ALSTON&BIRD

WWW.ALSTON.COM

Privacy & Security ADVISORY ■

JUNE 2, 2015

Russia's Tougher Rules on Data Collection Effective in September: U.S. Companies with Websites or Mobile Apps Targeted to Russia Beware

By Dominique R. Shelton, Evan Sippel-Feldman and David Caplan (Alston & Bird) and Anna Shashina (Bird & Bird LLP)

U.S. businesses with websites or mobile apps that collect personal information from Russian citizens will be subjected to new rules requiring companies to "first process" and store such personal information on servers in Russia on September 1, 2015. Accordingly, American businesses that are affected should begin the process of readying themselves for compliance. The current view is that Russian Federal Law No. 242-FZ (the "Russian Data Localization Law" or the "Localization Law") will apply to every foreign entity that targets Russian citizens, whether through a Russian language website directed at Russian nationals, or as an entity with regional headquarters in Russia. The effective date is September 1, 2015, and violators of the new law could see their websites shut down by Russian authorities. Applicable enforcement regulations, originally anticipated in March 2015, are still forthcoming.

If U.S. businesses do not have pre-existing servers on which to first process and store Russian citizens' personal data, they will need to either set up servers in Russia or contract with a third-party vendor to set up the necessary local servers in Russia. Businesses should consider recent guidance on vendor management from the Federal Trade Commission (FTC), National Institute of Standards & Technology (NIST), Securities and Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA), White House, Congress and the California attorney general to manage the risks of a data breach incident in connection with using a third-party vendor.

Compliance with the Russian Data Localization Law

Article 2 of the Russian Data Localization Law amends a previous Russian personal data statute (No. 152-FZ). The new Localization Law states:

> When collecting personal data, including via the Internet information and telecommunication network, the operator shall record, systematize, accumulate, store, specify (update, change) and retrieve personal data of citizens of the Russian Federation, using databases located in the Russian Federation....

Thus, the Russian Data Localization Law requires businesses collecting and storing Russians' personal information to first process the data in Russia and use databases physically situated in Russia to store the data.

The head of Roscomnadzor, Russia's data protection and enforcement agency (DPA), stated at a conference on November 5, 2014, that the Russian Data Localization Law would not prohibit the cross-border transfer of personal data.

Therefore, while the initial collection and processing of data must first occur in Russia, the data may subsequently be transferred out of the country to a duplicate database. Note however, the head of the DPA also stated that:

> …[T]he transfer of personal data into the territories which do not ensure **adequate** protection of personal data and do not fulfill the requirements of the Russian jurisdiction shall not be carried out without the consent of the personal data subject.

The DPA's statement reflects the current cross-border transfer provisions in the Russian personal data statute No. 152-FZ (*see* Article 12(4), covering Cross-Border Transfer of Personal Data). The U.S. is not considered to have adequate protection of personal data under the original Russian data protection law. Accordingly, U.S. companies will want to be sure to obtain written consent from the data subject before transferring data to a U.S. server, rely on an international agreement to which Russia is a party or transfer personal data to discharge an agreement to which a data subject is a party. Note that Russian law requires that the written consent provide the full name and passport data (number of passport, issue date, issuing authority) of a data subject, full name/company name of the data operator and its address, purposes of processing, scope of personal data which is subject to consent, full name/company name and address of the third-party processor (if any), scope of data processing operations and general description of the types of processing (automated, non-automated), term of the consent, procedure for revoking the consent and signature of the data subject. Alternatively, if U.S. companies have servers in other parts of the EU deemed to have adequate protections (e.g., France, Germany, Italy, the Netherlands, Ireland and other members of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No.: 108), they may consider maintaining duplicate databases there.

When the Russian Data Localization Law was enacted, there was some confusion whether it purported to cover the collection of Russian expatriates' personal information. However, unofficial statements made by the DPA clarified that the Localization Law will not apply to Russians living abroad.

