Security

Reinforcing data protection laws

Flexible security solutions

Orange Business Services' flexible solutions are helping companies address Russia's new far reaching and hard hitting data protection laws.

Russia recently introduced tough new legislation on data protection and data retention obligations. Under Russian law, companies operating or storing data in the country must carefully assess their governance and compliance strategies, or leave themselves open to large fines and Internet site close downs.

Russia introduced the legislation as an amendment to its data protection law, which took immediate effect from September 1, 2015. It is designed to protect the personal data of Russian citizens and deliver national data sovereignty.

Under the new law, all companies doing business in Russia – regardless of where they are headquartered – are required to process and store personal data relating to Russian citizens within the Russian Federation (first and last name, personal phone number, email, address, personal biometrical and medical data, etc.). This means that any cloud services, databases and other facilities that store personal data on Russian citizens must have servers located within the Russian Federation. This includes companies selling goods online in Russia who have no physical presence in the country.

Additionally personal data transfer is not allowed via open channels, and channel encryption is required. Standard encryption does not comply with the amended legislation. Companies require a dedicated encryption box with FSB- and FSTEC-certified cryptographic algorithms, which Orange Business Services can supply as part of its managed services on the connectivity side. According to Federal Laws #152 and #242, Government Decree #119 and FSTEC Order #21, any servers that are used for keeping personal data must use certified software and be protected by a certified firewall (which can be provided by Orange as a part of a managed solution) and antivirus.

Companies are required to notify the Russian data protection authority, Roskomnadzor, about data processing on Russian citizens. The authority has the power to block websites and to maintain a registry of data violators.

Russia based companies – including subsidiaries of multinationals – need to take action to comply with the country's data protection law, if they haven't already, or face significant penalties.

Roskomnadzor estimates that around **2.6 million** companies process personal data in the country.

One instance is LinkedIn, the major global professional social network, which was banned in Russia following accusations of failing to comply with the 2014 federal law that requires Internet companies that process Russian citizens' personal information to store their user data on servers located in Russia.

orange™ Business Services

Data sovereignty challenges

To ensure that companies comply with the Russian data sovereignty laws, there are a number of questions companies must ask themselves.

Understand what personal data means

Companies need to understand the Russian definition of personal data. They need to know what personal data they are storing and how it is being used.

Look at where your data is stored

You could be storing data in several locations across the world. If you are using a cloud-based solution, you must re-architect it to make sure that Russian data essentially resides in Russia.

Know your cloud

Find out from your cloud providers exactly where they are storing the data, and the costs involved moving it.

Keep ahead of the curve

Compliance and guidelines are expected to continue to develop around the Russian Data Sovereignty law, so companies need to ensure they are up-to-date with future legal changes or enforcement practices.

Know your partner

Don't underestimate the time and cost of data migration. For IT departments this could be one of the largest data migrations they have undertaken. Does your partner know the market and have specialists on the ground to ensure a smooth migration?

Migration roadmap

A migration roadmap is essential to ensure that business processes run smoothly during data migration and mission-critical data is not left exposed.

Use case 1: adapting business operations

A multinational retailer with major plans to expand into the Russian market, with online and “bricks n mortar” shops, plus its own production facilities, needed to adapt its business to comply with changes to the personal data law in Russia.

The company faced a challenge in localizing its e-commerce platform, including both its website and mobile app, in Russia. The legal change came into effect on September 1, 2015, requiring companies processing Russian citizens’ data, either collected online or offline, to record, process and store such data in databases located only within the Russian Federation. Companies not complying have had their websites blocked.

The multinational retailer first had to answer a number of questions:

- What personal data on Russian citizens did it hold?
- How large was its personal data issue?
- What was required to encrypt data?
- What was the best way of making this data compliant with Russian law?

Solution

With significant plans to expand its Russian footprint, the multinational retailer needed a flexible and scalable solution that would comply with the country’s legal requirements.

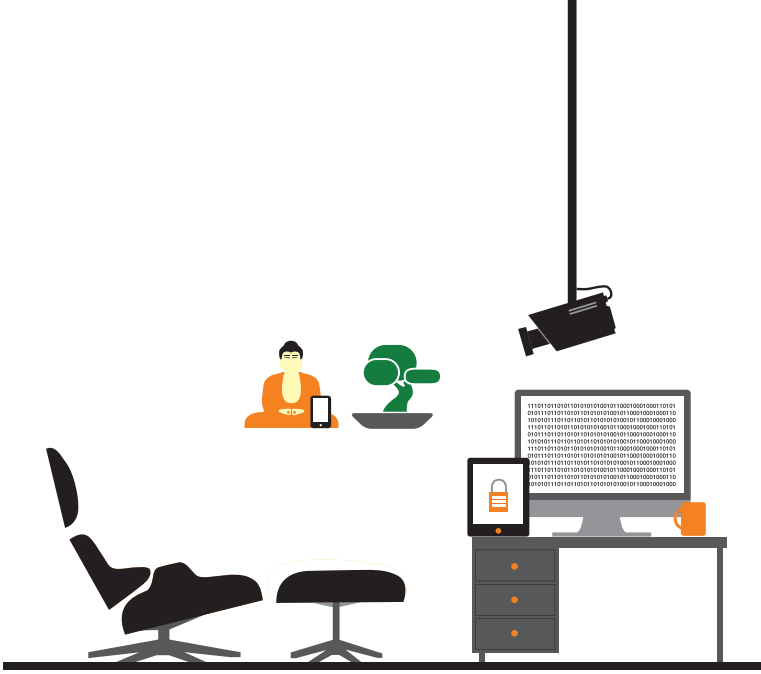
Flexible Computing Advanced, a shared private cloud solution from Orange, was chosen as the most cost efficient and relevant to the company’s needs. Flexible Computing Advanced allows enterprises to build a Virtual Data Center (VDC) with fully-scalable resources, including CPU, RAM, storage, backup and network bandwidth. Orange offers end-to-end service level agreements (SLAs) and management for the entire infrastructure.

By building the company’s cloud infrastructure onto a globally consistent, secure and reliable virtual private cloud, Flexible Computing Advanced has given the multinational retailer the scalability it requires to scale its resources up or down to match demand – paying only for what they need.

Orange was selected for its local cloud expertise, ability to provide strong SLAs that underscore the company’s compliance needs, and a possible future collaboration in connecting new retail shops.

Benefits

Through the flexibility and scalability of Flexible Computing Advanced, the company can efficiently and cost-effectively manage and secure its data across sites, while being fully complaint with Russian legislation.



Use case 2: localizing an e-commerce platform

A global luxury goods retailer needed to localize its e-commerce platform following changes the Russian Government made to the country’s law on personal data.

Due to the changes, the luxury goods retailer needed to locate its e-commerce platform locally in Russia. The company had two options – either invest in its own data center, or go with a service provider. The latter was seen as a more cost effective option as it provides both flexibility and scalability.

Solution

The company opted to go with Flexible Computing Private from Orange, a dedicated virtual IT infrastructure with flexible and automated resource and service management (IaaS model).

Flexible Computing Private is based on HP Enterprise servers located at the Orange Data Center in Moscow, Russia.

Benefits

The Flexible Computing Private solution has enabled the company to comply with Russian regulation and reduce costs by deploying its e-commerce platform at the Orange Data Center in Moscow and moving to an OPEX model. Thanks to the centralized infrastructure and the purchase of a solution as a service, it has also enabled the luxury goods retailer to make additional cost savings due to reduced capital IT expenditure.

Choose a flexible security solution from Orange Business Services.

For more advice on how flexible security solutions can help your business visit:

orange-business.com/ru-en

orange™ Business Services