

# Use of Public Cloud Services by Russian Financial Services Institutions

[This presentation contains references to Article “Use of Public Cloud Services by Russian Financial Services Institutions (FSI)” (hereinafter – the “Article”)]

Vladimir Kanashevsky  
Of counsel of Pierstone

# Regulation of cloud services

[see: Section 1A of the Article]

Currently there is no comprehensive, universal statute or other normative act regulating cloud services in the Russian Federation.

The storage of data in cloud per se is not prohibited and thus permissible under Russian laws, subject to observance of certain legal requirements and restriction which concern:

Personal Data Issues

Storing confidential information

Localization of electronic data bases of Russian banks

Licensing and certification requirements



# Storing personal data ("PD") in a foreign cloud. Cross-border PD flows

[see: Section 1B of the Article]

Cross-border transfer of PD of Russian citizens and its processing (storage, etc.) in foreign data hosting centers is permitted subject to certain requirements and restrictions:

The PD of Russian citizens shall be initially recorded and processed in databases located in Russia.

The personal data operator (i.e. the cloud provider) shall undertake the measures to ensure the security of PD and confidentiality (in particular, data encryption and data anonymization).



# Storing confidential information in a foreign cloud

[see: Section 1C of the Article]

When storing confidential information, the cloud provider must take certain security measures to protect the information entrusted to it. Such measures shall provide for the same level of protection as the relevant measures prescribed by Russian law.

## Confidential information:

Financial information

Certain tax information

Bank secrecy information

Information on security and technical measures

Information on security and technical measures

Credit history, insurance and pawnshops secrecy data

Certain internal corporate documents

Other information marked by a credit institution as "confidential"



# Localization of electronic data bases of Russian banks

[see: Section 2A of the Article]

A credit institution shall ensure that its electronic databases are located in the territory of Russia and store in such database information about its assets, liabilities, transactions, primary documents, etc.

A credit institution may transfer and store the respective data in a foreign cloud provided that:

- i. Such data is initially recorded in electronic databases located in the territory of Russia
- ii. The foreign cloud provider fulfills the respective security measures:
  - The database is up to date
  - The information is recoverable
  - The measures are taken to prevent damage (loss, malware infection, etc.) to information
  - The backup copies are created



# Licensing and certification requirements

[[see: Section 2B of the Article]

Some of the foreign cloud solutions involve encryption and other information security means. This may create a practical obstacle for use of cloud solutions of foreign providers.

In particular, only Russian entities are eligible to obtain licenses for work with encryption means and means for technical protection of confidential information.

One of the exclusion is the PD: if it is technically impossible to implement the certain measures for provision of PD security, the operator may deploy other (“compensatory”) measures for the neutralization of PD security threats.

However in respect of other information (bank secrecy information, financial information, etc.) the possibility of deployment of “compensatory” measures is not provided by the law.



# Non-credit financial institutions (NFIs)

[see: Section 3 of the Article]

Russian laws regulating various types of NFIs (insurance companies, micro-financial organizations, pawnshops, etc.) do not contain any provisions that would either permit or prohibit the relevant NFIs to use public clouds services (including those that are provided outside of Russia).

The absence in Russian laws of express prohibition of the use of public cloud solutions by NFIs suggests that NFIs may use public cloud services, including those provided by foreign providers (subject to certain requirements and restrictions).

The standards and recommendations applicable to banking organizations are likely to apply by analogy to NFIs pending specific regulations to be introduced for NFIs in that field.

