The risks of Russia's data localisation laws

Analysis of Russia's new data sovereignty law reveals concerns over the country's long term economic and political stability.

New Russian legislation requires foreign organisations to conduct all primary processing of customer and client data within Russia's territorial borders. Data may be transferred abroad under certain conditions, but many firms see this new legal and regulatory instrument as inimical to their commercial interests and are considering their options for continued operation in Russian markets. Russia is not alone in its new commitment to "data localisation", but it is unclear how this new directive serves its economic and political objectives.

Sovereign Data explores Russian data localisation policy and its implications for Russian economic growth and political stability.

Citation: "The risks of Russia's data localisation laws," *Sovereign Data* Vol. 1, No. 4 (October 2015).

Keywords: RUSSIA, DATA LOCALISATION, DATA PROTECTION, ROSKOMNADZOR
--
Explanation of dates:
Drafted: 2015-09-30
Information cut-off: 2015-09-25
Published: 2015-10-01

Personal data governance

Russia's new data localisation law amends and augments existing legislation which protects the collection and processing of Russian citizens' personal data — defined as any information that relates directly or indirectly to a physical person, although there is little specific guidance on what categories of data this includes. Federal Law No. 242-FZ, which came into effect on 1 September 2015, seeks to clarify the procedures for "personal data processing in information and telecommunications networks".[1]

The new law does not restrict the right or ability of foreign organisations to collect, structure or store the personal data of Russian citizens, nor does it affect their access to this data from abroad, but it does ban the "recording, systemisation, accumulation, storage, modification (updating, alteration) and retrieval of Russian citizens' personal data" using data processing services physically located outside Russia. This will not be retrospectively applied, and so data collected before 1 September 2015 can still be stored abroad. Any further data collected under these six categories must be stored within Russia itself.

This requirement puts the onus on foreign organisations doing business in Russia to comply with domestic data protection legislation regardless of where they are physically situated. Companies located in Russia, wholly or in part, will be subject to on-site audits of data processing. Those situated outside Russia but which target Russian users will be required to employ data processing services located within territorial Russia that can be more easily inspected. This means any foreign entity continuing to do business involving Russian citizens must have a physical base in Russia. The law therefore seeks to exclude unwilling organisations, whilst physically incorporating compliant companies within its sovereign territory.

Sanctions

The principal agent of the revised data protection regime is the state media regulator, Roskomnadzor, which has primary responsibility for data protection under the aegis of the Russian Ministry of Communications and Mass Media. Any party wishing to process the personal data of Russian citizens must inform Roskomnadzor of the location of the database in which this data resides, enabling

Sovereign Data is a journal of politics, data and risk in emerging markets.

Editor: Michael A. Innes
Author: Tim Stevens

ISSN: 2059-075X

For more information on the subject of this report, or to subscribe to our services, contact us at:

subscriptions@thesigers.com

"Thesigers" is a trading name of Thesiger & Company Limited.

Registered in England and Wales.
Registration number: 7234402.
VAT number: 135658985.

Office: 37 Great Russell Street, London, WC1B 3PP, England.

Phone (UK): +44 (0)134 430 6541
Email: enquiries@thesigers.com
Web: thesigers.com

© THESIGERS. All rights reserved.

both the identification of data infrastructures developed by foreign entities and the development of an inspection regime tailored to audit them. Non-compliant organisations will be added to a "Register of Violators of Personal Data Subjects' Rights" and may attract sanctions imposed by Roskomnadzor and the courts.

The principal proposed sanction is the blocking of foreign websites providing services to Russian consumers and clients. Roskomnadzor has extensive experience and capabilities in this field and is Russia's primary internet censor, backed by wide-ranging legislation which seeks to restrict internet content. Such tools can be easily applied to block the web assets of companies on Roskomnadzor's blacklist. These tools are imperfect and can be evaded by sophisticated internet users, however most foreign companies unable to operate legally in Russia would likely be unable to operate at all. Extensive technical infrastructure exists for comprehensive deep packet inspection (DPI) of internet traffic and the Russian government exercises control over internet "choke points".[2] The threats of website blocking are therefore neither idle nor hypothetical and may incentivise compliance with the data localisation law.

