Client Update
Russia 2016: Personal Data & Cybersecurity

MOSCOW
Dmitry V. Nikiforov
dvnikiforov@debevoise.com

Anna V. Maximenko
avmaximenko@debevoise.com

Nikolay S. Kiselev
nskiselev@debevoise.com

Elena M. Klutchareva
emklutchareva@debevoise.com

2016 was a notable year in Russia for the extension of control over, and further clarification of, data localization requirements;[1] establishment of a strategy for the further development of personal data legislation and an increase in attention to cybersecurity issues.

PERSONAL DATA LOCALIZATION: FIRST OUTCOME

On September 1, 2016, the Federal Service for Oversight in the Sphere of Communications, Information Technologies and Mass Media of the Russian Federation ("Roskomnadzor") published the first results of the application of personal data localization requirements, which demonstrated the following:

- 161 Internet resources were included on the Register of Violators of the Rights of Personal Data Subjects (the "Register") and blocked; and
- amongst all of Roskomnadzor's inspections in the sphere of personal data, the violations of personal data localization requirements amounted to 1.3 percent (23 violations out of 1822).

A warning order by Roskomnadzor to rectify the violation was the main penalty for violation of the data localization requirements.

Certain companies have managed to remedy violations after the receipt of a warning order by Roskomnadzor.

[1] The data localization requirement was introduced by Federal Law No. 242-FZ on Amendments to Certain Legislative Acts of the Russian Federation with Regard to Specifying the Procedure for the Processing of Personal Data in Data Telecommunications Networks dated July 21, 2014 ("Law No. 242") and entered into force on September 1, 2015. It provides that recording, systematization, accumulation, storage, updating (renewal, amending) and extraction of personal data of Russian citizens can be done only through databases located in Russia ("personal data localization").

PERSONAL DATA LOCALIZATION: CLARIFICATIONS

On November 9, 2016, Roskomnadzor published commentary clarifying certain aspects of the personal data localization requirements. Although the commentary does not have a binding effect on personal data operators, Roskomnadzor may take the commentary into consideration during its inspections and when deciding whether a violation has occurred.

Restricting Access to Internet Resources Used for the Processing of Personal Data

Under the Personal Data Law,[2] access to Internet resources is restricted on the basis of a court decision. Thus, a personal data operator has an opportunity to provide evidence that it processes personal data in accordance with the requirements of the law.

The procedure restricting access to Internet resources can be initiated as a result of the following violations[3] of the Personal Data Law:

- personal data is accumulated in foreign databases;
- personal data is processed without their subject's consent;
- public access to publicly available personal data is provided in contradiction with the original scope and purposes of accumulation of such personal data; or
- a personal data operator fails to make its policy on the processing of personal data publicly available on the Internet.

Roskomnadzor uses publicly available WHOIS-service to determine an entity against which a claim restricting access is brought.[4]

Roskomnadzor noted that termination of operation of Internet resources does not qualify as a ground for its exclusion from the Register. An Internet resource can be excluded from the Register when the violation was cured or the court set aside the respective Roskomnadzor's decision on inclusion of an Internet resource on the Register.

---

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

[3] The list is not exhaustive.

[4] WHOIS allows for identification of the owner of a domain name. Identification through WHOIS of an entity violating the personal data localization requirements for the purpose of restricting access to Internet resources was held to be legal in several judgments of appellate courts and courts of cassation.

Clarification of Applicable Terms

Roskomnadzor explained the meaning of certain terms used in the Personal Data Law, including the following:

- "*database*" means any systematization of personal data, irrespective of their tangible media and processing facilities (e.g., archives, electronic databases, MS Word and MS Excel documents, etc.); transfer of personal data from paper documents to an electronic database is considered as a single process, which shall be effected in Russia (e.g., if a personal data operator accumulates personal data in paper documents in Russia and then transfers them to a foreign electronic database, the operator violates the Personal Data Law);
- "*collection of personal data*" means receipt of personal data directly from the subject of personal data; this term should be distinguished from the transfer of personal data for further processing;
- the law does not divide "*storage of personal data*" into permanent storage and temporary storage; use of such specifications in the personal data processing consent violates the law.

Cross-Border Transfer of Personal Data

The requirements on personal data localization do not impose any additional restrictions on cross-border transfer of personal data located in Russia. However, any update of personal data must be done in a database located in Russia first, and only afterwards can such data be transferred abroad. Parallel input of personal data in a Russian and a foreign database contradicts the Personal Data Law.

LINKEDIN CASE

In 2016, access to the LinkedIn[5] Websites[6] was restricted for persons using Russian IP addresses.[7] The decision to block the LinkedIn Websites was based, among other things, on the failure by LinkedIn to comply with the data localization requirements and to obtain the consent of the relevant citizens for the processing of their personal data by LinkedIn.

---

[5] LinkedIn Corporation ("LinkedIn").

[6] Access is restricted to the domain names, URLs and network addresses of the following websites: http://www.linkedin.com and http://linkedin.com (the "LinkedIn Websites").