The Russian Data Localization Law Applies to U.S. Companies Without a Corporate Presence in Russia

The DPA unofficially opined that the Russian Data Localization Law will apply to foreign companies (e.g., those based in the United States) which are targeting Russian data subjects—whether or not the companies have a branch or office in Russia. The Localization Law will apply to operators of websites translated into Russian, having a single webpage in Russian or having a .ru domain. The enforcement regulations have not yet been issued, so the full scope of the Localization Law as applied to foreign companies, like those in the U.S., remains as yet undefined.

On April 13, 2015, an online publication reported that at least two U.S. companies, a major Internet technology company and one of the largest e-commerce websites, plan to comply with the Localization Law and are moving some data storage facilities to Russia. Russian press reported that Bookings.com also announced that it will comply with the Localization Law.

Penalties for Noncompliance with the Russian Data Localization Law

The principal risk for U.S. companies for noncompliance with the Russian Data Localization Law lies in the risk of having their websites shut down. This can be particularly detrimental to e-commerce websites that rely on the use of websites or mobile apps in Russia. Noncompliance with the Localization Law could result in website access restrictions. After September 1, 2015, if a foreign business violates the Localization Law, the DPA may block its website or domain name. Procedurally, such access restrictions appear to require a court order following a complaint by a data subject. The DPA will create a public registry of the violators, and this appears to be a priority according to the DPA's April 20, 2015, press release.

If U.S. companies use local vendors located in Russia to first process and store Russian data, and that data is transferred to U.S. servers, care should be taken to ensure that the Russian vendors comply with best practices for security recognized in the U.S. For example, if vendors are cloud vendors, compliance with the new ISO 27018 cloud standard or other verification of security that is at least as stringent as that of the company should be explored with the vendor. Many of the mega-breaches featured in the recent U.S. press have originated through vulnerabilities exploited through inadequate vendor security.

While there are also possibilities for minimal fines under the Russian Data Localization Law, this risk seems inconsequential. Companies and officers who violate the Data Law may be fined, but currently, the maximum fine that may be imposed on a company amounts to only $200, and only $20 for an officer. There is an initiative to increase the maximum fine amount, and the draft law may be amended accordingly before it goes into effect.

Considerations for U.S. Businesses

U.S. businesses should explore whether consent is needed from data subjects before transferring data to a duplicate database in a country that is not considered to have adequate protections under Russian law—e.g., Japan, India, UAE.

U.S. businesses seeking to comply with Federal Law No. 242-FZ will likely require the support and services of vendors with data servers located in Russia. There are information technology vendors creating storage and processing solutions for non-Russian companies with the Russian Data Localization Law in mind. Engaging such vendors will invariably raise privacy and data security issues in light of recent high profile data breaches, enforcement actions and class action lawsuits. Companies hiring vendors working in Russia should assess those vendors' cybersecurity and privacy practices to ensure compliance with such laws, regulations and guidance as may be implicated. Various federal and state authorities have also recently provided guidance regarding vendor management.

Government-Recommended Best Practices

In February 2015, FINRA released its Report on Cybersecurity Practices. Though the report is directed at broker-dealers in the financial services industry, the report encapsulates the best practices that many U.S. regulators are calling for, including best practices concerning vendor management. The report highlighted such effective practices as implementing pre-contract due diligence, appropriate risk-based contractual terms (e.g., relating to confidentiality, data storage, breach notification responsibilities, right to audit, vendor employee access limitations and subcontractors), ongoing due diligence, risk assessment processes that account for vendor relationships, termination procedures related to vendor access and procedures for monitoring vendor entitlements. *See id*. at p. 26–30. The report included a case study on cloud computing and recommends that firms manage cloud service providers like other vendors, even though such services might be integrated more heavily within a firm's systems. *See id*. at p. 30.

Additionally, there are best practices that have been articulated by the FTC, President Obama, the United States Senate and the California attorney general in May 2014 that could apply to contractual commitments imposed on vendors handling information "reasonably linkable" to an individual. Such practices include contractually requiring vendors to ensure that data will be used only for purposes related to the vendor's agreement, e.g., not for its own marketing, and contractually requiring data brokers to offer a centralized website to enable consumers to access and correct information about themselves and to opt out of having some information included in certain marketing products.

