East-West Digital News

WITH THE SUPPORT OF

EY Building a better working world

PERSONAL DATA STORAGE IN RUSSIA

What international businesses should know to organize data transfer to Russia and maintain ongoing compliance with Russian law

V1.3 – SEPTEMBER 2015

WITH THE SUPPORT OF

IXcellerate DataSpace Selectel

MAIN RESEARCH AND MEDIA PARTNERS

CCI FRANCE RUSSIE
FRANCO-RUSSIAN CHAMBER OF COMMERCE AND INDUSTRY

internet RETAILER

J'son & Partners

NetMediaEurope

THE PAYPERS

RUSSIA BEYOND THE HEADLINES

About this white paper

Intended for organizations that collect, store or make use of personal data related to Russian citizens, this white paper offers recommendations on how to comply with the existing Russian legislation in this field, taking into account legal, organizational and commercial aspects.

The document includes contributions from the EY Intellectual Property Center of Excellence in Russia and CIS, data center companies Ixcellerate, DataSpace and Selectel, payment operator PayU, and market research company J'son & Partners.

About the publisher

East-West Digital News is the first international information company dedicated to Russian digital industries. Its website EWDN.COM provides news, market data, business analysis and updates pertaining to the Internet and mobile industries, e-commerce and e-marketing software and hardware innovation as well as the related investment activity and legal developments.

The company also publishes authoritative industry reports covering, in particular, Russian e-commerce, online video, and venture markets.

A consulting branch, East-West Digital Consulting, provides international players with assistance for business development in Russia and advises Russian companies on their international strategies.

For more information, please contact us at **contact@ewdn.com**

Copyright policy

Advertising, sponsorship and distribution opportunities

To inquire about advertising and sponsorship opportunities, or if your would like to get involved in the distribution of this white paper, please contact us at **ads@ewdn.com**.

Chief editor's note

Adrien Henni, East-West Digital News

Starting from September 2015, companies operating in Russia have been required to store their users' or clients' personal data on servers located physically on Russian territory.

Many businesses are impacted – but with considerable differences depending on the sector and type of business.

This document offers a full set of recommendations on how to transfer data to Russia, encompassing the legal, organizational and commercial aspects of this migration.

Also included is a comprehensive legal analysis of the questions that will arise *after* the data is transferred to Russia: How should law-abiding businesses organize the collection and protection of personal data, and how can they use them, in Russia's specific legal and business conditions?

Our special gratitude goes to the pool of experts who brought their contributions to this document. This includes the team of the EY Intellectual Property Center of Excellence, the experts of data storage company IXcellerate, payment operator PayU, and the J'Son & Partners consultancy.

We hope you enjoy this collaborative effort and wish you every success in your projects involving Russian users.

Sincerely,

Foreword

Guy Willner, IXcellerate CEO

Uncertainty can be the biggest regulatory challenge facing the general counsel of multinational companies: “Give me enough certainty – clear rules and guidance – and I can structure my operations for success.”

In December 2014, the Russian government made amendments to the Information Law No. 242-FZ, which meant that the it will take effect much earlier in September 2015 and not 2016 as originally expected. The law simply states that the personal data of Russian citizens has to be stored locally on domestic servers. However just as with any new law there is much uncertainty and many questions surrounding it. What are the steps to follow? What a company can and cannot legally do in order to comply?

We founded IXcellerate in 2011 after two years looking at the market in Russia. Together with solid finance partners Sumitomo Corporation and IFC (present in Russia for 50 and 21 years, respectively), we built Phases 1 and 2 of a 15 Megawatt 15,000m^2 campus near central Moscow. With over 20 telecoms networks now connected and international customers such as Thomson Reuters and Sprint, the business has developed fast despite the challenging economic environment.

The only IBM Level3 compliant datacentre in Russia (equivalent to Tier3), Moscow One is the first of a series of datacentres we have planned in the region, with help from experts from some of the world's leading players such as Equinix and InterXion.

Running IXcellerate, with its head office in London, I kept coming across international as well as locally based Russian companies, with servers abroad concerned about the new law. What I found was that local enterprises were aware of the law, but had little idea of what exactly was needed in order to comply. With international players I was meeting in London, their story was much more complicated. Many were not even aware of the new law. Small to medium businesses were worried, once I shared the information with them, that their operations in Russia would be illegal unless something was done very quickly. With large companies the story was not unusual; some employees seemed to be aware, but were waiting for instructions from senior management to react, rather than proactively forming work groups and implementing an action plan.

As the law evolves legally and technically, we have teamed up with EY, one of the leading law advisories, and EWDN, a digital news distributor in Russia, to raise awareness of the changes coming and simplify compliance process for all those affected. I hope that this white paper will prove to be effective leaving you with a clear understanding allowing you to implement all necessary changes swiftly and efficiently in order to comply with this fast approaching deadline.

Sincerely,

Participating companies

EDITORIAL CONTRIBUTIONS

EY Building a better working world

J'son & Partners

payU

DataSpace

IXcellerate

Selectel

NETWORKING SUPPORT

CCI FRANCE RUSSIE
FRANCO-RUSSIAN CHAMBER OF COMMERCE AND INDUSTRY

RBCC
RUSSO-BRITISH CHAMBER OF COMMERCE

MEDIA PARTNERS

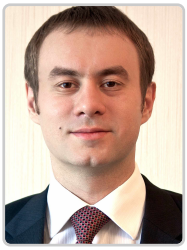
internet RETAILER

THE PAYPERS

NetMediaEurope

RUSSIA BEYOND THE HEADLINES

Authors and contributors



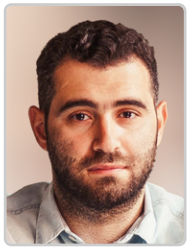
Mikhail Chentsov
Head of the Business legal support division of the Legal dpt., Otto Group Russia

Dmitry Fokin
Managing Director IXcellerate Moscow Datacentre

David Hamner
Co-founder and Chairman DataSpace

Adrien Henni
Chief editor East-West Digital News

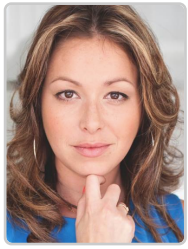
Anastasia Kuznetsova
Lawyer, Intellectual Property Center of Excellence (CIS), EY Russia



Lev Leviev
CEO Selectel

Pavel Marceux
Lead Analyst East-West Digital News

Igor Nevzorov
Head of Intellectual Property Center of Excellence (CIS), PhD (Law), EY Russia



Julia Shelygina
PR & Marketing Manager PayU Russia

Sergey Zolkin
Senior Consultant J'Son & Partners Consulting

See contact details on page 60

Table of contents

PERSONAL DATA STORAGE IN RUSSIA

PART 1: LEGAL ASPECTS

Lead authors:
Igor Nevzorov, EY Russia
Mikhail Chentsov, Otto Group Russia

Contributors:
Anastasia Kuznetsova, EY Russia
Adrien Henni, East-West Digital News

Introduction

The new legislation forbidding storage of Russian citizens' personal data in foreign countries has posed new challenges to many foreign and domestic companies which store their users' data in borderless clouds. Not only do these companies have to organize data migration to Russian servers, they must also comply with the demanding Russian personal data legislation in its entirety, including its provisions on data collection, storage, use, and protection.

Compliance with this legislation remains one of the most important and sensitive issues when conducting or establishing a legitimate online business in Russia.

Originally based on the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981),[1] Russian legislation was subject to major changes in recent years. After strict regulations were introduced in 2011, the 2014 amendments forbid storage of personal data of Russian citizens in foreign countries.

Many legal and industry experts have provided negative feedback regarding the 2011 and 2014 amendments, underlining their formal defects and foreseeing a range of practical difficulties in their implementation.

Among the main criticisms to the 2011 amendments were the following:

- The law uses the main terms of international conventions – but unlike the national legislation in many European countries, it does not specify with sufficient detail or clarity the instruments necessary to enable compliance;
- The law establishes requirements for personal data processing that are very strict, often very costly and hardly adoptable without assistance from specialized companies with corresponding government licenses;
- The cost of implementation of these requirements, or of outsourcing them, may be considerable;
- The specificities of certain types of businesses are not taken into account – the requirements are the same for all, from banks to large companies to small businesses;
- A side effect of the implementation of this law, some argue, may be a significant increase in corruption in this field.

The 2014 amendments on storage location also triggered a wave of criticism in and outside Russia. Some panicked foreign players even saw in the new rules the beginning of the end to their digital business in Russia.

1. The Federal Law on Personal Data was enacted in 2006 after Russia's ratification in 2005 of the 1981 Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. However, in practice many provisions of the law had been put on hold and their effective implementation had been postponed several times. In the absence of clear regulations and requirements for personal data privacy, state agencies have equated personal data with secret government information. Despite a lack of adequate regulation, the provisions of the Federal Law on Personal Data came into effect as of July 1, 2011 in a very restrictive version.

There is also another important 2014 amendment that is connected more with storage of data than storage of purely personal data. Nevertheless, in the Internet business context it should be mentioned too. It refers to the so-called "bloggers law" – new provisions in the law on information and information technologies establish a number of limitations for information extension on the Internet and lay additional responsibilities on organizers of information distribution in the Internet.[2] Such organizers are obliged to notify the competent state authority (Roskomnadzor) about acting in this sphere and to store on Russian territory information on facts of receiving, transfer, delivery and/or processing of voice information, texts, images, sounds and other electronic messages and information about users during 6 months from the end of these actions.[3]

Far from ideological discussions, this chapter describes the different aspects of the current Russian legislation on personal data and provides practical recommendations to the concerned players to comply with it.

*

Companies dealing with personal data – including those operating from abroad – must comply with five fundamental rules. (These apply specifically to personal data, which should not be confused with any user-related data.)

1. **Personal data may be collected, stored and used only with the consent of the data subject** (the person the data refers to)**.** Where such consent cannot be obtained in written form, an operator should collect as much information as possible evidencing consent.[4]

2. **Data operators storing personal data are liable for keeping such data confidential and are not permitted to transfer, share or disclose such data without the consent of the data subject.** Moreover, special attention must be paid to internal control mechanisms over employees or agents handling personal data in order to avoid any violation of the law.

3. **Full protection of personal data should be provided through a range of organizational and technical measures defined by the law.** These requirements must be met without exception.[5]

2. According to the article 10.1 of the Federal law on information, information technologies and protection of information, "organizers of information distribution in the Internet" are the companies ensuring functioning of informational systems and/or software used or intended to be used for receiving, transfer, delivery and/or processing electronic messages of users in the Internet. Uncertainness of definition makes these rules essential to deal with when holding the Internet business.
3. Government decree of the Russian Federation d/d 31.07.2014 No. 759.
4. For instance, the checking of the box "I agree" during an online registration procedure could itself constitute evidence of consent; but the law does not explicitly state how consent should materialize, and to date there has been no legal precedent.
5. In the event of any doubts as to the validity of the chosen measures, interested parties may consult specialized agencies or experts (information security officers) to evaluate the effectiveness of the measures taken to guarantee personal data privacy; however, from a legal point of view such consultations cannot be considered a guarantee of compliance.

4. **The Operator should work out and make publicly available an internal policy for processing personal data.** This document is obligatory for all operators, and an operator may be held liable for failure to have it in place. On the other hand, detailed personal data processing policies help companies achieve their various objectives and comply with complicated personal data legislation.

5. **Starting from Sept. 1, 2015, personal data should be processed by means of information data bases that are physically located in the Russian territory.**

*

As for practical implementation, there are considerable differences depending on the type of business and database architecture. Certain business are not even affected by the law, if their activity is regulated by an international agreement or specific legislation – which is the case of air carriers and related ticket booking companies, as stated by the Russian authorities.

Until just weeks before the Sept. 1, 2015 deadline, implementing the new rules was difficult due to the lack of clarity and precision of the law in several important respects. Ambiguities remained regarding the scope of the law, the possibility of storing of copies of personal data outside Russia, the way to identify Russian citizens, and many other issues brought before the Russian authorities by the business community. Some statements from the authorities did concern some of these points, but they had no formal value.

In the months preceding Sept. 1, meetings with the regulator helped businesses clarify the situation. In August 2015, as a results of these meetings and of numerous requests from personal data operators, the Ministry of Telecom and Mass Communications (Minkomsvyaz) expressed its interpretations of the law on its official website. These statements are not legally binding, but may be regarded as guidelines provided to businesses to comply with the law in good faith.

According to these official interpretations, personal data initially collected and stored in Russia can be transferred abroad or processed in databases located abroad.[6] The key issue here, in order to protect the subject of personal data, is the initial location.

The questions of whether or not the law would apply to data collected before Sept. 1, 2015, has also been clarified. The rules are not retroactive; only personal data collected starting from Sept. 1, 2015 must be stored in Russia.

The Ministry of Telecom and Mass Communications also announced that the law will not apply to airlines and air ticket booking systems.

These clarifications, however, have not made the law less demanding. As a result, some players, including several important international companies, are considering leaving the Russian market due to these legal complexities and the unfavorable economic context.

