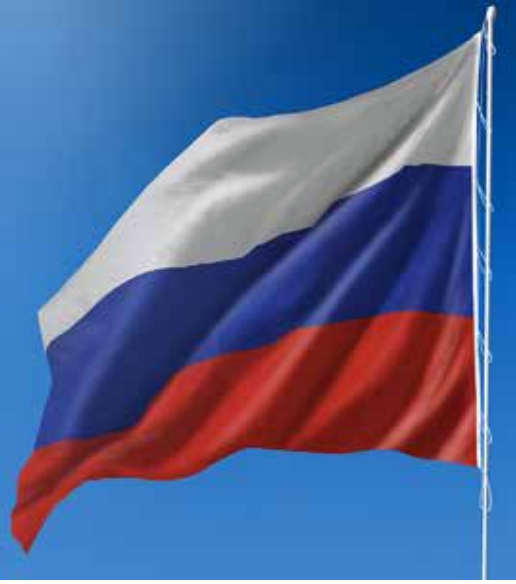

The "localisation" of Russian citizens' personal data

Compliance with the Russian law on personal data

Requirements governing personal data processing were formulated in Russian law as far back as 2006. Since then the legislation has undergone various changes, with the most well-known probably being the requirement to "localise" the personal data of Russian citizens.

Overview

On 21 July 2014 Federal Law No. 242-FZ "On Amending Certain Legislative Acts of the Russian Federation Regarding Clarifying the Personal Data Processing Procedure in Information and Telecommunication Networks'' was approved. One of the changes related to Federal Law No. 152-FZ dated 27 July 2006 "On Personal Data", and added Part 5 to Article 18 "The Obligations of the Operator when Collecting Personal Data" of the Law.

In accordance with this part, "when collecting personal data ("PD"), including via an information and telecommunications network (the Internet), the operator (i.e. Company – KPMG note) is obliged to ensure the recording, systematisation, accumulation, storage, clarifications (updates / modifications) and extraction of the personal data of citizens of the Russian Federation using databases located in the Russian Federation ("Russia")…".

Informally called a requirement to "localise" the personal data of Russian citizens, this legal norm entered into force on 1 September 2015.

Official position of the Russian Ministry of Digital Development, Communications and Mass Media[1]

The Federal Law «On Personal Data» (Part 5, Article 18 – KPMG note) focuses on the Internet resources used by an individual to perform specific activities in Russia that can be blocked in a prescribed manner, should their owner fail to comply with the requirements of the Federal Law «On Personal Data».

"Personal data subject to localisation are personal data received by an operator in the course of activity aimed at collecting such data, and not as a result of accidental (not requested) access to personal data; for example, if received by email or other mail that contains personal data."

"The personal data of a Russian citizen, initially entered into and updated in a database in Russia, may then be transferred to databases located outside Russia and administered by other persons, subject to the provisions on cross-border data transfer. Granting remote access to databases located in Russia from the territory of another country is not prohibited under Federal Law 242-FZ."

"If personal data were during their collection entered into a database located in Russia, such personal data may subsequently be entered by an employee (representative) of the operator into its own electronic database located outside Russia."

"Certain types of processing of personal data, prescribed in Part 5 of Article 18 of Federal Law No. 152-FZ, including the collection of personal data on paper media and their subsequent entry into an electronic database, should be performed as a single process within the legislative framework governing the obligation to keep personal data in Russia."

[1] *Source: http://minsvyaz.ru/ru/personaldata/*

Our view

A company must ensure the initial collection and subsequent recording, systematisation, accumulation, storage, clarifications (updates / modifications) and extraction of the personal data of Russian citizens using databases located in Russia.

Subsequent clarifications (updates / modifications) of personal data, as indicated above, should also be performed first in a database located in Russia.

Subsequently personal data can be transferred to a server (information system) located outside Russia, in accordance with the legislative requirements governing the cross-border transfer of personal data.

New penalties in force since July 2017

Since 1 July 2017, new penalties for non-compliance with the Russian legislation on the processing of personal data have been applied. For more details, see Article 13.11 of the Russian Code of Administrative Offences. Also, no separate penalty exists for failure to comply with the requirement to "localise" the personal data of Russian citizens; however, this does not mean that the requirement can be ignored. The regulating authority (Roskomnadzor, the Federal Service for Supervising Communications, Information Technology, and the Media) may use such measures as restricting access to the company's information system from Russia, and issuing orders to eliminate violations based on the results of inspections. The implementation of such orders will in most cases simply be impossible, due to the timeframe allowed by the regulating authority (usually three-to-four months).

Personal data of Russian citizens

For example:
- First name
- Surname
- Contact information
- Passport details
- Finance information
- Race / ethnic origin
- Political views
- Religious / philosophical beliefs
- Health status etc.

Database located in Russia

- Collection
- Recording
- Systematisation
- Accumulation
- Storage
- Clarification (updates, modification)
- Extraction
- Use
- Transfer (distribution, delivery, access)
- Anonymisation
- Blocking
- Deletion
- Destruction

Database located abroad

- ~~Collection~~

Only after collection in Russia:
- Recording
- Systematisation
- Accumulation
- Storage
- Clarification (updates, modification)
- Extraction

No limitation:
- Use
- Transfer (distribution, delivery, access)
- Anonymisation
- Blocking
- Deletion
- Destruction

"In our practice we have come across an incorrect interpretation of the requirement to "localise" the personal data of Russian citizens, i.e. as a ban on the storage of their personal data abroad. It is important to ensure that the initial collection of the personal data of Russian citizens is performed using databases located in Russia; then, subsequently, in accordance with respective cross-border data transfer requirements, personal data can be transferred abroad, if necessary. The same requirement applies to making changes to personal data: first they should be made here in Russia, and then abroad."

Note

- The requirement to "localise" the personal data of Russian citizens does not prescribe limitations on their subsequent cross-border transfer.
- The initial collection of personal data from a subject should be performed using databases only located in Russia.
- Changes to personal data should be made first using databases located in Russia, then the changes may be transferred to databases located outside Russia.
- Limitations apply only to the location of databases; information systems can be located outside Russia.

Contacts

Benny Bogaerts
KPMG Advisory
Partner
T: +32 (0)3 821 18 93
E: bbogaerts@kpmg.com

Kara Segers
KPMG Advisory
Manager Advisor
T: +32 (0)2 708 39 57
E: ksegers@kpmg.com

Ilya Shalenkov
Information Risk Management group
Senior Manager
T: + 7 495 937 4444, ext. 10138
E: ishalenkov@kpmg.ru

Andrey Alekseev
Information Risk Management group
Manager
T: + 7 495 937 4444, ext. 15238
E: andreyalekseev@kpmg.ru

Kristina Borovikova
Information Risk Management group
Senior Consultant
T: + 7 495 937 4444, ext. 16358
E: kborovikova@kpmg.ru

kpmg.com/be