Bloomberg BNA

Privacy and Security Law Report®

Residency Requirements for Data in Clouds—What Now?



By Lothar Determann, Edward Bekeschenko and Vadim Perevalov

On Dec. 31, 2014, Russian President Vladimir Putin signed a law[1] that advances the effective date of a previously enacted Russian data residency law.[2] As of Sept. 1, 2015, Russian and foreign companies will be required to record and store personal data of Russian nationals using databases located on Russian territory. Companies—particularly providers and users of social media and e-commerce, Internet, cloud and various other information technology and communications services—are concerned about the new requirements.

1. Data Transfer Restrictions Versus Data Retention and Residency Requirements

Data transfer restrictions and data residency and retention requirements are often confused or referenced synonymously.[3] But they are actually very different and quite opposite concepts.[4] Data transfer restrictions limit companies' ability to transfer personal data from one jurisdiction to another, but they do not require companies to keep data for a particular minimum time period (data retention laws do that) or in a particular place (data residency laws do that). Conversely, neither data residency nor data retention laws restrict companies in their ability to transfer data.

1.1. Data Transfer Restrictions

In 1995, the European Commission harmonized data protection laws across European Union member states in Data Protection Directive (95/46/EC)[5] because diverging national standards and cross-border transfer

[1] Sergei Blagov, *Russia Sets New Sept. 1, 2015 Deadline for Companies to Utilize Local Servers*, 14 Bloomberg BNA Privacy & Sec. L. Rep. (Jan. 5, 2015) (14 PVLR 31, 1/5/15).

[2] *See* Edward Bekeschenko, et al., *Companies Are Required to Store and Process Personal Data of Russian Citizens on Russian Territory* (July 2014), *available at* http://www.bakermckenzie.com/alrussiapersonaldataju l14; Sergei Blagov, *Russian President Signs New Measure Requiring Local Storage of Personal Data*, 13 Bloomberg BNA Privacy & Sec. L. Rep. 1332 (July 28, 2014) (13 PVLR 1332, 7/28/14).

Lothar Determann is a partner at Baker & McKenzie LLP's Palo Alto, Calif., office and teaches data privacy and e-commerce law at the University of California Berkeley School of Law and the Freie Universität Berlin in Germany.

Edward Bekeschenko is a partner and Vadim Perevalov an associate at Baker & McKenzie-CIS Ltd.'s Moscow office, specializing in information technology law and dispute resolution.

This article reflects the authors' personal opinions and not those of Baker & McKenzie, its clients or others.

[3] *See, e.g.*, Vaultive, *Data Residency—Addressing Data Protection Directives and Privacy Laws*, http://www.vaultive.com/cloud-risks/data-residency/ (last visited Jan. 31, 2015); Steve Pate, *Here, there, everywhere: Data residency and the public cloud*, Computerworld, Apr. 23, 2013, http://www.computerworld.com/article/2475145/cloud-security/here—there—everywhere—data-residency-and-the-public-cloud.html; Perspecsys, *Data Residency & Sovereignty*, http://perspecsys.com/how-we-help/data-residency-sovereignty/ (last visited Jan. 31, 2015).

[4] *See* Lothar Determann, *Data Privacy in the Cloud: A Dozen Myths and Facts*, 28 The Computer & Internet Lawyer 11, 1, 4 (2011) (Myth 6).

 ISSN 1538-3423

restrictions had become an obstacle to trade in the common market.[6] Before agreeing to a free flow of personal data between member states, Germany and other member states with historically high data protection standards insisted on a prohibition of data flows outside the European Economic Area (EEA). Consequently, restrictions on international data transfers were codified in Articles 25 and 26 of the 1995 Data Protection Directive, subject to a number of narrow, enumerated exceptions.[7] More and more countries have followed the European example and enacted restrictions on international transfers of personal data, including Russia in 2006.[8]

With restrictions on international data transfers in data privacy laws, countries try to ensure that local companies do not transfer personal data abroad, except with the data subject's consent or certain other protective measures, including data transfer agreements, binding corporate rules and the U.S.-EU and U.S.-Swiss Safe Harbor Programs.[9] Companies do not have to keep local copies of transferred data. Privacy laws do not require that companies keep data for any minimum time period or in a certain place. Under data privacy laws, companies are usually required to keep as little data as possible and only as long as necessary.