6. See section 3.2. According to earlier statements by Roskomnadzor representative Vadim Ampelonsky, the duplication of personal data abroad was not regarded as possible http://top.rbc.ru/technology_and_media/05/02/2015/54d243839a794700b562da40

1. How the law defines personal data

According to the law, the primary characteristic of "personal data" is the ability to identify among many persons a specific, unique individual. For example, if only parts of someone's personal information are stored – for example, a person's name and paternal name (patronymic) but not his or her family name – this will not be considered personal data because it is insufficient to identify the person. In this case, the data will be considered impersonal and the law on personal data will not apply. Not every piece of information related to the individual qualifies as personal data.

- **Are email addresses and phone numbers considered personal data?**

The Federal Law on Personal Data did not address this question, even though the previous Federal Law on Advertisement prohibited the transmission of advertising messages by electronic means – including phone and Internet networks – to identified persons without their prior consent.

It is impossible to state unequivocally that email addresses and phone numbers fall within the definition of personal data as defined by the Federal Law on Personal Data. On the one hand, based on this definition, postal and email addresses are treated equally. On the other hand, a postal or email address may not be enough to identify a person. Therefore one can assume that an email address will not be considered personal data unless it contains in itself information that allows the identification of the concerned person (e.g. name.surmame@companyname.com) or if it associated with additional information that makes this identification possible – such as the person's family name.

- **Are there any special categories of personal data regulated by law?**

Russian personal data legislation, same as the basic provisions of the Strasburg Convention groups personal data into several classes with different levels of protection and the related obligations of the personal data operator. For example, the processing of certain special categories of personal data is generally forbidden: this includes information about the race, nationality, political opinion, religion and philosophical beliefs, health, sexual life and criminal convictions. Russian law establishes a wider list of special personal data categories than the Convention (including the purely philosophical category of philosophical opinions and beliefs).

- **What is biometrical personal data?**

Russian personal data legislation also introduces the category of biometrical personal data, which refers to the physiological and biological characteristics of the individual that make it possible to identify that individual. Biometrical data is used by operators for identification purposes (photo, video, body metrics etc.). The requirements for processing such data are stricter than even the special personal data categories mentioned before: in particular, there are fewer situations where such data may be processed without the personal data subject's consent.

- **Social networks: do they contain personal data?**

Blogs and social networks contain a huge amount of personal data that is usually made publically available by personal data subjects themselves. Meanwhile, this online business segment is exposed to a high risk of unauthorized use of personal data by both the operator and other users. This includes the problem of fake accounts in social networks like VKontake, Facebook or Instagram: we are aware of several cases where Roskomnadzor ordered the deletion of fake profiles from these networks upon the request of the subjects of personal data.

PRACTICAL GUIDELINES

Being aware of the legal status and requirements to the processing of special (or, in other words, "essential") personal data may be important, especially in such market segments as social networking, medicine or recruitment. As the general approach of both the law and state authorities is to protect the rights of subjects of personal data, these categories are more likely than others to be scrutinized by the state. That is why it is important to understand if there are any special categories of personal data obtained and processed by the operator, to check the legal basis for the processing, to obtain written consent of the personal data subject, or to stop all activities with such data to avoid negative legal consequences.

CCI FRANCE RUSSIE

FRANCO-RUSSIAN CHAMBER OF COMMERCE AND INDUSTRY

EXPERT CONFERENCE

"PROTECTING AND LOCALIZING PERSONAL DATA: RUSSIAN AND INTERNATIONAL PRACTICE"

Over the past decade, the infrastructure of global information has experienced an incredible rate of growth the world over. This leads to a massive accumulation of data, including personal. The complexity of providing adequate legal personal data protection, both globally and country-wide, increases with a comparable speed. In this situation it is very important to secure the balance of interests of individuals, whose data is being protected, with interests of the regulator while ensuring such protection.

Along with the adoption of amendments to the Russian law on personal data, coming into force September 1, 2015, the topic of protecting and localizing personal data has become extremely relevant and meaningful to the business community of Russia.

The conference will host representatives from Russian regulatory bodies, lawyers from major Russian and foreign law companies, representatives from the business community, as well as recognized foreign experts on the subject. They will discuss the challenges facing private Russian citizens and businesses, and will give practical advice on how to build a system for safeguarding data, while keeping a balance of personal, professional and public interests. They will also present global trends in the development of personal data protection and will share their experiences.

WHEN AND WHERE

- DATE: 16 October 2015
- TIME: 9am – 3pm
- VENUE: Hotel "Metropol" (2, Teatralniy proyezd, Moscow)
- LANGUAGES: Russian, French (simultaneous translation)

HOW TO ATTEND

- PRICE:

8,000 rub + VAT for members of CCI France Russie
12,000 rub + VAT for non-members of CCI France Russie

- REGISTRATION:

If you are a member of CCI France Russie please register through your personal account
If you are not a member of CCI France Russie, contact us on moncontact@ccifr.ru

2. Personal data processing

2.1. Notification of state authorities

Before beginning to process personal data, the operator has to notify the relevant state authority (Roskomnadzor) about personal data processing and provide them with the information required by law. Roskomnadzor keeps a special register of personal data operators and updates it for new information.

There are only a few exceptions to this rule, and the aspects relevant to the internet business are as follows:

- personal data is processed in accordance with labor legislation;
- personal data is processed to sign and execute a contract with an individual in the interests of that individual;
- the data processed has been made publicly available by the personal data subject;
- the data processing includes only the first and last name of the individual.

PRACTICAL GUIDELINES

While the above exceptions often do not cover all current and potential future personal data processing issues, we still recommend notifying Roskomnadzor. A notice template can be found on the Roskomnadzor website.

The Operator should also notify Roskomnadzor about any changes in the information related to personal data processing within 10 days of such change.

2.2. Data subject's consent

▪ Situations in which the data subject's consent is mandatory

The main and general condition for legal collection and processing of personal data is the data subject's consent for clearly indicated actions.[6] However, the Federal Law on Personal Data establishes several exceptions to this general rule, most of them applying to governmental bodies. But some of them are relevant to business entities too.

The first exception applies when personal data processing is required for *law-abiding operations of the mass media*, provided that a person's rights and lawful interests are not violated. This type of operation is rather rare for business entities because of the difficulty of obtaining the necessary license.

The second exception relates to the processing of personal data for the purpose of executing and formalizing a contract for a person in his or her interests. Described in this way, the exception may seem to offer considerable freedom – which may explain why some companies try to fit their business within this exception.

6. Should consent for personal data processing be provided by a representative of the personal data owner, the data operator must verify that the representative was entitled by the data subject to provide his or her consent.

However, the exception must be used very cautiously. For instance, if a company collects a data subject's personal data for the purpose of executing a retail purchase and sale contract, then it has a right to collect personal data without the data subject's consent. But such personal data can only be used within retail purchase and sale contract terms to notify data subjects of order status, to make deliveries to the address indicated in the personal information or to give refunds for non-quality products.

If a retailer intends to store the personal data in a special database and keep it after execution of the retail purchase and sale contract for future advertisement communications purposes or loyalty programs, or disclose it to third parties for advertisement purposes, then absence of the data subject's consent for further use of his personal data would be a serious violation of the law.

PRACTICAL GUIDELINES

The exceptions described above are limited and do not cover all business needs related to the usage and distribution of personal data to third parties (common practice in industries such as insurance and distance sales), so it is recommended that the operator obtain the data subject's consent for personal data processing beyond the contract execution whenever such data is stored in a database, regardless of the purpose.

▪ Forms in which the data subject's consent must be obtained

Consent for personal data processing must be provided in a conscious and voluntary way, excluding any pressure from a third party. For example, it is unacceptable to force data subjects making a purchase to consent to further use of their personal data, since such consent is not necessary to execute the retail purchase and sale contract.

The law recognizes the following types of consent:[7]

1. **Consent in written form with the data subject's signature.** This form of consent is mandatory when the data relates to the data subject's health status or biometric data. In the case of any commercial businesses, even though written consent is not formally required by the law, many data operators tend to request it as irrefutable evidence of a data subject's consent.

2. **Electronic document signed electronically.** Because of the difficult regulation of electronic signature use in compliance with the Federal Law on Electronic Digital Signature, it is unlikely that this form of consent will become widely used, especially by small and middle-sized businesses.

7. In the 2011 version of the law, an important principle was stated: consent for personal data processing may be provided by the data subject – or his authorized representative – in any form that allows confirmation of the fact of consent. This in fact means that the legislation concedes, though not explicitly, that consent may be provided in forms other than writing.

3. **Other forms of consent not outlined specifically in the law**: oral consent over the phone; online registration; electronic mail without digital signature; other forms of expression of will.

In the 2011 version of the law, an important principle was stated: consent for personal data processing may be provided by the data subject – or his authorized representative – in any form that allows confirmation of the fact of consent. This in fact means that the legislation concedes, though not explicitly, that consent may be provided in forms other than writing.

Introduced by the 2011 amendment to the Federal Law on Data Protection, the option to obtain consent in any other form that allows confirmation of the fact of consent provides an interesting opportunity for personal data processing. However, the law leaves unanswered the question of how the evidence of consent can be provided in the absence of the written form. The question is particularly sensitive for example in the case of distance selling, where the law states explicitly that personal data processing is illegal if the data operator fails to prove the data subject's consent for further personal data use.

Thus an interesting legal situation has been created. On one hand *(de jure),* there is no requirement for obtaining written consent; on the other hand *(de facto),* given current bureaucratic practice in Russia, in most cases the only evidence of a data subject's expression of will tends to be a written form of consent.[8]

Companies dealing with cross-border trade thus have to create and store information that confirms data subject consent. While this may be difficult for many market players, especially the small ones, all major companies working on the Russian market try to obtain a data subject's consent in both oral and written form in order to minimize possible legal and administrative risks.

The most widespread "other forms of consent" are electronic, with fields filled in upon registration on a website or completion of an order placement in an online store. But such electronic procedures must be designed taking into account specific legal requirements.[9]

8. It is impossible, of course, to prove with 100% certainty a data subject's provision of consent for his personal data processing, even if such consent has been provided in writing. A data subject can always claim that the application or questionnaire was filled out by someone else, that his passport information was written down without his will, etc.

9. In particular, it is important to remember the following rules:

a. When creating fields of personal information on Internet websites for online completion, it is necessary to provide fields not only for the client's name, surname, paternal name (patronymic) and address, but also for the name and address of the data operator obtaining the person's consent; the purpose of the personal data collection; a general description of the personal data processing methods used by the data operator; the expiration date of the consent; and the terms of consent withdrawal.

b. Obtaining consent for personal data processing should under no circumstance be "disguised." The person should not be misinformed about a mandatory requirement to obtain such consent for placing an order. A disclaimer must be easily available and readable on the website and such consent must be the person's free act and deed.

c. Uploading information with personal data to a server and its storage in an automated information system require a series of organizational and technical measures to ensure the protection of said data, as discussed further.

PRACTICAL GUIDELINES

The choice of the form in which the personal data subject's consent is to be obtained should take into account the specifics of the business, size of the company, structure and characteristics of the data being processed. A consent obtained by electronic means does not release the operator from any legal requirements, nor does it constitute a waiver of any of the personal data subject's rights. The operator should store all information related to obtaining such consent in case of potential disputes with personal data subjects or state authorities.

2.3. Other rights of data subjects

As long as one of the most important purposes of legal regulation of personal data processing is to guarantee and respect human rights, there is a number of rights the subjects of personal data have and the corresponding obligations of companies dealing with personal data. In addition to the need to obtain consent to the processing of personal data, there is another important right, which is the right of the data subject to gain access to his or her personal data.

Some aspects of this right should be kept in mind:

- Upon request, the personal data subject should be provided with the personal data processed in respect to that individual and information related to the processing.
- The personal data subject may send a repeated request not earlier than 30 days after sending the last request.
- The personal data subject may send a repeated request on an earlier date if the information provided under the previous request was incomplete.
- The personal data subject may request that the operator update, block or remove personal data if the data is incomplete or not updated, is inaccurate, or obtained in violation of the law or processed for purposes other than those declared

PRACTICAL GUIDELINES

The following information should be provided by the operator:

- Confirmation of the fact of personal data processing;
- Processed personal data and information about the source of data
- Legal grounds and purposes of personal data processing
- Methods of personal data processing
- Name and address of the operator and information about the persons (except employees) who have or potentially could have access to the personal data
- Conditions of personal data processing, e.g. storage
- Procedure of exercise of the personal data subject's rights
- Information about the actual or proposed cross-border data transfer
- Name and address of the third party processing personal data under an agreement with personal data operator

Providing updated and complete information is important for general compliance with personal data legislation: this way you will avoid early repeated requests from the personal data subject, or will have legal grounds to refuse an inappropriate repeated request, or have reasonable legal position in case of a dispute with the data subject or state authorities.

