



We hope you find this information useful. The expert's comments represent his own viewpoints and do not necessarily represent the views of the DMA or eec. Please review your email program with your legal counsel to ensure that your program is meeting appropriate legal requirements. The information provided is for your background and overall guidance and should not be considered as legal advice for your specific needs.

As you may now know Russia passed a new law requiring the local storage in Russia of the personal data of Russian citizens. Under the Data Localization Law, businesses and data operators processing data of Russian citizens, whether collected online or offline, are obliged to record, systematize, accumulate, store, update, change and retrieve such data in databases located within the territory of the Russian Federation. It is clear that the new Law will be applicable to Russia-based data operators (including subsidiaries and representative offices of foreign companies). Under the current version of the Law, it will come into force on 1 September 2015.

What's odd about this change is that Russian law does **ALREADY** offer consumer protections...

For regulating marketing communications, for example;

- The Federal law "On Advertisement" as of 13.03.2006 No. 38-FZ. This regulates marketing communications sent inter alia by electronic means including email, SMS etc.;
- The Russian Code on Administrative Infractions dated 30.12.2001 No.195-FZ. This regulates issues of responsibility for commission of administrative offenses in connection with processing of personal data or distribution of marketing communications.

And there are laws geared at processing personal (consumer data)... Specifically outlining requirements of data processors, for example;

- The Law of the Russian Federation "On Personal Data" as of 27.07.2006 No. 152-FZ, regulating the processing of personal data by means of automation equipment. It is the operator who is required to comply with that Act;
- The "Regulations on securing personal data being processed in personal data systems" enacted by the Russian Government Regulation as of 17.11.2007 No. 781.
 - The Regulations contain mandatory security regulations to be complied with when processing and storing personal data;

The legislation has been criticized for its vague wording and practical implications. The important aspect of this law is the fact that it is so far reaching. Even where a business has Russian customers but no legal presence in Russia, it should note that Russian data protection law is considered as public order for all companies collecting and processing personal data of Russian citizens, with no exceptions for foreign companies. Therefore, if a business holds Russian personal data in the US and UK, the law is, technically, applicable to that business.

The business community has applied pressure since the New Law was announced to obtain clarification from the authorities on the implications for those conducting business in Russia and dialogue between businesses and the authorities continues.

Russian law has an extremely broad definition: Personal data – any information relating directly or indirectly to an identified or identifiable individual (personal data owner). Under their law, personal data means any data related to a directly or indirectly identified or identifiable individual (data subject), including his/her first name, middle name and last name, year, month, date and place of birth, marital and social status, welfare, education, profession, income, etc. and at this time.

What is cited as POSSIBLE new processes due to this new law are:

- Companies conducting business in Russia could be forced to open data centers with data storage capacities in Russia or face the risk of being blocked and/or added to the register of websites which contain infringing information i.e. storing personal data of Russian citizens outside of Russia. The New Law gives Russian data subjects and/or the DPA the right to obtain a court order to have an "infringing" website added to the Register, the idea being that the DPA will then contact host and service providers and arrange for access to the relevant website to be blocked via a notice and takedown procedure.
- Any foreign companies collecting the personal data of Russian individuals will be required to install servers in Russia and only use these servers to process information about Russian citizens. Recent discussions have suggested that this is very unlikely, given that the DPA has admitted that it has no jurisdiction over foreign companies.
- The cross-border transfer of personal data of Russian citizens is also at issue, particularly as the New Law now conflicts with Russia's existing laws on international data transfers.

When asked about the application to others outside of the Russian Federation., the Russian President's Administration to the Association of European Businesses distributed to the public certain clarifications that were very unclear, formal, and technical and their response stipulated:

- Companies should not make copies of the databases outside of Russia
 - The Law says nothing on this, and, therefore, the data should be kept on servers located in Russia.

- The Law applies not only to the storage of personal data collected from the Law's effective date, but also to personal data that was collected prior to such effective date.
- The Law covers not only Internet companies, but all other operators as well.

However, as we look closely at this, the literal wording of the Law does not explicitly require data operators to perform data processing operations solely within the territory of the Russian Federation; it just requires that a copy of the data be stored in Russia. There is also no explicit prohibition of cross-border transfer introduced into the Law. ***“Organizations may transfer personal data outside of Russia provided that the receiving jurisdiction provides a similar level of protection for personal data; the affected data subjects have been informed or have provided consent; and reasonable steps have been taken to safeguard the personal data to be transferred. Furthermore, international data transfers will be considered valid provided that appropriate data transfer agreements (model contracts) or other prescribed measures are put in place”***

The likely outcome is that cross-border transfers will continue to be permitted. Once this is clarified it is anticipated that a legally compliant 'structure' for businesses will be:

- Personal data of Russian citizens is first aggregated in Russian located servers;
- Parties put in place a data transfer agreement in which the parties agree to transfer data outside of Russia.
- The personal data can then be transferred outside of Russia.

The Law contains a procedure for adding a data operator that violates the law into the register, and restricting access to that operator's website if found guilty of violating the laws data localization requirements which would be similar in nature to the Great Firewall of China which many know is China's ways of censorship to prevent their citizens from seeing the free world of information.

As of today, the fines that may be imposed on legal entities for violation of the general rules of collection, storage, use or distribution of personal data amounts to RUB 10,000 (approximately US \$200) and the Law does not provide any individual right of action. No official clarification as to whether the fine is to be introduced per claim or per violation. Currently in practice these fines are usually imposed per claim. The Russian DPA has frequently commented that the amounts of the fines should be increased.

There are some exceptions to the New Law (which remain to be clarified) including:

- Processing for purposes required by law of an international treaty;
- Judicial purposes;
- Processing by state authorities; and
- Mass media purposes.

However, these are of little to no assistance to the business community as they are predominantly non-commercial exceptions.

So again, the law explicitly indicates the party responsible for personal data collection, at the point of collection, is required to store the authoritative data records pertaining to Russians within Russian Federation boundaries.

Within this requirement, however, only the “data structure” which holds Russian PII has to reside in Russia.

- The term “data structure” can refer to a Microsoft excel spreadsheet, a word document table, of course a database, and even the organized contents of a mailbox.
- Essentially, any logical data arrangement which collects Russian citizen PII fits the bill, and must be located within Russian federation boundaries.
- However: Any peripheral or supporting web infrastructure can be hosted elsewhere.

So now what?

- Companies conducting business in Russia could be forced to open data centers with data storage capacities in Russia.
- Any foreign companies collecting the personal data of Russian individuals will be required to install servers in Russia and only use these servers to process information about Russian citizens.
 - **Recent discussions have suggested that this is very unlikely, given that the DPA has admitted that it has no jurisdiction over foreign companies.**
- The cross-border transfer of personal data of Russian citizens is also at issue, particularly as the New Law now conflicts with Russia's existing laws on international data transfers.
- Do nothing.

So at this particular moment nobody in Russia knows for sure which options with regard to personal data storage are prohibited and which are not after 1 September 2015.

We will continue to monitor this issue and keep you updated.

-Dennis

Dennis Dayman, CIPP/US, CIPP/E, CIPT
Vice-Chair, eec Member Advisory Committee
Chief Privacy and Security Officer
Return Path, Inc.
<http://www.returnpath.com>