1.2. Data Retention and Residency Laws

Germany and other EU member states may not enact laws that require companies to keep personal data in Germany or other specific EU member states because the basic freedoms under EU law and the principle of free flow of data within the EEA would invalidate such discrimination. EU member states can pass, and some have passed, limited laws to require certain records to be available to local authorities.[10] Countries usually enact data or record retention and residency laws to secure access to records for their governments, including accounting records for tax authorities, books of financial service institutions for regulators and communications records for law enforcement agencies.[11] European data protection authorities have opposed and challenged European data retention requirements as hostile to data privacy. A number of national courts in the EU and ultimately the European Court of Justice have invalidated communication data retention laws.[12] As a consequence, there are few, if any, data retention or residency laws left in the EEA.

2. Political Developments After Snowden Revelations

When Edward Snowden started leaking classified information about U.S. National Security Agency surveillance programs in June 2013,[13] politicians in the U.S. and abroad immediately called loudly for stronger data privacy laws. The European Commission was leading a charge to establish a ''European cloud.''[14] German politicians and companies, including Deutsche Telekom AG, were advocating for ''E-mail made in Germany,'' a ''German Internet'' and new laws that would require companies to route domestic Web traffic through servers exclusively located within Germany.[15] Brazil and the EU talked about developing an undersea data cable to circumvent U.S. spying, and Brazil worked on an ''Internet Constitution'' (''Marco Civil da Internet''), which was supposed to include a local data storage requirement for Brazilian companies.[16]

But, after some initial outrage and international finger-pointing, it became clear relatively quickly that none of the hastily proposed new privacy laws or data residency requirements would effectively rein in cyber espionage.[17] It turned out that many European and other intelligence agencies had been heavily cooperating with the NSA and were intent to continue to do so

---

[5] Official Journal of the European Communities of 23 Nov. 1995 No. L. 281 p. 31; *see also* European Comm'n, *Reform of Data Protection Legislation*, http://ec.europa.eu/justice_home/fsj/privacy/ (last visited Feb. 10, 2015).

[6] The author's home state—the German State of Hessen—passed the world's first data protection law in 1970, quickly followed by other German states and European countries.

[7] Lothar Determann, *International Data Transfers from Europe and Beyond*, 25 Rev. Bank Fin. Serv. 1 (2009).

[8] Article 12 of the Federal Law of the Russian Federation No. 152-FZ, dated 27 July 2006, ''on Personal Data.'' Recently, Russia amended its list of countries providing adequate safeguards, from a Russian perspective, and dropped Switzerland and Hong Kong from its ''safe'' list. *See* Sergei Blagov, *Russia DPA Drops Hong Kong, Switzerland From Its Adequate Privacy Protection List Flag of Russia*, 13 Bloomberg BNA Privacy & Sec. L. Rep. (Dec. 22, 2014) (13 PVLR 2168, 12/22/14).

[9] *See* Lothar Determann, *Determann's Field Guide to Data Privacy Law: International Corporate Compliance* ch. 3, p. 40 et seq. (2d ed. 2015).

[10] Baker & McKenzie, *New Rules on Keeping Books for Tax Accounting: Germany Allows Cross-Border Outsourcing* (July 2009), *available at* http://www.bakermckenzie.com/files/Uploads/Documents/Germany/Newsroom/New%20Rules%20on%20Keeping%20Records%20for%20Tax%20Accounting_schwarz.pdf.

[11] *See* examples discussed in Business Roundtable, *Promoting Economic Growth Through Smart Global Information Technology Policy: The Growing Threat of Local Data Server Requirements* (2012), *available at* http://businessroundtable.org/sites/default/files/Global_IT_Policy_Paper_final.pdf; Stuart Lauchlan, *Secret Plans to Rip Up Data Sovereignty Rules, but Does Data Center Location Matter Any More?*, Diginomica, July 2, 2014, *available at* http://diginomica.com/2014/07/02/secret-plans-rip-data-sovereignty-rules-data-center-location-matter-more/; *New Rules*, *supra* note 10.

[12] *Digital Rights Ireland Ltd v. Minister for Commc'ns, Marine & Natural Res.*, No. C-293/12 (E.C.J. Apr. 8, 2014), *available at* http://curia.europa.eu/juris/liste.jsf?num=C-293/12#; Stephen Gardner, *ECJ Invalidates EU Data Retention Directive; Member State Laws Now Open to Challenge*, 13 Bloomberg BNA Privacy & Sec. L. Rep. 660 (Apr. 14, 2014) (13 PVLR 660, 4/14/14).

[13] Wikipedia, *Edward Snowden*, http://en.wikipedia.org/wiki/Edward_Snowden (last visited Jan. 26, 2015).