[7] Based on the publicly available information, LinkedIn met with Roskomnadzor on December 8, 2016 in order to discuss Roskomnadzor's localization request, in particular, reasonable timing for localization. In January 2017, Apple and Google removed the LinkedIn application from their Russian application stores following a demand by Roskomnadzor.

To demonstrate the practicalities of the case, its details and background are set forth in Annex 1 to this update.

STRATEGY FOR PROTECTING RIGHTS OF PERSONAL DATA SUBJECTS

On March 31, 2016, Roskomnadzor adopted the Strategy for Institutional Development and Public Activities in Respect of the Protection of Rights of Personal Data Subjects to 2020 (the "Strategy"). The provisions of the Strategy are not binding, and their main goal is to set a roadmap for the future legislative and law enforcement activities of Roskomnadzor.

The Strategy promotes:

- self-regulation of the processing of personal data;
- consideration of industry specifics influencing the processing of personal data;
- increase of Roskomnadzor's public activity (e.g., joint projects with professional communities of personal data operators); and
- transparency of activities aimed at strengthening personal data protection.

Basic actions provided by the Strategy include, among other things:

- creation of incentives for compliance with personal data legislation and improvement of existing regulatory mechanisms (which is expected to result in a decrease in personal data violations by 30 percent); and
- improvement of law enforcement and methodological instruments (which is expected to result in an annual decrease in the number of identified violations by 2 percent).

BILLS ON SECURITY OF RUSSIAN CRITICAL INFORMATION INFRASTRUCTURE

On December 6, 2016, Bill No. 47571-7 on the Security of the Critical Information Infrastructure in the Russian Federation and the related Bills No. 47591-7 and No. 47579-7 amending certain legislative acts of the Russian Federation in accordance with Bill No. 47571-7 (the "Bills")[8] were submitted to the State Duma of the Russian Federation.

[8] For additional information on the Bills, please refer to: http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=47571-7&02, http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=47579-7&02, http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=47591-7&02.

The Bills establish basic principles for ensuring the security of Russian critical information infrastructure ("CII"),[9] and define the rights, duties and responsibilities of persons owning or otherwise legally holding CII facilities and telecom and information system operators supporting the interconnection of such facilities.

The Bills propose, among other things, the following:

- that a special register of significant CII facilities be created to ensure security of such CII facilities;
- that CII owners (including entities legally holding CII facilities) be required to report cyber incidents and assist the respective authorities in detecting and preventing cyberattacks, eliminating their consequences and determining the causes and circumstances contributing to such cyber incidents;
- that the criminal liability for improper interference with Russian CII (including creation and/or distribution of software or computer information deliberately designed for improper interference with Russian CII or unauthorized access to protected computer information stored in Russian CII) be set forth in Chapter 28 of the Criminal Code of the Russian Federation addressing cybercrime, with the maximum penalties, depending on the wrongdoing, being a criminal fine of up to RUB 2 million (approx. USD 33,333) or imprisonment for up to 10 years; and
- that the list of information classified as state secrets be amended to include information on the security measures in respect of CII facilities falling within one of the significance categories and information on the evaluation of the level of protection of Russian CII.

On January 27, 2017, the Russian State Duma passed the Bills in the first reading.

ACTIVITIES OF THE CENTRAL BANK OF RUSSIA

On April 11, 2016, the Central Bank of Russia issued Recommendations in the Sphere of Standardization for the Maintenance of Information Security of Institutions of the Banking System of the Russian Federation with regard to prevention of data leaks.

The document sets forth, among other things:

[9] According to Bill No. 47571-7, CII facilities include, among other things, networks, information and telecom systems of government bodies, and networks, information and telecom systems operating in the defense, healthcare, transport, banking spheres, energy, fuel, nuclear, mining, metallurgical, chemical, space-rocket industries.

- measures recommended for adoption in order to prevent possible leaks of confidential information and recommendations with regard to the implementation of such measures;
- recommendations for the maintenance of the necessary and adequate level of monitoring and control of possible leakage channels; and
- types of data recommended for inclusion in the category of confidential information.

Moreover, in 2016, the Central Bank of Russia put forward two significant initiatives:

- to develop remedial actions in respect of banks with low information security levels (specific measures to be specified); and
- starting from 2017, to evaluate and develop regulations addressing remote banking services (in particular, to run an overall security check of online banking services for individuals and remote payment services for legal entities, introduce certification of such remote services for compliance with information security requirements, lay down requirements for such remote banking services and adopt the above requirements as national standards).

Particular documents supporting these initiatives of the Central Bank of Russia are under development.

We anticipate further development in the sphere of personal data protection and localization, as well as some initiatives regarding cybersecurity issues by the Russian banking community.

* * *

Please do not hesitate to contact us with any questions.