2.4. Data collection methods

The term "collection of personal data" falls under the general definition of "processing of personal data" and is therefore not regulated separately. Practically, the term "processing of personal data" includes the actions of a data operator in collecting information containing personal data, either directly from individual persons or from third parties who obtained personal data legally. Personal data can be collected in various ways, from questionnaires or discount card applications filled by data subjects to the acquisition of a database formalized by a contract.

Although not addressing in complete detail the process of personal data collection, the Federal Law on Personal Data provides a basis for legal analysis.

Three main data collection methods can be distinguished:

1. **Direct obtainment of personal data from data subjects** by phone, in written form, via a web interface or other means directly related to the core activity of the data operator.

2. **Collection of personal data through marketing actions,** from enrollment in a discount or loyalty program to participation in a contest or a lottery; a variety of tools can be used to collect personal data when the provision of information is motivated by a material advantage, such as a discount or a chance to win something. Legal requirements for personal data collection in this case are the same as for direct obtainment, but one should take into account Russian legislation on marketing activities.

3. **Receipt of personal data from a third party,** either through the acquisition of a database containing personal data or through the collection of personal data via the third party's means without database acquisition.

▪ Acquisition of a database containing personal data

To minimize legal risks, the acquirer should, in particular, take into account the following recommendations:

- First, the acquirer should verify that the owner of the database is a data operator of personal data in the legal sense of the term, which implies inclusion in the special registry of the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (Roskomnadzor).[10]
- Second, even before signing the contract one must verify that the owner of the database has been permitted by the data subjects to use their personal data and ***transfer it to a third party***. From a legal point of view, it is important that the contract between the owner and the acquirer of the database mention and guarantee data subject consent.[11]
- Third, before processing personal data received from a third party, the acquirer of the database must inform the data subjects of his name and address; of the purpose and legal basis of the prospective use of the personal data; of the identity of potential users of the personal data; of the rights of the data subjects' regarding the use of their data; and – as per a new norm in 2011 – of the identity of the data operator who initially collected and transferred the personal data.[12]

3. Use of personal data

3.1. Use of data on Russian territory

The 2011 amendments to the Federal Law on Personal Data incorporated the term "use of personal data" into the general definition of "processing of personal data," without separate definition of this term. Therefore it is advisable to use the definition provided in the previous edition of the law – any actions or operations on personal data performed for the purpose of decision-making or execution of other actions resulting in legal consequences for the owner of the personal data or of another person, or affecting in any other way their rights and freedoms.

In other words, the use of personal data includes the distribution and sharing of as well as access to such data – along with many other actions that could result in consequences for the data subject.

10. This can be checked easily on the website of Roskomnadzor http://www.rsoc.ru/. In a dedicated section, one may enter the name of the data operator, or his INN identification number. The database offers legal information on the data operator, including the date of entry into the registry, as well as the category of personal data and the methods and purpose of their collection and use.
11. Unless it is expressed in written form, a data subject's consent cannot be fully confirmed. But the contract may include a clause that guarantees the existence of a data subject's consent, specifies that the owner of the database is ready to confirm it upon demand and that it takes full responsibility (indemnity) in case of any claim from data subjects, third parties or government bodies.
12. This implies that the acquirer of the database must at least include this information in the first message sent to the data subjects. In addition, it is arguably better to request once again the data subjects' consent for the use of their personal data in the form of a disclaimer, since one cannot be 100% sure that this consent was initially obtained in due form.

For commercial companies, this translates into any actions with personal data that could help gain financial benefits from the data subject. This notably includes sending commercial offers to the data subjects (potential clients); exposing them to customized or personalized advertisements; sharing the personal data with a third party by selling the rights to a specific database; and allowing the collection of personal data by third parties through communication channels owned by the company.

The main condition for the use of personal data in compliance with the Federal Law on Personal Data is the data subject's consent, which may be obtained either in written or any other willful form in compliance with all legal requirements.[13] The list of activities for the purpose of personal data processing must be announced to the data subject at the moment of obtaining consent for personal data processing. For example, this list can be provided in a disclaimer signed by the data subject.

3.2. Cross-border use of personal data

While storage of personal data on servers located abroad was allowed with some restrictions so far, the new rules adopted in 2014 demand that, starting from Sept. 2015,[14] only servers located physically on the Russian territory be used for such purpose.

According to new legislation, a range of activities involving personal data – including collection, recording, systematization, accumulation, storage, update, amendment and retrieval of personal data of Russian citizens – should be performed through databases located in the Russian Federation.

Explicit exceptions to this restrictive approach are few; they all relate to the activities of state authorities, public interests as well as media, scientific, literary or other creative activities, as well as to the fulfillment international agreements (for example, in air ticket booking services.) There is no exception for any other categories of personal data operators based on, e.g., market segment, business line, size etc.

Despite the lack of specific and plain requirements for personal data operators and the lack of concretization in official regulations, many provisions of the law have been clarified on the official website of the Ministry of Communications and Mass Media.[15]

13. All types, forms and exceptions related to the obtainment of consent for the processing of personal data are listed in section 2.2. In the sense of the law, the term "processing" includes both use and collection of personal data.
14. The initial text, adopted in July 2014, made data storage on domestic servers mandatory starting from *September 2016.* In September 2014, the Russian parliament considered setting the deadline at *January 2015.* The short period left was so obviously unrealistic for most of the concerned companies – including key Russian players in the airline and insurance industries – that the final deadline was set at *September 2015.* http://www.ewdn.com/2014/12/26/personal-data-storage-on-russian-servers-will-be-mandatory-starting-from-september-2015/
15. http://www.minsvyaz.ru/ru/personaldata/#1438548328715

1. The law did not specify whether foreign companies without a physical presence in Russia would be affected by the law. The answer is yes, as clarified by the Ministry: the legal requirements do apply to any organization targeting Russian audiences. This may be reflected by the use of such domain name extensions as .ru, .su, .moscow, Russian-language advertisements, online transactions executed with the Russian currency, etc. Theoretically, the requirements to store personal data in Russia even applies to such businesses as hotels hosting Russian citizens in other countries.

2. As the law law does not contain any definition of "primary data collection," the obligation to record, systematize, accumulate, store, update, amend and retrieve personal data using databases located in Russia applies wherever the data is collected.

3. While recorded and stored primarily in servers located in the Russian territory, personal data may still be accessed from abroad, or transferred abroad according to cross-border data transfer rules. Thus Russian citizens' personal data may be processed in databases located outside of the Russian Federation provided that any newly collected data is primarily stored in Russia, and that the major or equal part of such data is still processed in databases located in the Russian Federation. In such cases, all the data stored abroad should be simultaneously stored in Russia.

4. The question of how exactly the citizenship of users can be determined is to be resolved by each operator of personal data.

5. According to the ministry's position, the law does not impose any restrictions for Russian citizens using any services outside of the Russian Federation in case their personal data are processed outside of Russia, in compliance with international agreements or federal legislation or within another explicit exceptions provided by law. Provisions of the Russian personal data legislation do not legally bind non-residents organized and acting in other countries.

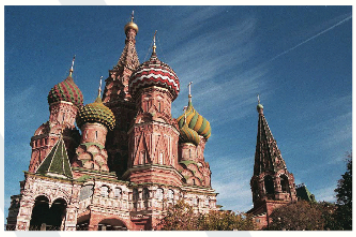
PRACTICAL GUIDELINES

Personal data operators must notify Roskomnadzor about the particular location of their information databases, be it in the notification about the start of personal data processing or in the notification sent to update the information contained in Roskomnadzor's register of personal data operators. The notification updating the information already included in the Register should be sent not later than 11 September 2015 since the obligation comes into force on 1 September 2015 and the operator has 10 days to notify Roskomnadzor about any changes in personal data processing.

RUSSO-BRITISH CHAMBER OF COMMERCE

THE BRIDGE BETWEEN BRITISH AND RUSSIAN BUSINESS

Through its offices in London, Moscow and St Petersburg, the RBCC has worked continuously since 1916 to give practical help to British and Russian Member companies in establishing and developing their contacts and enterprises in both countries.



With senior representation at Advisory Council and Board level from both UK and Russian business, the RBCC is uniquely well-informed. Busy programmes in both countries include a range of events from business networking evenings and industry seminars to conferences, including our annual flagship events – RBCC Business Summit in London, RussiaTALK Investment Forum in Moscow and Retail Conference in St Petersburg.

The Chamber's quarterly magazine, RBCC Bulletin, highlights the major business and economic trends in the UK and in Russia, and offers access to an audience of over 6,000 business and policy leaders in both Russia and the UK. The weekly e-mail newsletter, RBCC Observer, provides a convenient source of information for business readers interested in becoming part of our network, expanding their horizons and exploring new opportunities.

Contact us:

LONDON
11 Belgrave Road,
London, SW1V 1RB
Tel: 0207 931 6455
Fax: 0207 233 9736

MOSCOW
Office A 604,
'Galeriya Aktyor'
Moscow. 123056
16/2 Tverskaya St,
Tel.: +7 (495) 961 21 60
Fax: +7 (495) 961 21 61

ST PETERSBURG
Ostrov Business Centre
36/40 Sredny Prospekt,
Vasilyevsky Island,
St Petersburg 199044
Tel +7 812 327 80 45 ext 218

www.rbcc.com

4. Organization of data processing and protection of personal data

Companies storing and processing personal data must comply with a variety of requirements to organize the processing and to protect them.

These requirements are the following:

- An employee of the organization must be appointed as responsible for the processing of personal data;
- The awareness of the current status of personal data legislation among employees dealing with personal data must be ensured;
- The organization's policy regarding personal data must be laid out in documents made easily available to persons and data subjects (for example, on the organization's website);
- Legal, organizational and technical measures for personal data protection must be undertaken along with measures to control the effectiveness of personal data protection and the level of protection of the information systems involved;
- Certified personal data protection tools (software and hardware) must be used; tools already in use should be certified;
- Internal control policies to ensure the compliance of personal data processing with applicable legislation must be defined and applied;
- Any "damages" – a term as yet undefined in law – that could potentially be caused to the data subjects by misuse of their personal data must be assessed;
- Potential threats to personal data security must likewise be assessed;
- Physical carriers of personal data must be registered;
- Instances of unauthorized access to personal data must be made known and appropriate measures taken;
- In case of alteration or deletion of personal data as a result of unauthorized access, the data must be restored;
- The organization must define access rules to the information system where personal data is processed. All actions performed with personal data in the system should be recorded.

Such requirements make compliance with the law a complicated matter. While small organizations may not have employees specializing in information security who are sufficiently trained to meet these requirements, outsourcing the implementation of these measures can entail considerable expense.

18. For large organizations, the cost for these services can range in the hundreds of thousands of USD.

PRACTICAL GUIDELINES

The 2011 amendment to the Federal Law on Personal Data requires that data operators publish a document outlining their personal data policy. A detailed policy should contain the description of measures related to personal data processing, ways of communication with third parties, personal data subjects and state authorities and other substantial provisions on the organization of data processing. An absence of such policy on the company's website could result in a liability for the operator.

Also important is the fact that the term "personal data" has been legally equated with the term "confidential information" by the Russian government. Fulfilling the requirements of the Russian Federal Service for Technical and Export Control (FSTEC)[19] related to personal data protection therefore requires a specific license.[20]

Outsourcing these operations is, de facto, the only way to avoid a number of problems related to applying for this license – and the even more acute difficulties that may arise with FSTEC inspectors in the absence of the license. The law treats activities carried out without the appropriate license as criminal offenses.[21]

It is highly recommended that the provider who will deal with the personal data be chosen with great care. In particular, it is important to verify that the provider is listed in the Roskomnadzor registry of personal data operators (see Section 2.2) and possesses the required FSTEC license. It is also important to verify that the software and hardware tools used by the provider for information protection are duly certified.

▪ Relationships with third parties related to personal data processing

Compliance with personal data legislation in some situations requires an attentive and responsible approach to the relationships with third parties.

There are three possible data transfer scenarios:
- obtaining personal data from third parties that are not the subjects of the personal data;
- transfer of personal data to third parties as part of the personal data operator's operations;
- outsourcing personal data processing services.

19. For further information on this authority see: www.fstec.ru.
20. "License for activities related to the technical protection of confidential information" *(Лицензия на осуществление деятельности по технической защите конфиденциальной информации)*
21. Some have suggested that such a license should not be required if the organization conducts these activities for its own internal use. However, the FSTEC – the authority that issues such licenses – has clearly expressed its position: the license is required in all cases. This was also confirmed by the new Federal Law on Licensing Particular Activities, adopted in May 2011. Meanwhile, the 2011 version of the law on personal data has made necessary the obtainment of data subjects' consent for the transfer to a third party of operations related to personal data processing and protection. In the case of written consent, the name and address of the third party must be specified. The requirements related to personal data security are retained, but the responsibility is borne by the data operator, the third party being liable only to the data operator.

As the personal data operator is ultimately responsible for the processing, it is important to ensure that third parties comply with all requirements to personal data processing.