Strengthening Vendor Contracts

Congressional scrutiny of vendor management issues has only increased recently, as many of the federal government's own vendors have been at the center of data breaches or fraud. On April 22, 2015, the House of Representatives Committee on Oversight and Government Reform, held a hearing on Enhancing Cybersecurity of Third-Party Contractors and Vendors. The committee discussed breaches at the Postal Service and Office of Personnel Management resulting from lapses by contractors and mirroring vendor management concerns in the private sector. Office of Personnel Management Chief Information Officer Donna K. Seymour discussed the importance of contracting clauses that strengthen relationships with vendors, such as implementing an initial security assessment validated by an independent assessment organization, continuous monitoring, requiring data segregation, encryption of sensitive information and a data breach incident response and notification plan.

The discussions in this hearing and the best practices reports provide a framework for U.S. companies seeking assistance from third-party information technology vendors. Such guidance will be particularly useful when engaging vendors to comply with the Russian Data Localization Law.

Contact Information

If you have any questions about the Russian Data Localization Law, please feel free to contact Dominique Shelton, David Caplan, Evan Sippel-Feldman, one of the attorneys in Alston & Bird's Privacy and Data Security Group, or Anna Shashina at Bird & Bird.

If you would like to receive future *Privacy & Security Advisories* electronically, please forward your contact information to **privacy.post@alston.com**. Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Members of Alston & Bird's Privacy & Security Group

Atlanta

Kacy McCaffrey Brake
kacy.brake@alston.com
404.881.4824

Kristine McAlister Brown
kristy.brown@alston.com
404.881.7584

Angela T. Burnette
angie.burnette@alston.com
404.881.7665

David Carpenter
david.carpenter@alston.com
404.881.7881

Lisa H. Cassilly
lisa.cassilly@alston.com
404.881.7945

Julia Dempewolf
julia.dempewolf@alston.com
404.881.7169

Maki DePalo
maki.depalo@alston.com
404.881.4280

Clare H. Draper, IV
clare.draper@alston.com
404.881.7191

Peter K. Floyd
peter.floyd@alston.com
404.881.4510

James A. Harvey
jim.harvey@alston.com
404.881.7328

John R. Hickman
john.hickman@alston.com
404.881.7885

William H. Jordan
bill.jordan@alston.com
404.881.7850
202.239.3494

David C. Keating
david.keating@alston.com
404.881.7355

W. Scott Kitchens
scott.kitchens@alston.com
404.881.4955

Dawnmarie R. Matlock
dawnmarie.matlock@alston.com
404.881.4253

Bruce Sarkisian
bruce.sarkisian@alston.com
404.881.4935

Peter Swire
peter.swire@alston.com
404.881.4259

Katherine M. Wallace
katherine.wallace@alston.com
404.881.4706

Michael R. Young
michael.young@alston.com
404.881.4288

Los Angeles

David Caplan
david.caplan@alston.com
213.576.2610

Kimberly K. Chemerinsky
kim.chemerinsky@alston.com
213.576.1079

Jonathan Gordon
jonathan.gordon@alston.com
213.576.1165

Katherine E. Hertel
kate.hertel@alston.com
213.576.2600

Sheila A. Shah
sheila.shah@alston.com
213.576.2510

Dominique R. Shelton
dominique.shelton@alston.com
213.576.1170

Evan Sippel-Feldman
evan.sippel-feldman@alston.com
213.576.1098

Washington, D.C.

Louis S. Dennig, IV
lou.dennig@alston.com
202.239.3215

Kimberly K. Peretti
kimberly.peretti@alston.com
202.239.3720

Eric A. Shimp
eric.shimp@alston.com
202.239.3409

Paula M. Stannard
paula.stannard@alston.com
202.239.3626

Jason R. Wool
jason.wool@alston.com
202.239.3809

Bird & Bird

Anna Shashina
anna.shashina@twobirds.com
+44 (0)20 7415 6000

ALSTON & BIRD