Interestingly, Russia has framed the new law with specific reference to European data protection legislation, particularly the controversial "right to be forgotten" provision of the European Union's Data Protection Directive. This concept has been part of European law since 1995, but a recent ruling reaffirms the right of the individual under certain conditions to request that their personal information be removed from the internet.[3] Russia's new data localisation law gives Russian citizens the ability to trigger "right to be forgotten" proceedings through the courts. As in Europe, the concern is that this instrument may be abused: instead of protecting citizens from unwarranted and undesired exposure, it may be deployed to promote and protect vested interests.[4]

Economics of data localisation

Data migration is costly and the prospect of transferring primary databases to Russia is unattractive to foreign companies. Some will bear those costs as the price of operating in Russian markets, but others are likely to leave.

There has been some confusion about the precise application and effects of the data localisation law. The Ministry of Communications published a non-binding commentary on the legislation in August 2015, only weeks before its implementation.[5] This clarified many issues of liability and exemption, notably that airlines would not be required to comply as this would breach international conventions on air travel and aviation security. The new law is generally respectful of Russia's international treaty obligations and international law, but the principal objection to data localisation remains commercial rather than normative.

Data migration is costly and the prospect of transferring primary databases to Russia is unattractive to foreign companies. Some will bear those costs as the price of operating in Russian markets, but others are likely to leave. Google, Facebook and Twitter—all of which have established offices in Russia—were disputing the time-frame for compliance until the eve of the law's implementation and seem to have elicited a stay of inspection until January 2016.[6] Big companies such as these have leverage in Moscow not available to smaller enterprises, but they have yet to make firm decisions on the future of their Russian operations. Like many others, they may elect to restructure in a manner that will affect the ability of Russian firms to capitalise on the global market in cloud services and IT support.[7]

Those seeking to comply with the law may find it cost-effective to contract with local partners rather than risk the costs of physical relocation. This presents opportunities for domestic data processing companies, a consideration surely not far from Russian government thinking and in keeping with its general drift towards import substitution.[8] This policy, partly fuelled by deteriorating relations with the US and its imposition of economic sanctions, would be a long term challenge for any country, let alone one with a problematic history of protectionism and economic stagnation. In August 2015, the Russian Duma took steps to approve an import substitution plan for software which may help to offset some of the losses caused by data localisation.[9] However, the European Centre for International Political Economy calculates that new data localisation requirements will cost Russia RUB 286 billion

(GBP 3.7 billion; USD 5.7 billion), a figure which allows for government subsidies and other positive effects on the domestic data processing market. For this reason, the decision has been described as a "self-imposed sanction".[10]

Outlook

What, if anything, does Russia stand to gain from data localisation? The first point to consider is that Russia is not alone in seeking to assert data sovereignty this way. In the last two years, at least twenty states have proposed data localisation, often as a means of protecting against foreign government intervention of the type revealed by Edward Snowden in 2013. Nor are global technology companies the victims: many sell data sovereignty as a service, particularly to curry market favour in places like Germany and Brazil, which reacted to the Snowden disclosures with data localisation proposals of their own.[11]

In the last two years, at least twenty countries have proposed data localisation, often as a means of protecting against foreign government intervention of the type revealed by Edward Snowden in 2013

Russian data localisation is tied up with Putin's accusations, inter alia, that the internet is a "CIA project".[12] As previously reported in *Sovereign Data*, whether he truly believes this, is less important than the role of data localisation as an expression of Russian discontent with perceived US internet hegemony.[13] The logical extension of the argument is to further demarcate the borders around the Russian internet and ensure they are patrolled diligently against external subversion. This is not necessarily an authoritarian reflex, but history suggests that "walling-up" the internet goes hand-in-glove with domestic surveillance and political control. This may serve short-term political ends but is unsustainable if Russia's economy is affected by growing insularity from global markets which are increasingly reliant on the relatively unfettered exchange of information.

Internet scholar Rebecca MacKinnon notes there is always friction where nation-state sovereignty and the "commercial sovereigns" of the internet interact.[14] With regard to Russia's new data localisation law, however, the risk is that it will be detrimental for all companies wishing to do business in Russia. Investors and researches will need to be mindful of whether this presents merely a "speed bump on the information superhighway", as the old internet cliché has it, or a more fundamental obstacle to Russian economic growth and political stability.