Outsourcing personal data processing services is possible upon consent of the personal data subject on the basis of agreement. There are several requirements to this agreement – it should contain a list of specific services that are outsourced to the third parties, state the purposes of processing, obligations of the third party, ensure safety of the personal data and set out the requirements to the protection of personal data.

PRACTICAL GUIDELINES

An agreement with a third party should contain detailed obligations of the third party to fulfill all legal requirements and liability provisions of the third party in case of their violation.

5. Liability for violation of conditions of personal data processing

At least seven government bodies may be involved in ensuring that personal data is collected and used in compliance with the law – the FSTEC, Roskomnadzor, the Ministry of Communications and Mass Media, the Federal Security Service (FSB), the Interior Ministry, and the Prosecutor General's Office and the Investigative Committee.

Violators of the law on personal data bear civil, criminal and/or administrative liabilities.

5.1. Civil, criminal and administrative liability

Coming in addition to the Civil Code's clauses on privacy, personal and family secrets, honor, good name and reputation, the new law on personal data stipulates that moral damage in relation to personal data use must be compensated.

Article 137 of the Russian Criminal Code provides for liability to a fine of up to 200,000 rubles and detention up to 4 months, or imprisonment of up to 2 years, for the illegal collection, dissemination or publication of information about a person's private life.

Moreover, the unlicensed operation of a business involving the technical protection of confidential information, in cases when such a license is necessary – if this activity causes significant damage to private persons, legal entities or the government, or if it generates large-scale profit – is punishable by a fine of up to 300,000 rubles or imprisonment for up to 5 years in extreme cases, in accordance with Article 171 of the Russian Criminal Code.

The Russian Administrative Violation Code prescribes penalties of up to 20,000 rubles and temporary suspension of the violator's related business activities for cases of violation of the law in relation to the collection, storage or use of personal data, or in cases of use of non-certified means of protection of personal data.

On 22 December 2014, a draft of new administrative liability provisions was proposed to the State Duma by the Russian Government.[22] The proposed amendments to the Russian Administrative Violation Code specify particular violations such as:

- Violation of requirements to the scope of information to which the personal data subject's consent to the data processing should contain (with proposed amount of fine for companies from 15,000 to 50,000 rubles);
- Personal data processing without personal data subject's consent or any other legal conditions of data processing (with the proposed amount of fine for companies from 30,000 to 50,000 rubles);
- Processing of special categories of personal data in cases not described in personal data legislation (with the proposed amount of fine for companies from 150,000 to 300,000 rubles);
- Non-fulfillment of the obligation to publish the operator's personal data processing policy document and information about the means used to protect personal data (with the proposed amount of fine for companies from 15,000 to 30,000 rubles);
- Non-fulfillment of the obligation to provide the personal data subject with the processed personal data and information about processing (with the proposed amount of fine for companies from 20,000 to 40,000 rubles);
- Non-fulfillment of the data subject's or state authorities' request to update, block or remove personal data if the personal data is not full, outdated, illegally obtained or does not correspond to the declared purposes of the processing (with the proposed amount of fine for companies from 25,000 to 40,000 rubles);
- Non-fulfillment of the obligation to ensure security of personal data where personal data is stored on physical media (with the proposed amount of fine for companies from 25,000 to 50,000 rubles).

5.2. Register of violators of personal data subjects' rights

The 2014 amendments are also heavily focused on the procedure for limitation of access to the information processed in violation of Russian legislation.

Provisions on a legal basis of such limitation and corresponding actions of Roskomnadzor and other subjects participating in website functioning (site owners, hosting providers and telecommunication operators) were implemented into the law of information and information technologies and will come into force simultaneously with the new requirements for data storage.

22. http://asozd.duma.gov.ru/main.nsf/(Spravka)?OpenAgent&RN=683952-6

The necessary condition of launching the limitation procedure is a court decision in which the personal data law violation on a particular website is stated. Roskomnadzor at its own initiative or upon request of the personal data subject includes the website in the register and initiate the procedure of limitation by informing the hosting provider about the court decision with the designation of current domain names or web addresses. The hosting provider should inform the site owner about the decision and the requirement to stop the violation. If the site owner fails to take appropriate steps, the hosting provider will have to limit access to the infringing website. If the hosting provider fails to take action, it should be taken by the telecommunications operator.

PRACTICAL GUIDELINES

Inclusion on the Register of Roskomnadzor as well as limitation of access even for a short time may cause reputational and economic damage. As the only "sign" for Roskomnadzor is the court decision, immediate execution of such decision is crucial for companies to avoid the negative consequences of violating the personal data law..

5.3. Practical consequences

In practice, violation of the law may lead to one or several of the following consequences:On 22 December 2014, a draft of new administrative liability provisions was proposed to the State Duma by the Russian Government.[22] The proposed amendments to the Russian Administrative Violation Code specify particular violations such as:

- The personal data processing activities being carried out in violation of the Federal Law on Personal Data may be suspended or terminated;
- The matter may be referred to the prosecutor or other law enforcement bodies, which can decide to prosecute the offenses;
- The licenses related to the processing of personal data can be suspended or withdrawn;
- Non-certified information protection tools may be confiscated;[23] and
- Prosecution for administrative and criminal liability of those guilty of violating the respective codes of Russia.

Thus, in order to avoid possible complications or prosecution resulting from violations of the Federal Law on Personal Data, companies dealing with personal data should see to it that they are in full compliance with the three fundamental rules mentioned at the beginning of this discussion.

23. Given the fact that certain security mechanisms are integrated into system-wide applications, in some cases there is a possibility of confiscation of those servers and workstations that process personal data.

6. Recent legislation amendments and case law related to personal data protection

Recent case law clearly illustrates current trends in personal data protection by the Russian courts.

6.1. Main legislation amendments

One of the most significant amendments has been the recognition of the jurisdiction of Russian courts to hear cases of personal data infringement initiated at the *claimant*'s location.

Previously the general rule in effect was that such cases could be adjudicated only at the location of the respondent. Such an amendment will afford all owners of personal data simpler legal recourse against the infringement of their privacy – particularly when the location of the infringer is unknown or the infringement was committed via the Internet – as well as enhance the adoption of timely injunctions against infringers.

Another new provision is connected with the abovementioned situation of processing personal data without the data subject's consent – the fulfilment of an agreement with the data subject. The rule now expressly states that the personal data operator has the right to process personal data in exercise of its right to transfer the agreement to a third party.

Other recent legislation amendments were not related to e-commerce or Internet activities. They included the determination of legal mechanisms for personal data processing within mobile number portability (MNP) statutes, and the itemization of the obligations of various major public authorities and entities relating to personal data processing.

6.2. Case law tendencies

Irrespective of the seven-year period of personal data protection in Russia, existing case law offers only meager examples of successful claims against infringers. At present most of this case law is related to cases initiated by state authorities monitoring the compliance of Russian companies with personal data requirements and resultant disputes over whether legal entities have properly performed all necessary measures to secure the secrecy of counterparties' personal data.

Official reports of Roskomnadzor show that the most common parties to enter court proceedings are credit organizations, housing and utilities companies, website owners, debt collectors and telecom operators.

Meanwhile, in comparison with foreign case law, neither Russian state arbitration courts nor Russian courts of common jurisdiction can yet count a sizable number of cases based on the claims of personal data owners against third parties unauthorized to process such information. And those few claims that have in fact been filed by personal data owners have usually been unsuccessful in the courts, presumably due to a low level of judiciary initiative, judges' unwillingness to resolve such cases in favor of claimants and to the undemonstrated *locus standi* of claimants.

In any event, at present it is fair to say that in normal practice the liability of an infringer for a violation of personal data law against a claimant in Russia is too low to consider such claims a significant threat to the infringer's business.

Even though the latest legislation amendments have demonstrated a willingness on the part of Russian state authorities to strengthen personal data protection, it is likely that Russian case law will need as least several more years of accumulated precedent to raise the significance of personal data protection cases to the level enjoyed by European Union countries.

(March 2015)

- The leading independent financial and corporate communications agency in Russia/CIS
- The only agency in Russia to offer a fully integrated PR and IR offering
- Deep sector expertise – tech, retail and consumer, banking and finance, industrials, utilities, infrastructure, oil and gas and oil services, metals and mining
- Our team has advised on more M&A, IPO's and other capital market deals than any other team

Em

More professionals dedicated to Russia and CIS than any other international agency

- We work with public companies and help them with their on-going IR and financial market communications
- We work with privately held companies who have an eye on international and financial markets
- We help companies with their communications and risk management in times of conflict and crisis
- We help international companies to manage their reputations in Russia

Financial PR, investor relations, IPO and M&A transaction support, crisis communications, reputation management, strategic advisory

Contact details: / info@em-comms.com / Moscow: +7-495-363-2844 / London: +44-20-7920-2364

PERSONAL DATA STORAGE IN RUSSIA

PART 2: IMPLEMENTING DATA MIGRATION

Authors:
Dmitry Fokin, IXcellerate
Julia Shelygina, PayU

Contributor:
Pavel Marceux, East-West Digital News

How to organize data transfer to Russia

By Dmitry Fokin, Managing Director, IXcellerate Moscow Datacentre

Moving data to Russian servers, in compliance with the personal data storage law, can be a hazardous and complex process. Dmitry Fokin has developed an 8-point practical guide and a timeline that spells out the necessary steps to consider when committing to data migration to Russia.

1. Choosing the right partner

Choosing the right partners for installation and transition is an essential element, but even more important is choosing the partner to host and take care of the equipment for the years to come. The equipment purchasing and installation troubles will be resolved in weeks, but business operations will continue to rely on the data center infrastructure and team and this is the essential part. The key words here are Trust, Reliability and Responsiveness.

In selecting the partner to operate in the unknown and not always transparent environment, it will be a mistake to rely purely on spreadsheet-based checklists and questionnaires, infrastructure descriptions and even acclaimed certificates. All of these can be manipulated and unfortunately it is not infrequent in Russia to grossly misrepresent information about the data center size, resilience level (tier) and other critical operational aspects.

Furthermore, a number of data centers are operated by licensed telecom operators, while claiming carrier neutrality, which might result in higher connectivity costs and risks. Finally, Russia is ranking high amongst the countries with most corrupt business practices, with data center industry being no exception and some larger-scale scandals recently hitting the public realm.[1] Considering multi-million penalties that the clients will face back home, if caught in engaging such stories, it is a good idea to invest a few thousand dollars into sending over an independent international team to run the selection process. Seeking documented evidence of an anti-corruption policy within your supplier can help reduce some risk.

1. In 2014, Russia ranked 136th in Transparency International's Corruption perceptions Index. https://www.transparency.org/cpi2014/results. Among the recent scandals were those involving Cisco http://www.buzzfeed.com/aramroston/cisco-kickbacks-russia#.djrvNVj15, and system integrator Krok with Sberbank http://www.vedomosti.ru/newspaper/articles/2014/05/19/kak-sberbank-mogli-obschitat-na-200-mln

Therefore, when looking at the data center provider selection in Russia, an international client will benefit by thinking of the key things that make their data center experience excellent back in the home country. They will undoubtedly include such things as: security, confidentiality, service excellence, ownership transparency, carrier neutrality and, of course, infrastructure quality.

It is these features that you need to be looking for in the first place, and this, combined with proper technical due diligence, will make your experience in Russia just as great

2. Cooperative working on technical solution during pre-sale phase (from 1 to 6 weeks)

Once you have chosen a partner, dedicated project teams on both, client and data center, sides are imperative for effective management of the IT infrastructure transition process, so it is highly recommended the client forms a task team to run the project and makes sure there is a dedicated team on the data center side as well.

Most of the time the technical solution, which includes type, configuration and amount of server equipment, as well as network layout, is driven by client requirements and – especially in larger corporations – often has a globally stipulated standard. For efficient planning process, it is necessary to have as detailed and structured specification from client as possible, not only on the equipment, but also on other features, such as sever rack layout, security, environment, needed support services, etc.

Once this is clearly defined, the next set of questions is related to procurement of the equipment to the data center. Key considerations here are: delivery logistics, timing and cost. Since timing is of importance, it is highly recommended to use existing import channels.

Usually the data center will have a number of reliable and previously tested partners to recommend to the client to choose from. These should be large local business integrators, or international suppliers who have dealer network in the country. Business integrators have a one-window advantage, but will usually charge a premium to equipment manufacturers. Other options, such as procurement by the client's own team, while appearing less expensive, present a significant risk in terms of reliability and timing.

An important question to address is equipment ownership. For different reasons, not every client has an ability to own (purchase and keep on the books) equipment it is planning to use in Russia. In that case, there is a number of alternatives (from leasing contracts to pure service provisioning) that need to be explored together with the data center team, and it is important to consider this aspect from the project outset as well.

Finally, it is useful to understand whether the client wants to contract for services within Russia or with an internationally-based company that contracts back-to-back with local data center. Very few Russian data centers can offer such option, but it is available and has many legal benefits. Therefore, legal team also needs to be involved in the project.

