Russia's Proposed Data Localization Law: Digital Sovereignty is the New Black

By Natascha Gerlach* and Cecilia Álvarez Rigaudias**

July 8, 2015

Proposals to Balkanize data are not new, and the not-so-distant Snowden revelations did their part to bring them back to the forefront of global information policy debate.[1] Recent examples in Europe are discussions around a suspension of Safe Harbor,[2] suggestions for an EU Internet[3], an all-German internet (or "Internetz")[4], or a "Schengen for data."[5]

Russia joined the trend in 2014, announcing what is generally referred to as a "data localization law," due to take effect on September 1, 2015, and potentially creating far reaching consequences for entities operating in Russia or with Russian employees, customers, or suppliers.

1. History

In July 2014 the Russian Duma passed amendments to existing personal data protection[6] related laws requiring that personal data of Russian citizens, including data collected on the Internet, be processed in databases located within the Russian territory.[7] The key amendment, inserting Art. 18(5) into the existing legislation, states:

---

* Natascha Gerlach is Managing Attorney for EU Litigation Operations with Cleary Gottlieb Steen & Hamilton, currently based in their Brussels office. She oversees Cleary's European Practice Support Department, which supports the eDiscovery needs of all European offices. Natascha specializes in Data Protection issues in connection with cross-border discovery and advises on data security issues. She is a member of The Sedona Conference Working Group 6.

** Cecilia Álvarez Rigaudias is the European Privacy Officer Lead of the pharma multinational Pfizer. Cecilia is Vice-president of APEP (Spanish Privacy Professional Association), Spanish member of CEDPO (Confederation of European Data Protection Organisations) and member of the Steering Committee of The Sedona Conference Working Group 6.

1. For a comprehensive study of this phenomenon, *see* Anupam Chander and Uyen P. Le, *Data Nationalism*, 64 EMORY L. J. 677 (2015), *available at* http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf.

2. *EU Developments News Flash, April 1, 2015: Quo Vadis Safe Harbor*, https://thesedonaconference.org/wgs/wg6/announcements/2015/eu-news-flash-040115.

3. *Angela Merkel Backs EU Internet to Deter US Spying*, FINANCIAL TIMES, Feb. 16, 2014, http://www.ft.com/cms/s/0/dbf0081e-9704-11e3-809f-00144feab7de.html#axzz3fPGF1zpl.

4. Frank Dohmen and Gerald Traufetter, *Spy-Proofing: Deutsche Telekom Pushes for All-German Internet*, SPIEGEL ONLINE INTERNATIONAL, Nov. 12, 2013, http://www.spiegel.de/international/germany/deutsche-telekom-pushes-all-german-internet-safe-from-spying-a-933013.html.

5. *Breton: "créer une sorte de Schengen des données*," EUROPE 1, August 27 2013, http://www.europe1.fr/economie/breton-creer-une-sorte-de-schengen-des-donnees-1620759.

6. Federal Law No. 152-FZ on Personal Data dated July 27, 2006 and Federal Law No. 149-FZ on Information, Information Technologies and Protection of Information dated July 24, 2006.

7. Federal Law No. 242 on Introducing Amendments to Certain Legal Instruments of the Russian Federation Related to Personal Data Processing over Information and Telecommunications Networks dated July 21, 2014.

> When collecting personal data, including collection via Internet information and telecommunication network, an operator shall provide a record that the organization, accumulation, storage, update and retrieval of personal data of citizens of the Russian Federation is held on databases located within the Russian Federation.

An "operator" is an individual or entity who processes personal data and determines its purpose,[8] which would be a concept somewhat similar – but not equivalent – to the "data controller" under EU law. The definition of "personal data" under Russian law is equally broad as under European law, and the Russian courts as well as the regulators have provided some guidance on the subject. Note that the definition of "data processing" under the Russian data protection law is "gathering, recording, systematizing, storing, updating, using, transferring (including circulating, disclosing, providing access), de-identifying, blocking access to, or destroying personal data," which is not identical to the activities regulated under the data localization amendments.

Initially the amendments were to go into effect on September 1, 2016. Legislation was proposed in the Duma to move the date up to January 1, 2015, but this was generally seen as insufficient time for compliance, and the proposal stalled after a large scale lobbying campaign. On December 31, 2014, Russia's President Putin signed a law which moved the effective date of the amendments to September 1, 2015.[9]

2. Scope

The amendments are surrounded by a great deal of uncertainty and discussion regarding the scope of their applicability, and reports on possible interpretation are not always in agreement. There is no formal guidance yet, but Russia's data protection agency, the Federal Service for Supervision of Communications, Information Technology, and Mass Media ("Roskomnadzor"), is reported to have held a series of meetings with representatives of different industries, including internet companies, banks, and ticket resellers, which could give some insight into how the amendments might be interpreted.[10] Here are some preliminary take-aways.