[14] Neelie Kroes, *Making Europe the Natural Home of Safe Cloud Computing*, European Commission blog (Nov. 14, 2011), http://ec.europa.eu/commission_2010-2014/kroes/en/content/making-europe-natural-home-safe-cloud-computing. Kroes is the vice-president of the European Commission.

[15] Leila Abboud & Peter Maushagen, *Germany Wants a German Internet as Spying Scandal Rankles*, Reuters, Oct. 25, 2013, *available at* http://www.reuters.com/article/2013/10/25/us-usa-spying-germany-idUSBRE99O09S20131025.

[16] Angelica Mari, *Companies Brace for Brazil Local Data Storage Requirements*, ZDNet, Mar. 7, 2014, http://www.zdnet.com/companies-brace-for-brazil-local-data-storage-requirements-7000027092/ (13 PVLR 519, 3/24/14).

[17] Lothar Determann & Karl-Theodor zu Guttenberg, *On War and Peace in Cyberspace: Security, Privacy, Jurisdiction*, 41 Hastings Const. L.Q., 1 (2014).

  PVLR ISSN 1538-3423

in the interest of their countries' national security.[18] All major privacy law reform proposals, including the long-awaited European data protection law regulation, expressly carved out national security activities.[19] Consequently, new data residency laws and requirements could only help secure better data access for local government agencies—and further erode citizens' data privacy.

In a last-minute change, Brazil removed data residency requirements from its Internet Constitution law, which was enacted in mid 2014,[20] and European politicians seemed to have moved on, too. Some countries kept sector-specific record retention laws in place, but no country applied broad residency requirements to all personal data—except one.

3. From Russia With Love

Russia originally enacted its data residency requirement in July 2014 with an effective date of September 2016.[21] A few months later, the Russian Parliament debated bills to accelerate the effective date to Jan. 1, 2015, and finally settled for Sept. 1, 2015.

Based on the new Russian law, companies have to process all personal data relating to Russian citizens in Russia. This requires operators of any computing and Web resources through which personal data of Russian citizens are collected to ensure that the databases used to record, systemize, accumulate, store, amend, update and retrieve data are located in Russia.

Unlike industry- or record-specific data retention laws, the Russian law is not focused on particular records or types of companies (e.g., invoices or banks). The Russian law covers any ''personal data,'' regardless of the type of record or company. Records that do not contain personal data are theoretically not covered by the law. However, in many practical scenarios, the most challenging point is to determine whether particular types of data qualify as personal data under Russian law. Given that the term ''personal data'' is very broadly defined, most records contain certain information that may potentially qualify as personal data under Russian law. Personal data include any information that relates to a directly or indirectly identified or identifiable individual.[22] There is no exhaustive list of such data, but normally they include the name, date of birth, passport data, address, education, family status and other information allowing the identification of an individual. Every signed business-to-business contract, commercial letter and any other document identifying its author contains a little bit of personal information. Therefore, most kinds of databases will be affected by the Russian law.

The law applies both to online and offline collection and processing of personal data. But, offline collection of personal data tends to occur on local systems anyhow, so the new law is expected to affect primarily companies that offer online services to Russian companies or individuals or multinationals with a Russian presence that have used centralized databases outside of Russia (in particular, centralized databases used for human resources, sales, client relations, document management, etc.).

To comply with the law, companies must perform at least initial collection, storage and extraction of personal data of Russian citizens using personal information databases located in Russia. This implies that the companies would need to reroute their data flows through servers located in Russia. From a practical perspective, the companies would need to either procure a dedicated server in Russia, lease it or use a duly secured cloud in Russia. The law does not require that a company fully localize IT systems in Russia and only covers the location of the databases in Russia.

The amendments are not clear on whether operations with personal data of Russian nationals will need to be performed solely with the use of Russian databases or whether the duplication of personal data abroad upon its initial recording in a Russian database will be allowed, as well. Starting in October 2014, the Russian authorities began producing various unofficial but very restrictive interpretations, expressing the opinion that any mirroring or using backup databases outside of Russia is prohibited.[23]

On the other hand, the recent law does not prohibit or impose additional limitations on cross-border transfer of personal data.[24] Almost all unofficial interpretations issued by the Russian authorities to date expressly support this. Also, the recent law does not require companies to delete databases that currently exist abroad and contain personal data of Russia citizens or to transfer such databases back to Russia. One could argue that such obligations are implied in the new Russian data residency law, but express requirements are notably absent from the new law, whose wording allows wide interpretations.