3. Finalization of commercial terms and signing of contract (from 1 to 4 weeks)

Based on the installation size and Scope of Work prepared during the planning stage, the Client should receive a standard commercial proposal and standard contract, including service level agreement (SLA) terms and Service Order specifying all the deliverables. Some data centers do not have formal SLAs, so it is a good idea to ask up-front to review the document. Depending on client internal policies and procedures, the contract revision process can take different time. In some instances the client will have policies that stipulate how certain risks and situations must be addressed in the contracts, which will require additional revisions on both sides.

There is also an issue with differences in laws between countries, so certain contract clauses may be difficult to mirror exactly as they are in the client's home country. For the sake of time saving, this may be another reason to contract with client's international partner. Alternatively, it is advisable to hire local lawyers that have knowledge of international law to review the contract.

Local data centers with international ownership have an advantage here since they already incorporate the common international standards into contract terms. If you consider dealing with a Russian company, check it twice that these requirements are met in the contract.

4. Equipment ordering (from 1 to 3 weeks)

It is advisable to involve equipment suppliers during the planning stage, which eliminates uncertainties with logistics, costs and delivery timelines. In that case equipment order stage will most likely be an accounting exercise and take little time. If negotiations with suppliers are not part of the early stage planning, there may be surprises with project timing and cost. During equipment ordering it is a good idea to check supplier stock and make sure the equipment being ordered has been certified for use in Russia.

5. Delivery (5 to 8 weeks)

Delivery of equipment – especially in larger installations – needs to be coordinated in advance. Different pieces of equipment will be arriving separately and some equipment commissioning and installation work can be taken care of while other equipment is still en-route, for the sake of time saving. Since temporary storage and equipment assembly facilities at the data centers have limited capacity, it is a good idea to plan the process in such a way that equipment does not end up sitting in the storage area, generating additional costs for the client.

Security control over client equipment that is not yet installed is an important aspect to check with the data center. Optimally, there will be no uncontrolled access by third parties to client equipment being stored. This is where storage becomes costly (after the allowed free-of-charge storage time expires) and, therefore, the whole process needs to be pre-planned. Data center facility managers should be able to lead this discussion and raise the question during the planning stage.

6. Installation (1-3 weeks)

Installation can be carried by client's own team, data center team, business integrators or equipment manufacturers. Often a combination of these is used, adding complexity. Installation procedures need to be defined and the critical success factor here is having one coordination point, which is usually the data center team, working closely with the client and suppliers. If there are no particular arrangements, such as global discounts on installation work by equipment manufacturers, it makes sense to outsource the whole process to either a local business integrator, or the data center team. Both options should be reviewed, ideally, to optimize cost.

Another critical element is to make sure there is full transparency and understanding of the installation design by all parties involved. Language barriers and terminology can create a nightmare out of this one. But – if that has not been done during the planning stage – rack schematics and drawings, floor plan, equipment and cabling labeling conventions need to be mutually agreed and meticulously followed. Otherwise testing can take a lot longer, revealing installation mistakes and delaying the service launch. If client has in-house conventions for rack layout design and labeling, the data center team should be able to understand and adopt them, while keeping its own records as well, ensuring consistent control of data center infrastructure. If the client does not have own requirements, data center methodology can be used as a basis.

7. Testing configuration (1 day to 2 months)

As with all the other steps, duration of testing stage is dictated by complexity and size of the technical solution. There may be equipment and software configuration issues that need to be resolved via distant access by client teams, or locally; there may be issues with how the equipment has been cabled (if specification was not accurately done). Other issues are far less common and usually revealed during the delivery stage (i.e. equipment damage or defects), but can also take substantial time.

8. Launch

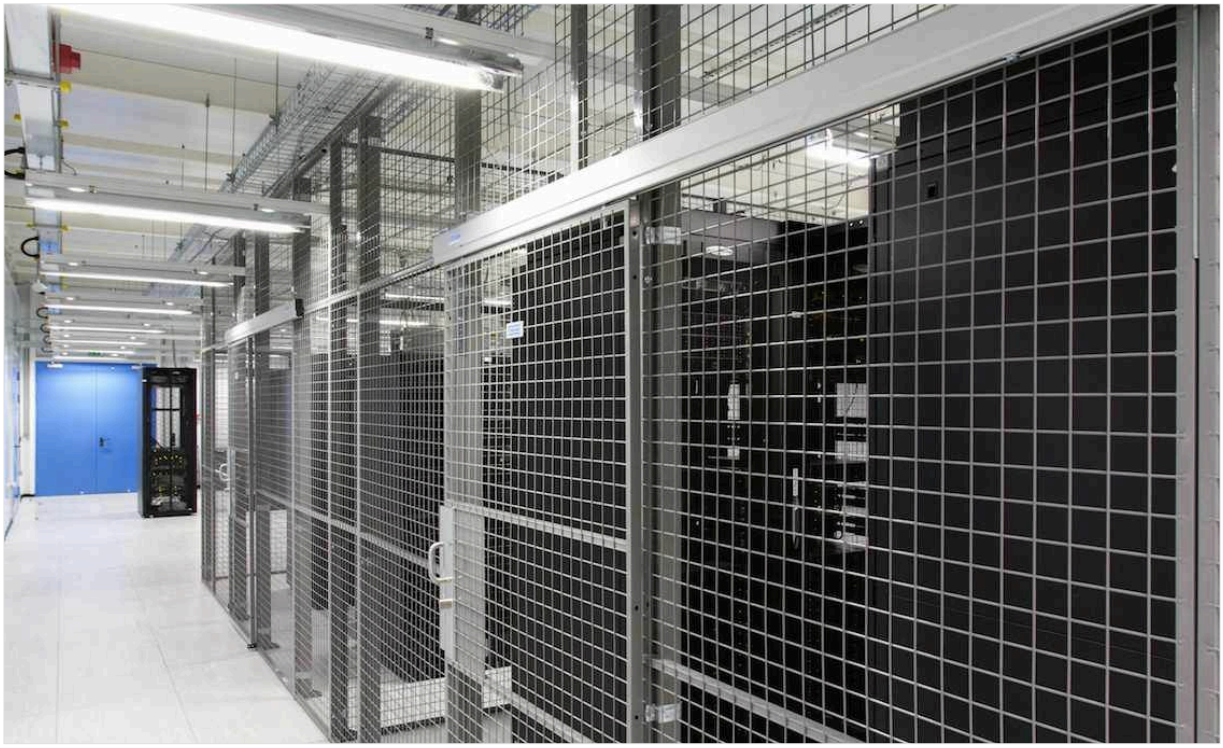
Getting to this stage is a factor of how the previous work was done, but launch is obviously more than a push of a button. There will often be a lot of questions in the first few weeks of operation and it is a good idea to make sure the data center team and other parties that participated in the process are on stand by to quickly react to any client requests. A properly run data center will have client service thoroughly specified, with procedures, documentation, 24-hour bi-lingual emergency phone line in place and online ticketing system to track status. But, given regular work pipeline any mature data center will have, it is advisable to reserve several hours of remote hands priority service for the first month, or for the entire contract period.

Data centers will often offer a fixed fee for the month, depending on estimated number of hours and make a discount on the hourly rate in comparison to the price-list used for ad-hoc service requests.

(February 2015)

A unique Marioff's HI-FOG fire suppression system is safe for the environment, humans and the equipment. VESDA early warning system allows prevention of fire at the very earliest stages. The BMS sensory system allows continuous monitoring of the data center's condition. (Photo credit: IXcellerate)

The area is regularly patrolled by security personnel. Log of incidents is kept and visitors' arrival and movements around the facility are strictly controlled.



IXcellerate provides tailor-made client solutions with a range of additional services. For instance, servers can be installed in racks or in high-security cages

TOP 5
Data Migration Tips

1 Give yourself a large timespan to fully implement the migration process

Just the delivery of servers itself can take up to two months alone while testing after installation can also amount to several months, amounting to a process that can easily stretch up to eight months.

2 Find a reliable local partner to assist you with the process. Involve head office team into selection process.

3 Use existing import channels to move equipment

Usually your Russia-based data center will have a number of reliable and previously tested partners to recommend. These should be large local business integrators, or international suppliers who have a dealer network in the country.

4 Manage complexity by transparent communication: make sure there is full understanding of the installation design by all parties involved

Language barriers and complex terminology can create major problems between client and contractor in this regard.

5 Don’t forget about after-migration support: data center team and other participating parties should be on stand-by after launch

A properly run data center will have client service thoroughly specified, with procedures, documentation, a 24-hour bi-lingual emergency phoneline in place and an online ticketing system to track status.

MOSCOW ONE DATACENTRE

MOSCOW ONE ДАТА-ЦЕНТР

- Your data in Moscow
- Compliance with Information Law
- Full migration support
- IBM Tier 3 Certified
- 99.999% Availability
- Full Tech teams on-site 24/7
- 18 telecoms networks
- PCI DSS Compliant

+7(499)201-79-56
info@ixcellerate.com

IXcellerate

CASE STUDY:

HOW INTERNATIONAL PSP PAYU IS PREPARING TO COMPLY WITH THE NEW LEGISLATION

By Julia Shelygina, Marketing & PR Director, PayU Russia

PayU, a leading international payment service provider in Russia, helps a variety of companies to process and aggregate electronic payments, including bank cards, electronic wallets, mobile payments, and Internet banking.

Until recently, the personal data related to the operations of PayU's clients was stored and processed in Poland, where the PayU head office for Eastern Europe is located. The new legal obligation to store personal data on Russian servers triggered us to undertake data transfer to Russia.

The migration of servers is a really complicated process, with several teams of developers and system administrators involved. The situation was complicated by the fact that equipment delivery may take around three months, with little time left for configuration. This is why the transfer operations began right away so as to make sure that all the conditions are complied with by the time the law comes into effect.

Prior to the start of work we determined the criteria to be met by the data center (see table on next page).

At this point very few data centers meet all the criteria. However, the new Russian legislation is driving improvements in Russian data centers, triggering them to get closer to international quality standards.

PayU employees are now busy migrating the servers, and by September 1, 2015 (the day when the new legal requirements on personal data storage will come into force), the system will run in a regular mode with service quality remaining unaffected.

(March 2015)

PayU's criteria for choosing a data center in Russia

Issue	Description	Requirements
Security	Physical security of the data center.	• Fire safety
Compliance	The data center must comply with physical security requirements and pass all the checking procedures, as well as be consistent with our internal policy.	• The data center shall comply with the following safety requirements: PCI-DSS standard: 9.1.1, 9.2, 9.3, and 9.4.
Specialists	The data center must have sufficient headcount of qualified employees.	• Minimum 12 engineers to provide support 24/7 • Someone must always be present at the data center • Minimum one specialist who speaks English
Location	The data center must be in a safe location to minimize the risk of accidents.	• The data center must be located in a protected building
Flexibility	The data center must respond to our requests and, should there be any problems, offer optimal solutions.	• Answer our questions for 4 hours

DataSpace chairman David Hamner: "Many companies won't meet the September 2015 deadline; but they hope to be granted some extensions."

You founded DataSpace in 2009; what did the Russian data center scene look like at that time and how has it evolved since then?

I was really astonished that the seventh or eighth largest economy in the world with most of that centralized in the capital city had no global commercial Data Center operators. Where was the data? What I found in the market in late 2008 were five or six very basic Tier I to maybe Tier II level commercial data centers that were largely operated by systems integrators. It seemed as though they had built some raised floor environments only as a bare necessity to satisfy the environmental demands of their IT businesses. Clearly, the skillsets to build and operate modern data centers didn't exist in the market then.

DataSpace is owned by Russia Partners, a group of funds made up of foreign direct investors and managed by US-based Siguler Guff & Company. They saw the opportunity to modernize Russia's economic infrastructure by introducing the first quality commercial colo product in the market. Many of the players back then were making false claims that they were Tier III level reliability. We originally considered acquiring some of the existing operators and building a new brand around some of the existing Colo product in the market. Because of that we were able to get a close look at what was in operation at the time and we certainly found nothing close to Tier III level redundancy (according to official Uptime Institute topology). Because some of the operators were making these false Tier III claims, we decided to build the real thing and involved the Uptime Institute at the beginning and engaged a world class design team to ensure we ended up with a truly Tier III Certified site that is concurrently maintainable.

Thus DataSpace pioneered the introduction of modern reliable facilities. So, today there are two certified Tier III Constructed Facility location sites in Moscow and a few Design-certified that may or may not become Facility certified. There is certainly an improved landscape of Data Center facilities available on the Russian market today. However the major global operators have yet to enter the market to build and operate.

What is DataSpace's positioning on the markets, are there any real specifics?

We made a significant investment in our first data center. We own our land, our building and are directly subscribed to electricity – that is unique in the market.