- **The amendments apply to all data operators who are processing data of Russian citizens collected from Russian territory**

This interpretation would exclude the data of foreigners residing in Russia (Mr. Snowden's data would be exempt, for instance). However the law appears silent on how to make that determination and Roskomnadzor also seems to leave the means up to the individual operator, recommending

8. Art. 3 of Federal Law No. 152-FZ defines "operator" as a "state agency, municipal authority, legal entity or individual who organizes and/or processes personal data as well as determines the purposes and scope of personal data processing".

9. Federal Law No. 526-FZ.

10. Hogan Lovells, *Russia Data Localization Law Update and Webinar: New Details Emerge from Meetings with Russian Regulator*, April 2, 2015, http://www.hldataprotection.com/2015/03/articles/international-eu-privacy/russia-data-localization-law-update-and-webinar-new-details-emerge-from-meetings-with-russian-regulator/; *recording and accompanying slide deck available at* http://www.hldataprotection.com/2015/04/articles/international-eu-privacy/recording-and-deck-from-webinar-update-on-new-russia-data-localization-law/.

the IP address as an indicator when in doubt. This would extend the scope of the law significantly (potentially re-including Mr. Snowden's data, for instance, as a sort of collateral damage).

There remains a question mark behind the storage of data of Russian citizens who are not on Russian territory at the time of collection, but according to Roskomnadzor's informal, non-binding guidance, their data may be considered exempt.[11]

The amendments are also silent on the physical location of the operator, but it is assumed that they would apply to a company that resides outside of Russian territory, but collects personal data (directly) from Russian citizens[12] on Russian territory.[13] A few limited exceptions may apply, as reflected in Federal Law No. 152-FZ on Personal Data, for instance when data processing is carried out pursuant to international agreements to which Russia is a party ,[14] or necessary for enforcement actions, or incidental to journalistic, scientific, literary, or otherwise creative purposes.[15]

- **While it is not directly clear from the law, Roskomnadzor seems to suggest that the primary database for personal data of Russian citizens must be stored in Russia**

There has been extensive speculation on whether the new requirements dictate that the data in scope can be stored ONLY in Russia, or if, for instance, storing a mere copy in Russia would suffice.[16] While the transfer of data out of Russia has not been further restricted by the law, guidance suggests that the data stored in Russia has to be equal to, or more extensive than, the data stored outside of Russia and the primary processing (such as updating) should take place in Russian-based data centers.[17] The Russian database shall be primary and a foreign database could

---

11. Francoise Gilbert, *Russia Data Localization Law: an Enigma* (Apr. 6, 2015), http://www.francoisegilbert.com/2015/04/russia-data-localization-law-an-enigma/.

12. *Russia's Data Localization Law: New Interpretations of the Authorities*, NOERR NEWS DATA PROTECTION, June 2015, http://www.noerr.com/~/media/Noerr/PressAndPublications/News/2015/russland/2015-06-24%20Russian%20Data%20Localization.pdf ("The following are the interpretations given by the DPA during our meeting with them on 23 June 2015. Apart from the caveat that the DPA is not entitled to officially comment on the Law, they shared the following views which they also asked to bear in mind when considering ways to comply with the Law. […] Territorial Applicability of the Law: The Law will apply to any legal entities, including foreign ones, irrespective of whether they have actual presence in Russia or not. The criteria for the DPA would be whether a foreign entity targets its offers, goods and services at a Russian individual. For instance an offer to buy goods allowing Russian citizens to make purchases would be considered as such targeting and, thus, would trigger the applicability of the Law.").

13. Dmitry Kurochkin, Marat Agabalyan and Saglara Ildzhirinova, *Russia's New Server Localization Law: Implications for Foreign Companies*, BLOOMBERG BNA WORLD DATA PROTECTION REPORT, Feb. 2015, http://www.dechert.com/files/Uploads/Documents/Bloomberg%20-%20Russia%20New%20Server%20Localization%20Law%20-%20Dechert%20LLP%20-%20February%202015.pdf.

14. For example, the airline industry may be excluded, according to letter from the Ministry of Communication to the Association of European Business. The Ministry responded to a letter from the Russian Association of European Business on May 29, 2015 (with their standard caveat that they are not entitled to provide an official interpretation) that the Data Localization Law is not applicable to airlines as there are international treaties covering this topic.

15. *Supra* note 11.

16. *Supra* note 13.