THESIGERS
Researchers • Rapporteurs • Pathfinders

HOW TO SUBSCRIBE
Sovereign Data is published monthly and distributed direct to subscribers via email as a PDF attachment. Subscribers to the Reporting Service benefit from daily, weekly and monthly reporting and analysis.

Thesigers defines "sovereign" and "data" broadly, in order to more fully understand the risks and opportunities associated with knowledge in all its tributary forms – "information", "data", "evidence", "intelligence", and so on.

Thesigers' view of sovereign data is that it contains essential elements of substance and form, of context and meaning – original, often perishable artefacts about people, places, events, issues and things.

Monthly Journal
Thesigers' monthly journal, *Sovereign Data*, provides short, digestible analysis of the state of the information environment. Each monthly issue focuses on a single, current topic selected by Thesigers staff, given additional context and assessed for relevance and impact.

Reporting Service
Thesigers' reporting service tracks current developments in sovereign data. Intended for clients who need more frequent, detailed updates, the service features summary reports and briefings based on locally-sourced news, data analytics, risk indexes and regular assessment.

Research and Development
Thesigers' conducts ongoing research and development through a sense-making program of workshops, system design and technology innovation. Workshops investigate problems covered in our reporting and analysis. Our systems and technology work creates working solutions to them.

For more information on the subject of this report, or to subscribe to our services, contact us directly at:

Email: subscriptions@thesigers.com
Phone (UK): +44 (0)134 430 6541

Notes

1. Federal Law No. 242-FZ, "On Amendments to Certain Laws of the Russian Federation in Order to Clarify the Procedure for Personal Data Processing in Information and Telecommunications Networks". This amends Federal Laws Nos. 149-FZ, "On Information, Information Technology and Data Protection", and 152-FZ, "On Personal Data" (both 2006).

2. OpenNet Initiative, "Russia". https://opennet.net/research/profiles/russia. [Accessed 25 September 2015.]

3. European Commission, "Factsheet on the 'Right to be Forgotten' ruling", C-131/12, n.d.

4. Privacy International, "Beyond the hype: the big issues in the European Court's 'right to be forgotten' ruling", 10 November 2014, https://www.privacyinternational.org/node/458. [Accessed 25 September 2015.]

5. Russian Ministry of Communications, "Handling and storage of personal data in the Russian Federation. Changes from September 1, 2015", 12 August 2015, http://minsvyaz.ru/ru/personaldata. [Accessed 25 September 2015.]

6. "Russia puts off data showdown with technology firms", *Wall Street Journal*, 31 August 2015.

7. RBTH, "Google will close its development center, but increase investment in Russia", 2 January 2015, http://rbth.co.uk/science_and_tech/2015/01/02/google_will_close_its_development_center_but_increase_invest_42631.html. [Accessed 25 September 2015.]

8. The Russian nuclear power agency was quick to offer its data services to Google and Facebook. See RBTH, "Rosatom invites Google and Facebook to store Russians' data next to a nuclear power plant", 1 September 2015, http://rbth.co.uk/business/2015/09/01/rosatom_invites_google_and_facebook_to_store_russians_data_next_to_a_48891.html. [Accessed 25 September 2015.]

9. http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=764677-6&02 [Accessed 25 September 2015.]

10. European Centre for International Political Economy, "Data localisation in Russia: a self-imposed sanction", Policy Brief, 6 (2015), http://www.ecipe.org/app/uploads/2015/06/Policy-Brief-062015_Fixed.pdf. [Accessed 25 September 2015.]

11. Katharine Kendrick, "Risky business: Data localisation", 19 February 2015, http://www.forbes.com/sites/realspin/2015/02/19/risky-business-data-localisation/. [Accessed 25 September 2015.]

12. "Putin calls internet a 'CIA project' renewing fears of web breakup", *The Guardian*, 24 April 2014.

13. "BRICS set out vision for International Information Security", *Sovereign Data*, No. 1 (July 2015).

14. Rebecca MacKinnon, "Playing favorites", *Guernica*, 3 February 2014.