1. Siguler Guff has been active for over 20 years in Russia and the countries of the former Soviet Union via six private equity funds that invested approximately $13 billion of capital commitments and more than 65 investments. http://www.sigulerguff.com

DataSpace1 is one of two commercial operators certified by the Uptime Institute as Tier III Concurrently Maintainable Facilities and the only Tier III Operational Sustainability-Gold certified operator in the market. The premium offering comes with a slightly higher price.

Therefore, our customers tend to be sophisticated and highly reliant on their data processing. Like other global markets this means financial exchanges banks, telcos and others that absolutely require top notch reliability and security. So our positioning is at the premium end. And having become the Moscow Stock Exchange's Data Center partner we're also attracting a lot of broker-dealers and ancillary services companies that want the same reliability as the exchange and optimal latency.

How did you see your clients — both foreign and Russian — react to the recent changes in the legal environment, especially the 2014 law that forces them to store the personal data of Russian citizen on Russian territory?

Russian customers have seen this coming for some time and we've seen a migration of operations from Europe back to Russia beginning with the banks and now including cloud operators and other enterprise customers who have known that the implementation of this law was coming and is inevitable.

DataSpace1 comprehensive security system incorporates a multi-zone access control system with biometric access scanners, reinforced mantraps and armed guards 24/7/365. (Photo credit: DataSpace)

With regards to the foreign customers I think that there was some delay as various lobbying efforts took their course to attempt to eliminate this legislation or postpone it. However now that it's been signed and there are specific dates and specific language in this legislation, they're coming to the realization that they need to make these difficult decisions and comply with the law to maintain their businesses in the Russian market. So the Russian demand has been steady for some time but the foreign demand is spiking now. Being a US owned operator with a US sales presence, today our sales pipeline of foreign customers actually exceeds our pipeline of domestic customers.

Did you see some of them consider simply stopping operations with Russia?

Not yet. However I've seen major cloud operators put on hold significant marketing campaigns until the back office service delivery logistics are sorted out

Has implementation been easy, or difficult? In which cases? Has it turned out to be simply impossible in certain cases, due to the law in itself or to the short timeframe provided to comply?

Compliance is easier for foreign companies that have business operations already in Russia. But for some who don't it becomes a complex situation of the establishment of commercial business operations in Russia; not just moving servers and outsourcing their management. Timeline is a challenge and many companies won't meet the September date. However many believe that if they can demonstrate activities to become compliant they may be granted some extensions or be subject to some manageable level of financial penalty.

According to Russian law, is the data exposed to state's eyes? In which cases can personal data be disclosed to the police or secret service?

We're not aware of any technology in our buildings that is in place to monitor traffic or data. That might be because of our foreign ownership. And, we are aware of instances at other data centers where the authorities have arrived with a list of servers to be confiscated. We, in our 3+ years of operations have never once been approached by the authorities. Again that might be because of our ownership. But the truth is it doesn't matter if you're in Phoenix, Arizona or London or Moscow, if the authorities arrive with proper search and seizure warrants, they will get what they came for.

Can data centers offer 100% certainty that personal data be protected from illegitimate intrusions — be they from hackers or the police?

Death and taxes are the only two things I'm aware of that offer 100% certainty. Data Centers vary greatly in reliability, security and skill level of the operator. What I can say about DataSpace is we are without question the most physically secure data center in the market starting with perimeter security, access controls that make extensive use of biometrics and many other security enhancements. In addition, our legal team is specifically trained to examine and validate the accuracy and legitimacy of any such warrant should that situation ever occur for a customer in our data center.

What should a foreign company seeking to move their data storage to Russia look for in a commercial colo provider?

There are several other risks besides the authorities that should concern of foreign data processing user entering the Russian market. In our market it's critical to have documents and ownership. I'd recommend a foreign company seeking to comply with this legislation find an operator that owns the data center facility, owns the surrounding land and directly subscribes to electricity.

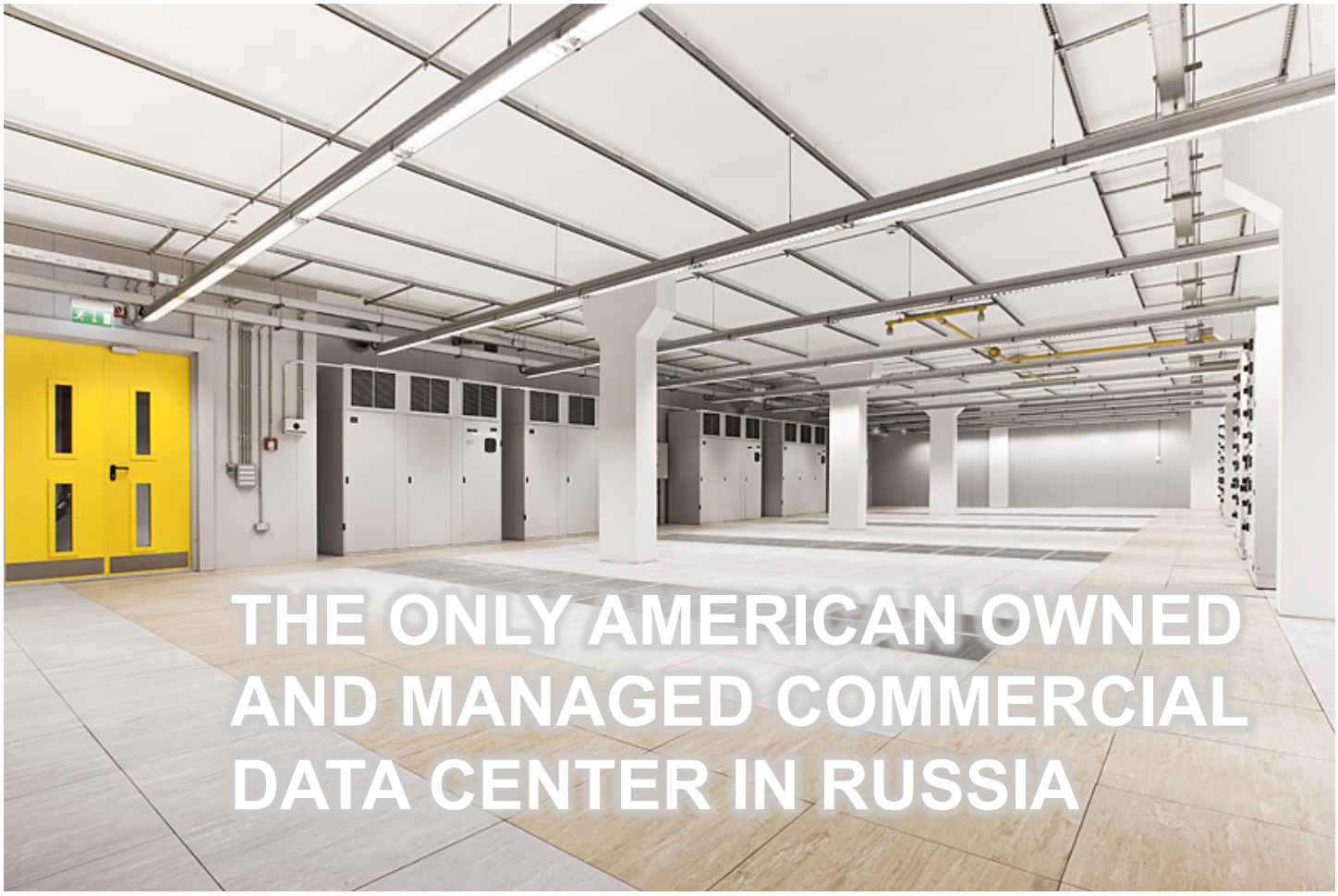
If reliability is important and, sometimes it is more so or less so, then partner with an operator that is fully certified Facility Tier III by the Uptime Institute (not just design certified) and is concurrently maintainable. Look at the counter party. Is it a transparent organization with a proven track record of service delivery? Legal defense? Physically secure? These specific market risks warrant these questions that should be asked and verified and also represent the barriers to entry that have caused global operators to hesitate before jumping in.

(March 2015)

DataSpace1 exterior comprehensive security systems were professionally planned and designed incorporating a multi-zone access control system with biometric access control, armed guards 24/7/365, reinforced mantraps. A three-meter-high full perimeter fence with anti-tunneling protection is topped with rotary razor poles and IR motion detectors to secure the territory. (Photo credit: DataSpace)

DataSpace®

SAFE HAVEN FOR YOUR SERVERS



TIER III DESIGN™ DataSpace DataSpace1 Moscow Data Center November 3, 2010 UPTIME INSTITUTE CERTIFIED

TIER III FACILITY™ DataSpace DataSpace1 Moscow Data Center September 30, 2011 UPTIME INSTITUTE CERTIFIED

TIER III OPERATIONS™ DataSpace DataSpace1 Moscow Data Center 27 June 2014 UPTIME INSTITUTE CERTIFIED GOLD

Sharikopodshipnikovskaya Street 11/8
Moscow 115088 – RUSSIA
T: +7 495 663 6564
E: info@dataspace.ru

WWW.DATASPACE.RU/EN

SELECTEL CEO LEV LEVIEV: "RUSSIAN LEGISLATION GUARANTEES DATA CONFIDENTIALITY IN THE SAME WAY AS IN THE US, UK OR EU."

Selectel is one of the major Russian commercial data centers. Please tell us a bit about company history and activities.

We opened our first data center in St. Petersburg in 2008. This was a pioneering move at that time, when few people in Russia had any idea what a data center even was. Since then, we've designed, built, and launched five other data centers in Moscow and Petersburg. Selectel has become a market leader in terms of both facilities and financial indicators.

At first, Selectel only offered base services, like server space and rack rental. After one year though, we started to develop our hosting services and simultaneously began adopting a multi-service model for our data centers. Right now, a significant part of our portfolio is made up of IaaS services, and the number of high-level services will grow in the future. We believe that because of the benefit it brings to both clients and data centers, cloud infrastructure will soon become mainstream.

How far is now the Russian market from international standards?

Since the market emerged in the late 2000s, competition has significantly increased, especially as international players have started to appear. The relationship between cost and quality has improved. The engineering culture and professionalism as a whole has grown. And finally, clients themselves have become much more competent and demanding.

As for Selectel in particular, we pay great attention to global technological and business trends. Almost every year we travel to the USA, where we meet with equipment vendors and visit major data centers. These have included those of Facebook, Terrmark, and SwitchNAP (the largest in the world). This helps us improve our own projects and bring them to an international level of reliability.

What potential difficulties do you foresee in fulfilling the new legal requirements for storing personal data?

Deadlines are an issue, because there is not much time left until the new law comes into effect. Companies that are planning on moving their physical infrastructure to Russian data centers simply may not make the cut-off date. There are a number of reasons why the process may drag on for 6-8 months.

Problems may be met when importing server equipment. Anyone who has dealt with Russian customs before has experienced a time when a shipment has just sat on the border for months. There are a number of reasons why this happens. Firstly, the bureaucratic machine is sluggish at best and simply doesn't care about deadlines. Secondly, customs procedures are regulated by an array of authoritative documents. Without the necessary experience, they may be impossible to figure out. What's even more complicated is filling them out properly. Here, just one mistake may be reason enough for your equipment not to cross the border. And thirdly, discussions about corruption at Russian customs are not unfounded.

Importing server equipment also entails serious expenses: getting the servers, paying to transport them, insuring the cargo.

The initial stages of the process will have to be monitored on site. This includes the delivery, installation, and testing of the servers. This means a visa, flight, hotel, and most importantly, time, which is something you cannot get back.

Cloud services offered by data centers in Russia are an alternative; what are their advantages and drawbacks?

The first advantage of Infrastructure as a Service, which is how we classify cloud services and dedicated servers, is that it doesn't require massive expenditures. You get top-level equipment that meets your needs and under favorable conditions. Since there is nothing more valuable than reputation, data centers keep their infrastructure up-to-date. Selectel, for example, is one of Intel's platinum partners. This proves how high the company has set the bar in terms of technical development.

In addition, by renting equipment from a data center that is already ready for deployment, you don't need to waste time on installation, testing, debugging, etc. Transferring data while monitoring security procedures may take, at max, a few days. In this case, the entire process (from concluding a contract to launching the server) can be finished in one week's time.

It's worth mentioning the freedom this grants a company. If you have a serious dispute with your service provider, you can switch to another in only a few days. This kind of mobility doesn't exist when a company keeps its servers in a data center. Switching providers becomes a complicated operation, requiring engineers to dismount and mount equipment and insured movers to transport it. And if the equipment is under warranty, then the vendor needs to approve of the movers.

On the other hand, if we think long-term, the cloud services will cost more than the colocation of your own equipment in a data center. The threshold for this is between 3-4 years. To avoid this, some clients may want to return their data from the cloud to physical servers. As a multi-service data center, we can perform the move all at once or in stages. We can also combine both virtual and physical infrastructures, which may be the more cost-effective option.

How do you ensure security for your services, including cloud services? This is a very poignant question especially if we talk about processing personal data.

