Morrison & Foerster Client Alert

September 28, 2015

The Russian Data Protection Authority, Roskomnadzor, Enforces New Russian Data Localization Law

By Marian Waldmann Agarwal

On September 9, 2015, the Federal Service for Supervision of Communications, Information Technology and Mass Communications (the "Roskomnadzor") reported on its website that it blocked an extensive online database of more than 1.5 million Russian citizens for violations of Russian Federal Law No. 242-FZ 2014, commonly known as the Data Localization Law. With the new Russian Data Localization Law having taken force only recently (September 1 2015), a question was how active the regulator would be with enforcing the law. While the Roskomnadzor announced that it will not be conducting compliance checks of technology companies such as Facebook, Google and Twitter before January 2016 at the earliest, it was unclear whether this would be the general approach. It is clear now that it was not and the Data Localization law is being enforced along with the Law on Personal Data as the Roskomnadzor works its way through its annual inspection plan. The blocked site that was the subject of this first enforcement action, http://abonenty-chast2.pw, reportedly contained personal information such as name, birth date, address, phone number and workplace and was hosted outside of Russia. The site also was placed on a register of violators of the Data Localization Law. No further details were provided by the Roskomnadzor on the action.

According to a statement released by the Roskomnadzor on September 2, the following multinational companies have already agreed to comply with the law's data localization requirements: Samsung, Lenovo Group Ltd., AliExpress, Booking.com, PayPal, eBay Inc., Uber Technologies Inc. and Citibank. The Roskomnadzor has also been engaging in discussions with Google, Facebook and Twitter. Russian newspaper Kommersant reported on September 10 that Russian data center IXcellerate was engaged by Booking.com to host their data on Russian citizens.

UNITED STATES

California

Tiffany Cheung	(415) 268-6848
Kimberly R. Gosling	(858) 314-5478
Rebekah Kaufman	(415) 268-6148
Christine E. Lyon	(650) 813-5770
David F. McDowell	(213) 892-5383
Purvi G. Patel	(213) 892-5296
Andrew Serwin	(858) 720-5134
Stephanie Sharron	(650) 813-4018
William L. Stern	(415) 268-7637
Nancy R. Thomas	(213) 892-5561
David M. Walsh	(213) 892-5262

New York

Cindy Abramson	(212) 336-4178
Melissa Crespo	(212) 336-4354
John F. Delaney	(212) 468-8040
Michael B. Miller	(212) 468-8009
Suhna N. Pierce	(212) 336-4150
Marian Waldmann Agarwal	(212) 336-4230
Miriam H. Wugmeister	(212) 506-7213

Washington, D.C.

L. Richard Fischer	(202) 887-1566
Adam J. Fleisher	(202) 887-8781
Libby J. Greismann	(202) 778-1607
Julie O'Neill	(202) 887-8764
Cynthia J. Rich	(202) 778-1652
Nathan David Taylor	(202) 778-1644

EUROPE

Berlin

Hanno Timner	49 30 72622-1346
Lokke Moerel	44 20 79204054

Brussels

Karin Retzer	32 2 340 7364
Sotirios Petrovas	(212) 336-4377
Alja Poler De Zwart	32 2 340 7360

London

Susan McLean	44 20 79204045
Alex van der Wolk	44 20 79204074

ASIA

Beijing

Paul D. McKenzie	86 10 5909 3366

Hong Kong

Gordon A. Milner	852 2585 0808

Singapore

Daniel P. Levison	65 6922 2041

Tokyo

Toshihiro So	81 3 3214 6568
Yukihiro Terazawa	81 3 3214 6585

THE DATA LOCALIZATION LAW

Enacted in July 2014, the Data Localization Law amends three existing laws, including Federal Law No. 152-FZ "On Personal Data" and requires that personal data on Russian citizens be stored in Russia. The law itself focuses on a few main provisions: storing personal data in Russia; notifying the Roskomnadzor of server locations; the Roskomnadzor's ability to block infringing websites; and the creation of a register of personal data rights violators and their violations.

Storing personal data in Russia

Personal data of Russian citizens must be stored in the territory of the Russian Federation. This applies to personal data in both electronic and paper form. Some non-business-related exemptions exist (e.g., processing for purposes required under the law or an international treaty, judicial purposes, processing by state authorities and mass media purposes).

For information collected in hard copy form, storing the original paper document in Russia will satisfy the law's requirements to maintain a local database, even if the paper is then scanned and transmitted outside of Russia. However, it would be a violation to remove all documentation from Russia, such as by sending the original papers to a vendor outside of Russia for storage with no originals in Russia.

Notifying the Roskomnadzor of server locations

All data operators who are subject to Roskomnadzor notification requirements under the Federal Law on Personal Data must notify the Roskomnadzor regarding the location of their personal data processing servers. This requirement does not apply to the processing activities that are exempt from registration under Article 22. A company is not required to register if, for example, the personal data belongs to employees or the company is only processing personal data on the basis of a direct agreement with an individual. Nor is a company required to register if the processing does not involve transfers to third parties without the individual's consent or if the data are used by the operator solely to perform the agreement. Therefore, if the collection and processing of personal data relates only to individuals who enter into a contractual relationship with the company (contractor, vendor etc.), and the relationship meets the other listed requirements, there may be no obligation to register with or notify Roscomnadzor.