Thus, a company should continue to be allowed to either transfer personal data to a third party outside of Russia or to internally access and use such personal data from other countries subject to a regular require-

---

[18] Julian Borger, *GCHQ & European Spy Agencies Worked Together on Mass Surveillance: Edward Snowden Papers Unmask Close Technical Cooperation and Loose Alliance Between British, German, French, Spanish & Swedish Spy Agencies*, The Guardian, Nov. 1, 2013, *available at* http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden; Hubert Gude, Laura Poitras & Marcel Rosenbach, *Mass Data: Transfers From Germany Aid U.S. Surveillance*, Spiegel Online International, Aug. 5, 2013, *available at* http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html.

[19] Determann & zu Guttenberg, *supra* note 17, at 1.

[20] *See* Flavia Rebello, *Brazilian Internet Civil Rights Framework Approved in the House of Representatives*, *available at* http://www.lexology.com/library/document.ashx?g=b2823f60-ea91-4519-8dbb-ea6e8b0b968a; *Brazil Enacts Internet Bill of Rights*, Privacy Laws & Business, Apr. 28, 2014, *available at* http://www.privacylaws.com/Publications/enews/International-E-news/Dates/2014/4/Brazil-enacts-Internet-Bill-of-Rights/ (13 PVLR 803, 5/5/14).

[21] Federal Law No. 242-FZ, dated 21 July 2014, ''On Introducing Amendments to Certain Legislative Acts of the Russian Federation with regard to Personal Data Processing in Information and Telecommunications Networks'' (13 PVLR 1219, 7/14/14).

[22] *See* Baker & McKenzie, *Global Privacy Handbook* 391 (2014).

[23] Letter of the Presidential State-Legal Directorate of the Russian Federation Presidential Executive Office No. A6-8442 dated 18 Sept. 2014; Letters of the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) No. 08AP-64078 dated 1 Oct. 2014 and No. 08AP-3572 dated 19 Jan. 2015.

[24] *See* Bekeschenko et al., *supra* note 2.

ment to obtain the data subject's consent and compliance with Russian data privacy laws.

Failure to comply with the data localization requirement may potentially trigger administrative or civil liability and subsequent administrative or criminal liability for continuous failure to comply. Only Russia-based companies—including subsidiaries of multinationals—are significantly exposed to a risk of fines, given that the Russian government cannot practically enforce fines against foreign companies.

Another and potentially more substantial risk for foreign companies is that Roskomnadzor (the Russian supervising authority in the sphere of personal data) could also impose sanctions by blocking access to the noncompliant online services at the level of Russian Internet access service providers. Blocking injunctions can be circumvented and ignored by online pirates but can seriously affect legitimate businesses. Also, the Russian government can affect foreign companies indirectly by taking steps against their local customer base.

4. Effects and Options for Foreign Cloud and Internet Service Providers

4.1. Establish Additional Data Center

As one possible reaction to data residency requirements, multinationals could establish an additional full-scope data center in each jurisdiction that enacts a data residency requirement and then keep all data also in the respective territory. This would accommodate the data residency requirements. For example, if a multinational business group established an additional data center hosting all groupwide databases in Russia, the Russian affiliate could process all personal data relating to Russian citizens in the database on Russian territory.

But this would create a number of other issues and concerns. First of all, not every company will be willing to make the additional investment to establish and maintain an additional data center. Second, potential access to the data in the new host country can create tensions under data privacy laws in other countries; notably, the EU data protection laws require data minimization and prohibit transfers of personal data to jurisdictions with overreaching government access to personal data. Third, multinational customers may not find it acceptable that all their data are suddenly hosted in more and more jurisdictions, with associated concerns for foreign government access to data. Fourth, the more countries enact data residency laws, and the more data centers multinationals have to establish, the less viable the rationalization benefits of cloud computing will become.[25]

Fifth, last but not least, any additional server or database location can create additional complications under international tax laws. For example, Russian law does not currently have a concept of a ''server-based'' taxable permanent establishment. However, many tax concepts developed by Organization for Economic Cooperation and Development countries are currently being implemented in Russia. In the long term, companies operating Russia-based databases in connection with their commercial activities might face the risk of ''server-based'' permanent establishment claims in Russia, especially in the e-commerce and cloud computing market segments.

4.2. Segment Databases and Keep Only Data Subject to Residency Requirements Local

Instead of storing all data locally, service providers could also reconfigure their architectures in a way that gives customers the option to have only certain data stored locally, e.g., Russian data in Russia. This will counteract some of the benefits cloud technologies offer and require additional investments, which providers will very likely try to pass on to their customers. But the Russian law, for example, does not require all IT systems to reside in Russia—only databases. Depending on the exact architecture environment, the additional investment of localizing only the database component of a system could be affordable for some companies.