Security is a very broad term; depending on what aspect we're talking about, responsibility may fall as much on the provider as it does on the user. What a data center should do is provide physical security, reliably protect the information infrastructure, and bring the risk of an emergency outage down to zero. Selectel data centers have a Tier III reliability rating. This lets us offer a 99.98% SLA for all of our services, including cloud services. The physical security of Selectel data centers and their information infrastructure is corroborated by PCI DSS certification. In the entire history of Selectel, there has not once been an instance of a data leak. We take these matters very seriously and value our brand's reputation.

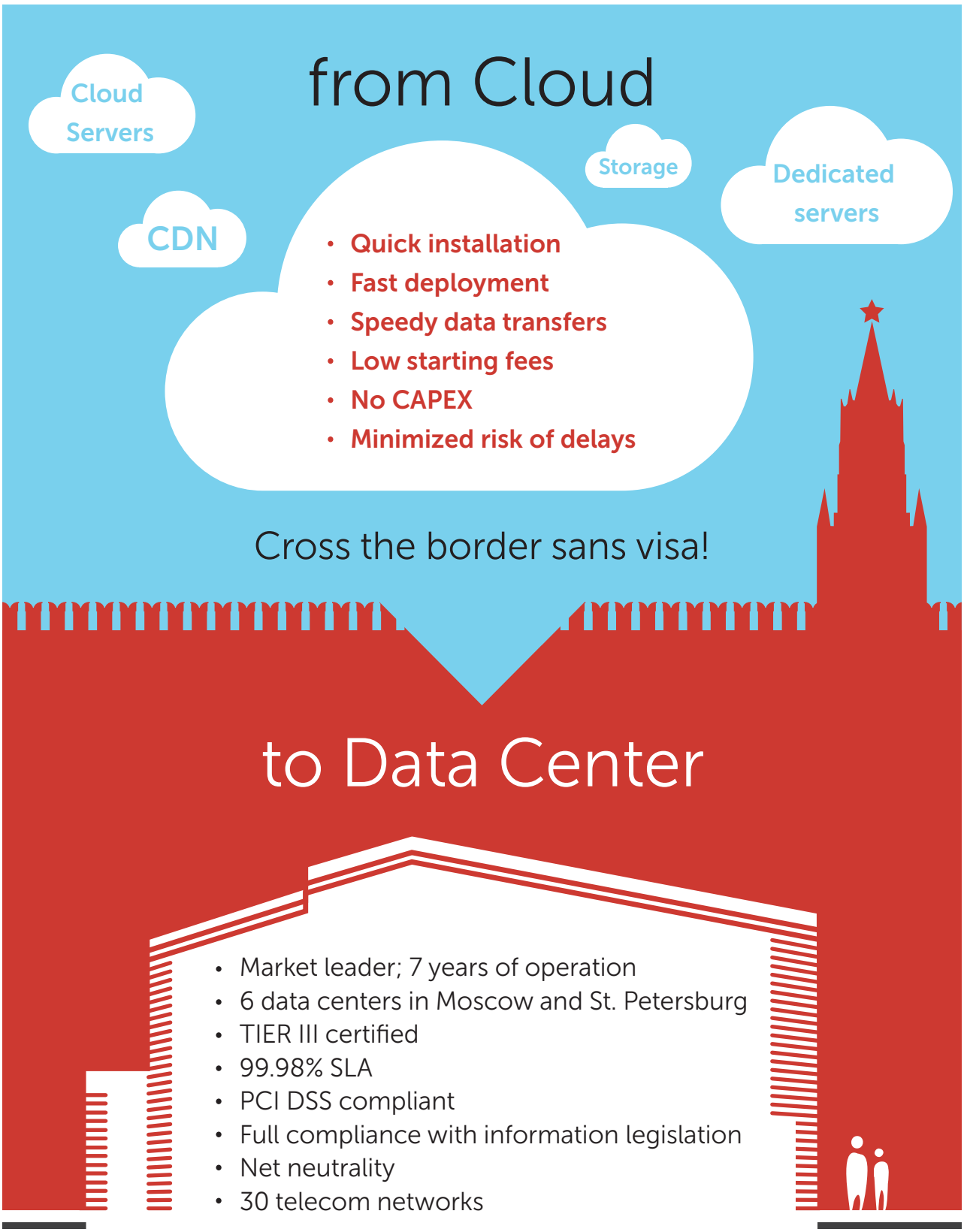
Are data servers operating in Russia required by law to let the authorities, including the secret services, access the data? In which cases may this happen?

Russian legislation guarantees confidentiality, but states that there are circumstances within which confidentiality may be breached. This is nothing out of the ordinary; you will find the same situation in the US, Great Britain, and EU. If the authorities have substantial reason to believe that somebody has engaged in an illegal activity, then by a court's decision, they may be granted access to their servers.

There's something particular about Russia though, and that's the stereotype that here, everything is under the watchful eye of the government. That couldn't be further from the truth though, in our case at least. Selectel is a 100% privately owned company. We have no federal bodies or government-run organizations as clients, and we are in no way funded by government contracts. Thus, all of our interactions with the authorities occur exclusively within the letter of the law.

The only thing our business depends on is how much our clients trust us, which is why we are always looking out for them.

(April 2015)



Selectel

Privately held company

selectel.com

Ask about our Welcome to Russia bonus!

St. Petersburg, Russia; phone: +7 812 677-80-36
Moscow, Russia; phone: +7 495 647-79-80
e-mail: sales@selectel.ru

PERSONAL DATA STORAGE IN RUSSIA

PART 3: THE RUSSIAN DATA CENTER MARKET

Author:
Sergey Zolkin, J'son & Partners Consulting

KEY TRENDS

- Commercial data centers are now used primarily as back-up data centers and corporate sites for online/cloud providers.
- Most corporate data centers were built in the mid-2000s and it is time to replace their core systems. In the current economic situation, companies refuse to use CAPEX, which stimulates the capacity utilization of corporate data centers in commercial use.
- The larger needs of companies in the "new economy:" relative (to revenue) data center space requirements of such companies are a magnitude higher than that of traditional enterprises.
- Corporate data centers of the "new economy" are used as a platform to provide:
  - Applied online services to end-users;
  - Base online and cloud services to other providers.

KEY TAKEAWAYS

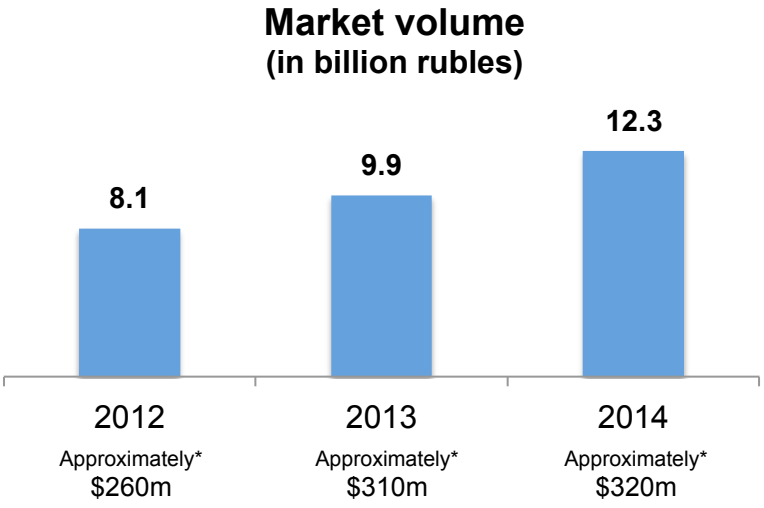
The high growth potential of Russia's commercial data centers is associated not so much with the legislative innovations, but with the technological, economic and organizational ones:

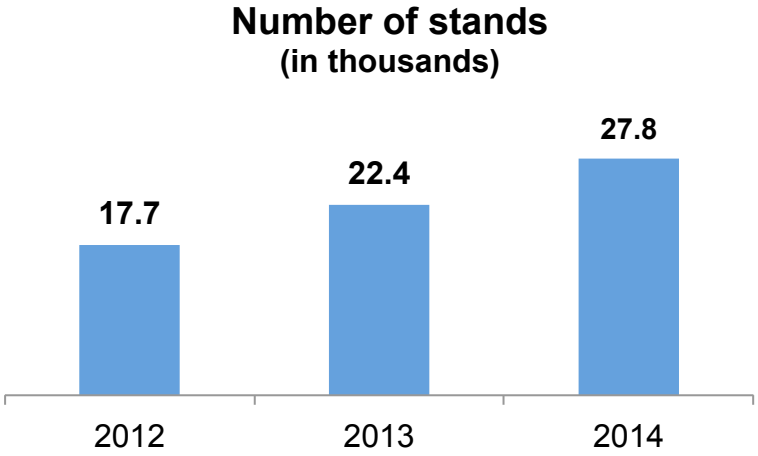
- The need to modernize corporate data centers in a scenario of a decline in IT budgets will force companies and organizations to more closely examine not only colocation but also cloud services as a possible alternative to the modernization of data centers.
- Development of online channels by Russian "non-IT" companies and the expanding presence in Russia of global online providers of cloud services will lead to the growth in demand for bigger data center capacity requirements.
- Stagnation of the economy has spurred the transfer of traditional enterprises into online models, and thus the recession is not an inhibitor but the main driver of the data center industry.
- Both commercial and corporate data centers will experience a fundamental economic and technological transformation, which will result in the formation of a higher-quality new data center services market in Russia

(March 2015)

KEY INDICATORS

Commercial data centers: Colocation and hosting



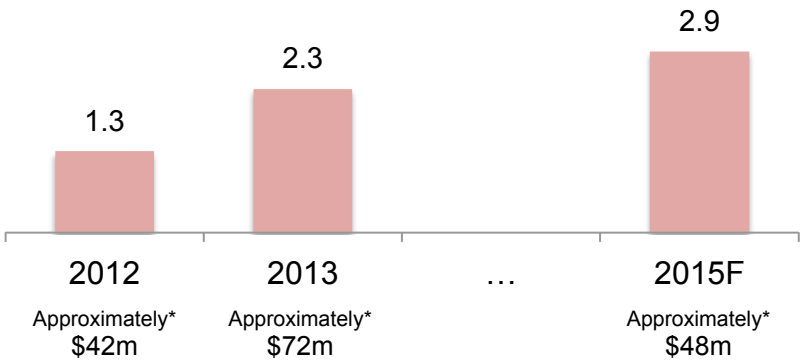


*At the average exchange rate of the corresponding year

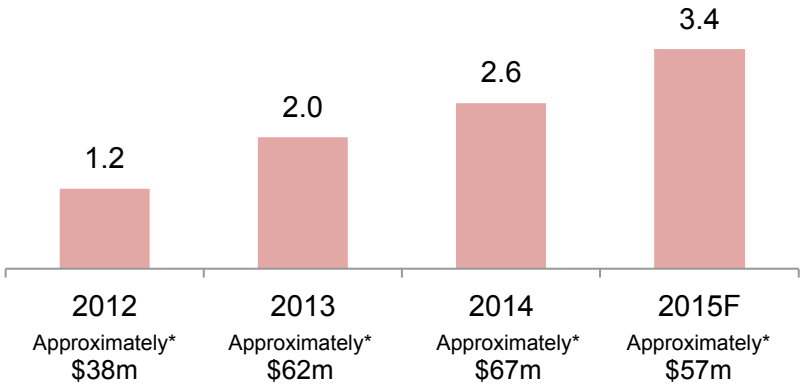
KEY INDICATORS

Cloud infrastructure – IaaS

Russian operations of global players
(estimate, in billion rubles)



Local players
(estimate, in billion rubles)



*At the average exchange rate of the corresponding year

J'son & Partners
Management Consultancy

J'SON & PARTNERS' LATEST MARKET RESEARCH:
"THE RUSSIAN DATA CENTER INDUSTRY: COMMERCIAL AND INVESTMENT PROSPECTS"

REPORT DETAILS

A distinctive feature of this study is its scope - it covers **not only commercial, but also the largest corporate data centers** to evaluate the potential of the data center industry. This is also important since commercial data centers can be classified as commercial in the near future.
The spectrum of analyzed services on data centers basis consists of traditionally described colocation and hosting services as well as the variety of cloud services and close to the cloud online services.

"The main goal of this report is not only to collect and process statistical data of data centers services market size in value and volume terms but also to elaborate promising business models of data centers services delivery and new approaches of traditional and new data center services promotion. We emphasize the qualitative factors of market transformation – be they technological, economic, or legal."

Sergey Zolkin, Senior consultant

ABOUT US

J'son & Partners Consulting is a leading consulting company in telecommunications, high technology, IT and media, with extensive experience in developing and auditing business plans, marketing and financial models, as well as in-depth Research of markets in Russia and CIS countries.

Industry expertise:
- IT, Data Centers & Clouds
- Broadcasting TV & Pay TV
- Fixed-line & Mobile services
- Digital Media & Entertainment
- Content, Distribution, Services
- Payment Systems, Bank cards etc.