Blocking infringing websites

Data operators found by a court to have violated Russian laws on processing personal data will have their websites blocked by the Roskomnadzor. The court procedure can be initiated either by an individual or the Roskomnadzor. Following the issuance of a court order, the Roskomnadzor will contact the respective hosting or communication service provider in order to block access to the infringing website. The Data Localization Law provides for a detailed "notice and take down" procedure, which based on draft regulations circulated earlier this summer, will be nearly identical to the Roskomnadzor's current notice and take down procedure used for copyright infringement and other violations. As noted above, Roscomnadzor already applied this procedure – in its first enforcement of the localization law on September 9 – to a website that was hosting personal data of a large number of Russian citizens abroad.

Violations register

Pursuant to the Data Localization Law, the Roskomnadzor will create a register of infringing websites with information about their violations. The register will be automated and operated by the Roskomnadzor or a sub-contracted entity. A website can be included in the register based on a court order.

PENALTIES FOR NON-COMPLIANCE

In addition to blocking the website and placement on the register, non-compliance with the data localization requirement could result in administrative penalties, civil penalties and damages and criminal sanctions. Administrative penalties are currently fairly low. The potential administrative fine is RUB 10,000 (USD 151) maximum for non-compliance with the personal data laws. In practice, we understand that the above fine has not been multiplied by the number of compromised data entries or specific violations, but rather applied once for the entire act of non-compliance. Still, it is possible under the law that each violation would qualify as a separate administrative offense and companies should not completely discount the risk that, in the future, the fine may be multiplied by the number of specific violations committed. Failure to notify may result in a separate administrative fine of RUB 5,000 (USD 76).

Furthermore, while the current maximum fines are very low, the Russian Parliament is currently discussing a draft amendment to the Russian Code of Administrative Offences that would increase the maximum fine to RUB 300,000 (USD 4,534). This amendment is expected to be adopted in the near future.

The Russian state magistrate courts responsible for deciding administrative fines also may issue an order to cure non-compliance with the law. Failure to comply with the magistrate court's order to cure may result in criminal liability for company executives.

The law also provides individuals whose personal data is not processed in compliance with the law with a private right of action for damages and compensation of moral harm. Generally, though, individuals prefer to file complaints with the Roscomnadzor or the Office of the Prosecutor because the Russian trial process is burdensome – it is incumbent on the individual to prove the damages (including moral harm) and the courts will not typically award the plaintiffs large sums of money. Once a complaint is reported, the Roscomnadzor can choose whether to inspect the data operator for compliance.

AUGUST 2015 MINKOMSVYAZ GUIDANCE

At the beginning of August 2015, the Ministry of Communications and Mass Media (Minkomsvyaz) issued guidance offering some clarity on the data localization requirements (available at http://minsvyaz.ru/ru/personaldata/#1438546984884). This guidance is technically non-binding; however, it does offer some insight into how the law will be enforced. One of the more noteworthy elements of the guidance is that it states that rules are targeted at processing by organizations engaged in Russian-oriented business (as opposed to any processing involving a Russian individual), and establishes some criteria for identifying which websites are likely to be covered by the rules. These include:

- the use of specific domain names such as .ru, .su and .moscow;
- the availability of the Russian-language version of a website;
- the presence of Russian-language ads; and
- the ability to carry out online transactions in Russian rubles.

The Minkomsvyaz guidance also addresses the following useful points relevant to multinationals:

- Personal information of Russian citizens collected before September 1, 2015, can remain in databases in foreign jurisdictions as long as the data remains unchanged. However, if these databases are updated and changed after September 1, 2015, then these databases become subject to the data localization requirements.

- The localization requirements will only apply to deliberate activities to collect information. For example, if a business makes the contact details of employees available to another business as a part of legitimate business activity, it will not be considered as personal data collection.

- The localization requirements will not apply to cross-border data transfers as long as personal data collection takes place in Russia (stored in primary databases), and personal data is then transferred to other jurisdictions (secondary databases).

- The Data Localization Law does not restrict remote access to databases in Russia. For example, according to the Minkomsvyaz, an employer will be able to transfer the personal data of employees to foreign jurisdictions as long as these transfers meet Russian data protection requirements.

The Data Localization Law does not restrict the disclosure of personal data by Russian citizens in order to use cross-border services rendered by foreign entities, such as online booking, banking services or the online order of goods. However, obtaining an individual's consent to process his or her personal data outside Russia will not provide data operators with legal grounds to carry out such processing. In other words, simple consent will not allow data operators to avoid localization requirements.

ROSKOMNADZOR ENFORCEMENT PLANS

The Roskomnadzor prepares and issues a plan for inspection each year that must be approved by the Office of the Prosecutor. The 2016 plan is expected to be approved in the final quarter of 2015 and will be available on the Roskomnadzor's website at: http://rkn.gov.ru/plan-and-reports/contolplan/. The annual plans are long and address compliance with the other areas that the Roskomnadzor is responsible for enforcing, such as telecommunications, mass media and broadcasting. Companies are listed by name on the plan, along with the company address, purpose of the audit, date of the company's registration and other relevant information. Apart from appearing on the plan, companies are only informed of an audit a few days before the Roskomnadzor intends to begin. Therefore, companies are advised to review the list on an annual basis to see if they are among the potentially targeted companies before the Roskomnadzor comes knocking. The Roscomnadzor will likely conduct inspections to review compliance with the Data Localization Law as it completes the remaining personal data inspections listed in its 2015 plan. The Roskomnadzor has also stated that inspections may be made in response to complaints received, and they may not be limited to the inspection plan.

Companies should prepare for possible inspections by maintaining documentary evidence of the location of their databases on Russian citizens. The head of the Roskomnadzor, Alexander Zharov, has stated in media interviews that the first inspections will be based on documents (e.g., requesting that a company produce agreements with a Russian data center or other documents proving the existence of a particular company's data center in Russia).

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law,*" or our free online Privacy Library, please visit our practice page and follow us on Twitter @MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.