17. *Supra* note 10.

be either a partial or a full copy of the Russian primary database.[18] Roskomnadzor also seems to include any type of structured data in the scope of the amendments, casting a wide net down to spreadsheets or even card files.[19]

- **Notification to Rokomnadzor of personal data processing must include the server location**[20]

All data operators which do not fall under the exemptions of article 22 of the Law (i.e. companies collecting only employee data or collecting data on the basis of a direct agreement with an individual without transfer to third parties) must notify Rokomnadzor of the location of servers with personal data.[21]

- **The amendments create "Registers of Offenders"**

The amendments affect the existing law "On Information, Information Technologies and Protection of Information" by creating so-called "registers of offenders"[22] for entities not in compliance. Roskomnadzor will be able to initiate the process and offenders may see their domain names entered into a register by court decision, and find themselves blocked from doing business on Russian territory.[23]

The amendments also added a limited form of a "Right to be Forgotten". The data subject would have the right to approach Roskomnadzor with a request to block access to data processed in violation of the law, based on a court order.[24]

The low monetary sanctions under the existing Russian data protection law remain in force,[25] however it is expected that new legislation will be implemented increasing the potential fine to a range of RUB 30,000 to 300,000. At current exchange rates, that translates into a range of €450/$520 to €4,500/$5,200.[26]

18. *Supra* note 12.

19. *Supra* note 11.

20. Section 22 of the Federal Law No. 526-FZ requires a general notification of the processing of personal data to the Roskomnadzor; the new law would add "information on the location of the database of information containing personal data of citizens of the Russian Federation" to the information to be reported.

21. *Supra* note 12.

22. Art. 1 of Federal Law No. 242, introducing Art. 15 (5) to Federal Law No. 149-FZ on Information, Information Technologies and Protection of Information.

23. *Important Changes to Russian Data Protection Rules*, DLA PIPER LEGAL ALERT, https://www.dlapiper.com/~/media/Files/Insights/Publications/2014/08/Important_changes_to_Russian_data_protection_rules.ashx (accessed July 9, 2015).

24. Art. 1 of Federal Law No. 242, introducing Art. 15 (5) to Federal Law No. 149-FZ on Information, Information Technologies and Protection of Information; Art 15 (5) No 6.

25. Current fines are very low, with a general maximum of RUB 10,000 (about €150 or US $175).

26. Draft Law No. 683952-6.

- **Cross border transfer has not been further restricted, it remains possible to transfer data into countries with adequate protection.**

The transfer of the personal data stored in Russia to third countries remains possible, provided that it is in compliance with the existing law[27] and the primary database is located in Russia.[28]

- **Retroactive effect**

The law is silent as to whether it addresses only data that is collected after September 1, 2015, or includes data that was collected previously and continues to be processed after September. According to comments attributed to Roskomnadzor, it would appear that "the Law will have no retroactive effect, thus, all databases with personal data created before 1 September 2015 can be still used after that date. However, any update of such databases can be performed after 1 September 2015 only with the use of a primary Russian database."[29]

3. Conclusion

The amendments to the data protection law in Russia leave many questions unanswered until more guidance is provided.

In any event, it is clear that it will create investment costs for companies currently active in Russian markets and those considering entry. Data storage in Russia is still expensive and it has been reported that tech giants such as Google and Microsoft have begun moving some resources out of Russia.[30]

In March of this year, the Russian Internet Ombudsman, Dmitry Marinichev, sent a letter to President Putin lobbying for foreign companies to be allowed to store data of Russian citizens outside of Russia, where consent was obtained.[31] The Ombudsman suggested application of the safe harbor rule for signatory countries to Convention 108,[32] currently in place for general data transfers under Russian law, for storing data outside of Russia.

Overall this development counteracts the very idea of cloud based services, and may restrict access by Russian citizens to some services. One can imagine innovation and development slowing down and prices increasing in Russia for services requiring personal data processing. And while the rhetoric has generally suggested that the amendments are aimed at protecting Russian citizens from what President Putin referred to as "the CIA project" (the idea that the CIA created the internet

27. In particular, Art. 12 of Federal Law No. 152-FZ on Personal Data.

28. *Supra* note 12.

29. *Supra* note 12.

30. Deniel Mero, *Is Google Headed Towards a Russian Exit?* FORBES, Feb. 20, 2015, http://www.forbes.com/sites/denielmero/2015/02/20/google-headed-russian-exit/.

31. *Russia: Internet Ombudsman Challenges Localisation Law*, DATA GUIDANCE PRIVACY THIS WEEK, Mar. 19, 2015, http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=3460.

32. COUNCIL OF EUROPE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (1981), available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

for their purposes),[33] one has to wonder whether the attempted localization of personal data may not have ulterior motives as well.[34]

33. Ewen MacAskill, *Putin Calls Internet a 'CIA Project' Renewing Fears of Web Breakup*, GUARDIAN, Apr. 24, 2014, http://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia.

34. *See supra* note 30; see also Christopher Kuner, et al., *Internet Balkanization Gathers Pace: Is Privacy the Real Driver?* 5 INT. DATA PRIVACY L. 1 (2015), *available at* http://idpl.oxfordjournals.org/content/5/1/1.