Some of the major cloud service providers, such as SAP SE and Microsoft Corp.'s Azure, have reportedly established cooperation with local data centers in Russia in order to allow their customers to adhere to their systems while ensuring compliance with the Russian residency laws.[26]

Another potentially viable database segmentation option is to record and store only personally identifying data in Russia (a portion of the database containing full names, contact details, etc.), while processing pseudonymized user transaction data in data centers located abroad.

4.3. Keep Data in the Cloud and Local Backup Copies

One way to ensure the availability of databases locally is to make and keep (partial) copies of databases locally, for example, by way of continuously creating local backup copies of data subject to residency requirements on a local, external data storage device. If the local company that is subject to data residency requirements uses a standard storage device and a backup software program, this approach would not create any significant additional costs and could prevent more significant disruption of cloud architectures. It should also largely satisfy a foreign government's objectives to secure easy access to the personal data of its citizens.

But this approach may not be acceptable to all government authorities. Roskomnadzor, for example, issued a nonbinding opinion in October 2014 that only databases located within Russian territory may be used for the processing of personal data of Russian citizens (recording, correction, alteration, extraction, etc.).[27]

4.4. Keep Data Subject to Residency Requirements Out of Clouds

Cloud and Internet service providers with a global customer base could also decide to stop targeting customers in countries with data residency requirements

[25] *See*, on the benefits of cloud computing more generally, Lothar Determann & David Nimmer, *Software Copyright's Oracle from the Cloud, Software Copyright's Oracle from the Cloud*, 30 Berkeley Tech. L.J. (forthcoming 2015); Lothar Determann, *What Happens in the Cloud—Software-as-a-Service and Copyrights*, 29 Berkeley Tech. L.J. 1095 (Oct. 18, 2014).

[26] Denis Voeykov, *Microsoft Moves Windows Azure to Russian DCs*, CNews.Ru, Jan. 28, 2015, http://www.cnews.ru/top/2015/01/28/microsoft_perevozit_windows_azure_v_rossiyskie_cody_592057; *The First Russian SAP Data Center Has Opened*, CNews.Ru, Dec. 24, 2014, http://www.cnews.ru/top/2014/12/24/otkryt_pervyy_rossiyskiy_datacentr_sap_591189.

[27] Letter of Roskomnadzor No. 08AP-64078 dated 1 Oct. 2014.

  PVLR ISSN 1538-3423

and post notices on their sites that the service or other offering should not be used as the primary database for personal data that are subject to residency requirements. If a local company uses the service anyway, possibly in violation of local law, it could not bring civil claims against the service provider and the foreign cloud or Internet service provider should not be otherwise exposed to foreign government sanctions. The foreign government might try to block Internet protocol addresses of the foreign provider, but this should not present major issues for a company that has decided not to target customers in the affected jurisdictions anymore.

Multinationals with local presences in countries that establish data residency requirements may have to consider setting up separate, local databases for their affected subsidiaries. Right now, where only Russia has a residency requirement, some multinationals may decide to just cut their local Russian subsidiaries off of centralized cloud systems that store personal data and instead process Russian personal data of local employees and customers in local databases (e.g., semi-manually on spreadsheets and local PCs if necessary). Companies with small presences may find such workarounds more tolerable than companies with larger presences in Russia.

Even multinationals with relatively small presences will probably face some compliance issues. For example, if a U.S. parent company wants to grant employee stock options to employees of its Russian subsidiary, it will not be able to get its U.S. stock plan administrators, brokers and other service providers to set up special databases in Russia for Russian employees who are eligible to receive equity in the U.S. parent company. It is unrealistic to expect Russian banks to be able to pick up this business, given the various compliance requirements arising under U.S. laws relating to equity accounts. Similar problems can be expected with any other groupwide, regional or centralized benefits or systems—the Russian entity and employees would have to be excluded.

Users of cloud and Internet services in countries that impose data residency requirements can expect a reduction in available options and offerings if foreign companies are unwilling or unable to accommodate the data residency requirements. Especially smaller, charge-free services may become unavailable, at least until local offerings develop. Foreign news and media companies could also be blocked based on the failure to comply. Perhaps this will boost the development and establishment of local, home-grown IT services providers. But, since economies of global scale will not be available to local alternatives, an increase in prices and reduction of available offerings could also be a more permanent consequence. Consumers and companies in countries with strict data residency requirements will likely not be able to benefit from the full potential of cloud computing solutions. This will possibly slow down local technological progress and increase the global digital divide further.