Consulting services:
- Market Intelligence and Analysis
- Strategy and Business Planning
- M&A, DD, Investment Advisory
- Capitalization & Brand Awareness Increase and Proportion

Our Clients and Partners: Investment Funds, Telecom / Cellular / Wireless / TV operators, TV Channels, Internet TV / portals / Businesses, Social Networks, Online Games Developers, Content Producers & Distributors, Vendors, Retailers in Russia & Abroad, Russian Government (including the Ministry of Communications), Moscow Government…

QUALCOMM HUAWEI NEC ORACLE CISCO SAP gemalto Google IBS Platformix SAMSUNG and many others!

CONTACT INFORMATION:

J'son & Partners Consulting
Russia, Moscow, Armyansky pereulok 11/2a
tel. +7 (495) 625-7245
fax +7 (495) 625-9177

Pavel Ermolich
Commercial Director
Pavel.Ermolich@json.ru
www.json.ru | www.json.tv

PERSONAL DATA STORAGE IN RUSSIA

PART 4: SELECT ARTICLES

These articles first appeared in East-West Digital News

New personal data storage rules to affect both foreign and domestic players – but still no "Chinese wall" surrounding Russia

By Adrien Henni, East-West Digital News, July 12, 2014

Some foreign players panicked last week when they learned about the new rules adopted by the Russian parliament regarding the collection and storage of personal data – which will be allowed only on the Russian territory starting from Sept. 2016.[1] Concerns were fuelled by inflated media reports, including a Google Translate-based article that appeared on an influential Californian tech blog.

While storage of personal data on servers located abroad is allowed under the existing legislation – with some restrictions – the new rules demand that only servers located physically on the Russian territory be used. Should an online resource fail to respect this obligation, access to it from Russia may be restricted or blocked by state regulator Roskomnadzor. Many businesses will be impacted – but with considerable differences depending on the sector and type of business. These rules will affect international players as well as some domestic companies that currently store users' personal data on servers located outside Russia – or in cloud storage capacities that are distributed in several locations.

No online hotel bookings for Russians?

International companies which currently centralize data from all countries on their own or third-party servers will have to treat and store Russian personal data separately. This concerns countless international websites, mobile application publishers, airlines, brands, manufacturers and even local small businesses with Russian users or clients. The operation of segregating Russian user data and storing it separately in Russia may be complex, depending on the architecture of the IT platform. The task could entail significant costs or, at worst, be simply unmanageable, believe the critics of the law. "As a result, it will become impossible for Russian citizens to book an air ticket via the website of a foreign airline or to book a hotel room via international booking systems, since personal data will be collected and stored [outside Russia]," stated industry association RAEC.

However, some market players believe that the law may still be modified before it comes into force in 2016. This might be the case in the field of air ticket bookings, said Biletix CEO Alexander Sizintsev in an exchange with Russian business daily Vedomosti.

Domestic players will also be affected by the new rule if they store user data, fully or partly, on foreign servers. Vedomosti provides the example of MegaFon, a leading mobile operator that stores its customers' data in the cloud.

1. The Russian parliament ultimately moved the deadline forward to Sept. 1, 2015

The new legal requirements "create a strict framework for businesses and will entail significant additional costs at the database level," the business daily quoted a company representative as saying.

Data repatriation for domestic players

In the vast majority of cases, however, compliance with the new requirements will not be out of reach for businesses. For companies dealing only with Russian users or clients, data repatriation – if necessary – will obviously be a manageable task. Russian flash-sales site KupiVIP.ru did so last year. "We moved everything from Germany, where we initially had our servers," said KupiVIP President Oskar Hartmann to East-West Digital News.

iMall.eu, a London-based online fashion retailer targeting Russian clients, will not be seriously affected by the new law, says its founder and CEO Martin Avetisyan. "No one is asking us to move to Russia, it's just a matter of storing personal data on Russian servers. No doubt by 2016 there will be lots of local hosting offers. Given the potential of Russian business, the implementation costs of storing data locally are absolutely minimum," Avetisyan wrote in an email exchange with East-West Digital News.

Data segregation for international players

As for multinational databases, several examples show that segregating user data by country of origin is also a manageable – though more complex and potentially costly – task. At La Redoute Rus, Russian users' personal data have been stored on Russian servers since the very beginning. "Our Paris headquarters didn't really understand our decision at that time, but we knew that the Russian authorities may, sooner or later, forbid cross-border personal data transfers. In addition, we surveyed our clients who expressed their preference for storing their personal data in Russia," La Redoute Rus General Manager José Metz told East-West Digital News.

Some personal data still transits via the group's international data center in Portugal, "but only temporarily" according to Metz. "Should this process be proven incompatible with the new legal requirements, we'll have enough time [two years until Sept. 2016] to bring the necessary changes."

According to a Western developer of international mobile applications, data segregation by country of origin is not a rare case. "For example, for copyright reasons, video content owners want their content viewed exclusively by mobile users from certain countries. From declared data, to geolocation, to browsing data, users' geographic origin can be defined rather precisely," the company's CEO told East-West Digital News.

"Complying with this Russian law will indeed be difficult for complex databases that mix international data – unless their design took into account such evolutions. However, the "data-without-borders" trend died with the NSA scandal. This Russian rule is forewarning of the next trend – the re-segmentation of the worldwide web on a national basis, and tech players need to learn to manage data differently," the CEO concludes.

Facebook, Google, Lamoda.ru, Otto Group and Ozon declined to answer EWDN's questions.

eBay and PayPal to comply with Russian personal data storage law earlier than Sept. 1 deadline

East-West Digital News, April 10, 2015

eBay has become the first US company to say it will comply with the new Russian legislation requiring businesses to store Russian users' personal data in Russia, business daily Kommersant reported earlier this week.

Vladimir Dolgov, eBay's general manager in Russia, met with a deputy head of telecom regulator Roskomnadzor last week to clarify "a series of questions" related to the law.

"eBay is working on transferring data from Switzerland to Russia. The law goes into force on Sept. 1, but the company will finish this work earlier," said a source cited by Kommersant.

A representative from eBay subsidiary PayPal also participated in the meeting and "expressed the same position as eBay," Kommersant's source said.

The company did elaborate on the volume of data to be transferred and on how said transfer and further operations will be conducted. eBay had 3.7 million customers in Russia as of the second half of last year, the report said.

Adopted last year, the new legislation on personal data storage poses new challenges for many foreign and domestic players that store their users' data in borderless clouds – with considerable differences depending on the sector and type of business.

Unlike eBay, "many companies won't meet the September date," said David Hamner, Chairman of data center company DataSpace.

"However many believe that if they can demonstrate activities to become compliant they may be granted some extensions or be subject to some manageable level of financial penalty," he added in an exchange with East-West Digital News.

PERSONAL DATA STORAGE LAW COMES INTO FORCE AS SOME KEY PLAYERS STILL NOT READY TO COMPLY

By Adrien Henni, East-West Digital News, Sept. 1, 2015

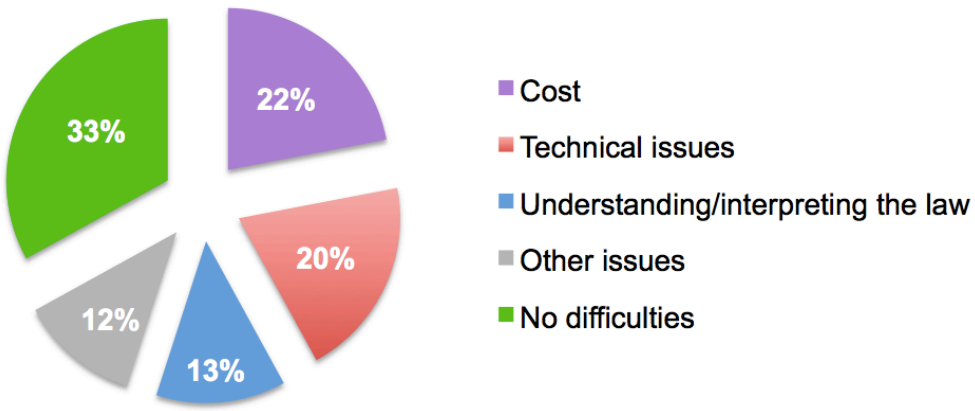
Starting from September 2015, the personal data of Russian citizens must be stored on servers located physically on the Russian territory. Adopted last year in a bid to affirm Russia's digital sovereignty, this new law has provided many players with challenges due both to its demanding requirements and the ambiguity of some of its key provisions.

A huge number of foreign and domestic players, who either store or used to store their users' data outside Russia or in borderless clouds, are concerned. Theoretically, even a hotel in the French riviera with names of Russian clients in its computers is supposed to store this data in Russia. Those failing to meet the new requirements will face fines. Ultimately, access to their site may be blocked by the Russian telecom regulator Roskomnadzor.

In practice, the challenges differ considerably depending on the type of business and database architecture of each. Many companies have worked hard to meet the law's requirements in time, as illustrated by the public announcements made by Booking.com, eBay, PayPal, Alibaba's subsidiary AliExpress, as well as international PSP PayU in the past few months. Some e-commerce players, such as KupiVip and La Redoute, had even anticipated the law by transferring their data away from foreign servers several years ago.

In July, 53% of the French, Russian and international companies surveyed by the French Russian chamber of commerce (CCIFR) stated that they will meet the deadline to comply with the law on September 1, while 39% said that they will comply but with some delay. Another 8% stated that they were not ready to comply at all.

What have been the difficulties in complying with the law?



Survey of 50 French, Russian and international companies in a variety of sectors, from late July 2015. Source: CCIFR.

But many international businesses have not been able to meet the Sept. 1 deadline. This seems to be true in the cases of several international Internet giants, if judging by media reports and the “no comment” or otherwise vague statements of their press services. However, Google has already signed a contract to deploy its equipment in Russia at Rostelecom data centers, while Apple has pledged to move its data by Jan. 1, 2016, reports RBTH.

Announcements about work in progress to transfer data to Russia have also been made by SAP, Samsung, Lenovo, and IBM.

Whether or not Facebook intends to transfer Russian personal data to Russia remains unclear, with the company insisting that user information does not constitute personal data.

Telecom regulator Roskomnadzor has announced that no sanctions for failure to comply with the law on storing Russians’ personal data will be applied till the end of the year. Thus, foreign companies have been given a deferral till Jan. 1, 2016, notes RBTH.

Meanwhile some other players, including some important international companies, are considering leaving the Russian market due to the complexities of the new rules and the unfavorable economic context of the present time.

Much-needed clarifications

Until just weeks before the Sept. 1 deadline, implementing the new rules was difficult due to the lack of clarity and precision of the law in several important respects. Ambiguities remained regarding the scope of the law, whether it was permitted to store copies of personal data outside of Russia, how to identify Russian citizens, and many other issues brought before the Russian authorities by the business community. Some statements from the authorities did concern some of these points, but they had no formal value.

Over the past few months, meetings with the regulator helped businesses clarify the situation. In August 2015, as a result of these meetings and of numerous requests from personal data operators, the Ministry of Telecom and Mass Communications expressed its interpretation of the law on its official website. These statements are not legally binding, but may be regarded as guidelines provided to businesses to comply with the law in good faith.

According to these official interpretations, personal data initially collected and stored in Russia can be transferred to or processed in databases located abroad. Key here, in order to protect the subject of personal data, is the initial location.

The questions of whether or not the law would apply to data collected before Sept. 1, 2015, has also been clarified. The rules are not retroactive; only personal data collected from Sept. 1, 2015, must be stored in Russia.

The Ministry also confirmed that certain businesses, whose activity is regulated by an international agreement or specific legislation, would not be affected by the law. This is the case of airlines and air ticket booking systems.

Contact information

To hear more from the experts who made this white paper, please feel free to contact directly:

- Adrien Henni, chief editor, East-West Digital News editor@ewdn.com
- Anna Kazaeva, Business Development, IXcellerate anna.kazaeva@ixcellerate.com
- Igor Nevzorov, Head of Intellectual Property Center of Excellence (CIS), EY Russia Igor.Nevzorov@ru.ey.com
- Julia Shelygina, PR Director, PayU Russia julia.voitenko@payu.ru
- Ekaterina Udalova, DataSpace Ekaterina.Udalova@dataspace.ru
- Alexander Vechersky, PR Director, Selectel vechersky@selectel.ru

East-West Digital News

A series of **in-depth reports** on digital industries in Eastern Europe

The Russia venture report

The most accurate report on the Russian venture industry, published by RMG partners in partnership with EWDN

- 63 pages
- Available for free in English and Russian

"E-commerce in Russia – Cross-border Sales"

A full set of market data with concrete advice on how to seize the opportunities of a market that grows by 75% annually.

- 8 chapters, 285 pages, updated quarterly
- Available in English language

"E-commerce in Ukraine"

The first-ever report on Ukraine's online retail market, in partnership with the Ukrainian Direct Marketing Association (UADM)

- Available in Russian language
- Free summary in English

To receive these reports or executive summaries at no charge, please contact us at report@ewdn.com