data Law and entail administrative fines or, subject to a claim brought by Russian citizen, inclusion in the special register of violators and possibly result in blocking of the website concerned.

Cross-Border Transfer of Personal Data

In worst case scenario, new data storage requirements may be interpreted as prohibiting cross-border transfer of Russian citizens' personal data. However, the current Personal Data Law allows for such cross-border transfer provided that data is transferred, in particular, subject to an individual's consent.

Implementation of the new data storage requirements might work in the following way. Personal data of Russian citizens can be stored both (i) in Russia as a mandatory requirement and (ii) abroad, subject to duly obtained consent for cross-border transfer storage of a Russian citizen's personal data outside Russia.

Therefore, personal data would be duplicated in both Russian and foreign data centers. Nevertheless, it is difficult to predict how the new data storage requirements will be interpreted by the RKN and the courts.

Effective Date

Please note that the effective date of the Amendment has recently been proposed to be moved from September 1, 2016 to January 1, 2015. A draft law (No. 596277-6) was passed by the Russian Parliament (the “**State Duma**”) in two readings at the end of September, 2014. However, based on reports in Russian press in mid-October 2014, the third final reading has been postponed indefinitely and the proposed date change is likely to be rejected in full at this stage. Therefore, the effective date of the Amendment continues to be September 1, 2016.

Our Findings

In view of the above and based on our conservative analysis of current legislative developments in the area of personal data protection, we are of the view that:

- The Amendment applies to the foreign companies regardless of their presence in Russia;
- Beginning 1 September 2016, all affected companies must facilitate the storage of Russian citizens’ personal data in Russia via a proprietary or leased database;
- The companies processing Russian citizens’ personal data and not covered by the exceptions provided by law (see above), will have to give notice to the RKN on the processing of Russian citizens’ personal data, specifying the location of the database containing such data in Russia when the Amendment will come into force.
- Whether it would be possible to duplicate personal data in databases located outside Russia, subject to obtaining prior consent from a personal data owner, is unclear. Also, it is unclear how the Amendments will be interpreted and applied to cross-border transfers of data.

It should be noted that currently there is no official guidance as to how foreign companies should determine whether personal data belongs to a Russian citizen in case he does not indicate his citizenship. It is also unclear whether all personal data of Russian citizens, which has been previously duly transferred and is being kept on servers abroad would have to be relocated to data centers in Russia when the Amendment comes into effect.

Blocking Websites

As stated above, the Amendment introduces a mechanism, allowing the RKN to block websites. A Russian citizen may claim with a court to limit access to his personal data on a certain website that processes personal data in violation of the Personal Data Law. If the court determines that there was a violation the RKN could then request the “hosting provider” of the website concerned to stop processing personal data of the Russian citizen on the website. The provider would then have to demand the owner of the website to stop processing such data and if the owner fails to do so the provider would be required to restrict access to the website. If the provider fails to do that, the RKN will be entitled to order Russian telecommunications operators (internet connectivity providers) to restrict access to the entire website.

For these purposes, the RKN will maintain a special register of violators of the rights of personal data holders that will contain such information as domain names and web addresses containing disputed data, court ruling details and other relevant information.

Recent Information Published in Mass Media regarding Amendment

The Amendment has been the subject voluminous criticism because the Amendment will touch on a vast number of standard business practices (e.g. cloud technologies, remote access to data), making them illegal, and increase the cost of doing business. The business community has engaged in robust advocacy for amendments.

The Foreign Investment Advisory Council, the Russian-German Chamber of Commerce, Digital Europe Association, Information Industry Association of Japan and the Russian Association of Trades And Manufacturers of Consumer Electronic and Computer Equipment (RATEK), among others, are on the record with their comments.¹ It appears that their voices may yet be heard. Officials of the Russian Ministry of Communications and Mass Media, which oversees RKN, stated that the Amendment will need to be supplemented with detailed legislation.²

Squire Patton Boggs Moscow LLC

Disclaimer – This article may be used for information purposes only. This article is made available by Squire Patton Boggs only to provide general information and a general understanding of the Amendment as it stands on 17 November 2014, not to provide specific legal advice. It should not be used as a substitute for competent, up-to-date legal advice from a licensed professional attorney. In resolving a specific data protection issue, separate advice must be sought together with an investigation of all circumstances pertaining to the case in question and laws applicable to it.

If your organisation requires assistance with compliance planning or wishes to provide comments or recommendations on implementing regulations to the Ministry responsible for overseeing the new law, Squire Patton Boggs can offer advice and support on all legal, policy and public advocacy aspects.

Contacts

Irina Golovanova

Senior Associate, Moscow
T +7 495 258 5253
E irina.golovanova@squirepb.com

Alexey Pashinskiy

Associate, Moscow
T +7 495 258 5250
E alexey.pashinskiy@squirepb.com

1 ‘Kommersant’ newspaper No.193 dated October 23, 2014. Available in Russian on <http://www.kommersant.ru/doc/2595552>.

2 ‘RBCDaily’ newspaper, dated October 10, 2014. Available in Russian on: <http://www.rbcdaily.ru/politics/562949992598106>.