ANNEX 1

LINKEDIN CASE

Roskomnadzor's Claim

On June 16, 2016, Roskomnadzor filed a lawsuit against LinkedIn in the Taganskiy District Court of Moscow claiming that the operations of the LinkedIn Websites on the collection, use and storage of personal data of Russian citizens were illegal. Roskomnadzor also moved to include the LinkedIn Websites on the Register.

Roskomnadzor used the following arguments:

- LinkedIn failed to localize the processing of personal data in Russia as required by the Personal Data Law,[10] which provides that as a general rule, when collecting personal data (including through the Internet), an operator of personal data must procure that the recording, systematization, accumulation, storage, updating and extraction of personal data of Russian citizens be performed through a database located in Russia;
- LinkedIn did not obtain the consent of particular individuals to process their personal data in violation of the Personal Data Law,[11] because by synchronizing with users' e-mails and devices, LinkedIn also collected and processed the data of individuals who were neither "members" nor "visitors" of the relevant websites and, in Roskomnadzor's view, were not covered by LinkedIn's User Agreement or other documents; and
- according to the information from the LinkedIn Websites, LinkedIn, located outside of Russia, is responsible for the services of the website "linkedin.com"; moreover, this legal entity is the administrator of the domain name of the website "linkedin.com", and therefore, this entity was considered as the defendant.

At that stage, LinkedIn neither participated in the court proceedings nor sent a defense.

On August 4, 2016, the Taganskiy District Court of Moscow, having taken into account that LinkedIn's activities on the organization of personal data collection were purposeful, issued a judgment against LinkedIn and declared that LinkedIn violated the Personal Data Law and the respective privacy rights of Russian citizens.

[10] Art. 18, par. 5 of the Personal Data Law.

[11] Art. 6, par. 1 of the Personal Data Law.

As a result, Roskomnadzor included the LinkedIn Websites in the Register and, consequently, access to the LinkedIn Websites was restricted.

LinkedIn's Appeal Against the Judgment

LinkedIn appealed the judgment of the Taganskiy District Court of Moscow to the Moscow City Court, and claimed, among other things, that:

- the Roskomnadzor lawsuit was brought against the wrong legal entity, since LinkedIn Ireland Unlimited Company is processing the personal data of individuals residing outside of the United States, and not LinkedIn Corporation;[12]
- the provisions of the Russian legislation were not applicable to foreign companies;
- there was no violation of the rights of personal data subjects, as the complaints of Russian citizens with respect to the LinkedIn Websites were not provided; and
- LinkedIn was not duly notified about the time and place of the hearing in the court of first instance.

On November 10, 2016, the Moscow City Court dismissed LinkedIn arguments and upheld the judgment of the Taganskiy District Court of Moscow.

Roskomnadzor's position supported by the Moscow City Court was based, in particular, on the following arguments:

- LinkedIn is the operator of personal data responsible for the compliance with the Personal Data Law:
  - according to the information from the LinkedIn Websites, LinkedIn is responsible for the services of the website "linkedin.com" and this legal entity is the administrator of the domain name of the website "linkedin.com";
  - the "linkedin.com" website is hosted on technical platforms located in the United States which are owned by LinkedIn; and

[12] Par. 1.2 of LinkedIn's User Agreement as of October 23, 2014 provides that if an individual resides outside of the United States, then the agreement is entered into by LinkedIn Ireland Unlimited Company and the respective individual (https://www.linkedin.com/legal/user-agreement?trk=hb_ft_userag).

- under the Personal Data Law,[13] an operator of personal data is also defined as a legal entity which, among other things, organizes and/or processes personal data in cooperation with other parties.

- the provisions of the Russian legislation are applicable to LinkedIn:
  - under the Information Protection Law,[14] the usage of information and telecom networks in Russia is subject to the requirements of Russian law;
  - under the Russian Civil Code,[15] the choice of law governing a contract may not deprive a consumer of the protection of their rights provided by the mandatory provisions of the law of the country of the consumer's place of residence if the other party to the contract (the professional party) in any way focuses its activities on the country of the consumer's place of residence; and
  - LinkedIn focused its activities on Russia because, in particular, (a) the LinkedIn Websites have a Russian version and provide for the placement of advertising in Russian, and (b) LinkedIn, being an entity engaged in business activities, understands that restricting access to the LinkedIn Websites in Russia will affect its interests.

As of the date of this client update, the LinkedIn Websites remain inaccessible in Russia.

[13] Art. 3, par. 2 of the Personal Data Law provides that an operator of personal data means a governmental body, municipal body, legal entity or individual that personally or jointly with other parties organizes and/or processes personal data and determines the purposes of personal data processing, the content of personal data to be processed and the actions (operations) involving personal data.

[14] Art. 15, par. 1 of Federal Law No. 149-FZ on Information, Information Technologies and Protection of Information dated July 27, 2006 (the "Information Protection Law").

[15] Art. 1212, par. 1 of the Civil Code of the Russian Federation (Part 3) No. 146-FZ dated November 26, 2001 (the "Russian Civil Code").