INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

From Safe Harbor to Privacy Shield: Where are we now?

EU Commissioner Věra Jourová hopes that the new arrangement for transatlantic data transfers will be in force in approximately three months' time. By **Laura Linkomies**.

A political agreement for the new arrangement for EU-US data transfers was reached on 2 February. Commissioner Věra Jourová announced the plans to the European Parliament's LIBE Committee the same evening, but was unable to provide any documentation – such was the last minute rush in getting a deal done. In fact, just two days before, speaking at the CDPD conference in Brussels, the parties seemed to differ on several points.

Continued on p.3

Overlap of DP and cyber breach reporting affects some sectors

The EU Network and Information Security Directive: How the GDPR's 'little brother' aims to tackle the big problem of cyber security. By **Claire Walker**.

Cyber security breaches will often compromise personal data too, so organisations which are within the scope of the NISD will need to comply with both regimes.

The EU Network and Information Security Directive (NISD, or Cyber Security Directive), was agreed in Brussels in December, shortly before the General Data Protection

Continued on p.5

Issue 139 **February 2016**

Russia's data localisation law affects foreign online businesses

Brian Zimbler and **Ksenia Andreeva** examine the impact of the new data localisation law.

At the end of 2015 and the beginning of 2016 a number of new Russian laws strengthening governmental control over the mass media and the Internet in Russia entered into force. One of these laws, amending Federal Law No. 152-FZ "On Personal Data" of 2006, obliged companies to store all personal data on Russian citizens in Russia (the 'Localisation Law').

According to the Russian privacy regulator (the Federal Service for the Supervision of Communication, Information Technology and Mass Media, Roskomnadzor), the aim of the Localisation Law is to ensure that the personal data of Russian citizens is protected and secured. Originally, the Localisation Law was expected to enter into force on 1 September 2016 but it actually came into force one year earlier, on 1 September 2015. Much concern has been expressed about its earlier enforcement, as companies were left with limited time to adapt to the changes introduced by the new law and were still assessing the risks of non-compliance.

It was expected that the ambiguity of the Localisation Law's language could automatically lead to a situation where the Russian regulators would have considerable discretion as to how they interpret and enforce the new law. However, in September 2015 Roskomnadzor's press spokesman, Mr. Vadim Ampelonsky, confirmed that they did not plan to impose penalties on companies that are non-compliant until at least January 2016, further noting that Roskomnadzor's 2016 inspection plan was to be approved in the fourth quarter of 2015 by the General Prosecutor's Office. Roskomnadzor's spokesman also added that they planned to issue official guidelines and interpretations of the Localisation Law. However these guidelines had not yet been issued by the end of January.

In January 2016 Roskomnadzor started taking actions for a violation of data localisation requirements under the Localisation Law. Roskomnadzor blocked a number of websites and added them to the register of violators of data subject rights for maintaining an illegal Internet database containing the contact details of over a million Russian citizens. The results of the inspections are publicly available at the websites of Roskomnadzor's territorial subdivisions. However, at this stage Roskomnadzor's practice is still uneven, and interpretation of the Localisation Law is not unified.

Scope of the Data Localisation Law

A single sentence in the Localisation Law contains the core of the new obligations that companies operating in Russia now have: "when collecting personal data, including by means of the information and telecommunication network 'Internet' a data operator must provide the recording, systematization, accumulation, storage, alteration, retrieval of personal data of citizens of the Russian Federation with the use of databases located in the territory of the Russian Federation".

Unfortunately, the Localisation Law does not define any of the terms it uses or elaborate on how to implement the new requirement. This creates uncertainty for companies that do business with Russian citizens, and specifically for those companies which have no legal presence in Russia but work with Russian individuals selling them goods and providing services both on and offline. The general consensus among experts is that companies with no corporate presence in Russia (either in the form of a subsidiary, a branch or a representative office) should not be subject to the Localisation Law. At the same time, online businesses could still be affected, particularly if they customise their websites for Russian users, accept payments in Russian rubles or promote their services in Russia.

The Localisation Law contains some non-business related exemptions from the general rule. In particular, data operators are allowed to store Russian citizens' data in foreign data centres, if such processing is necessary:

1. to achieve goals prescribed by an international treaty or other Russian laws and necessary for the operators to perform their functions, authorities and obligations imposed on them by the laws of the Russian Federation
2. for the administration of justice or enforcement proceedings
3. for the provision of public/municipal services by the Russian state and municipal authorities, local government authorities and entities
4. to enable journalists' professional activity, and
5. the legitimate activities of mass media or scientific, literary and creative activities.

Clarifying the exemptions

Less than a month before the Localisation Law went into effect, the Russian Ministry of Telecoms and Mass Communications (the 'Ministry') published its clarifications of the exemptions from the Localisation Law. Strictly speaking, these clarifications are not legally binding, but they have been interpreted by the market as the official position of the Russian authorities.

The Ministry identified exemptions in addition to those expressly referred to in the Localisation Law. According to the Ministry, the law does not cover the following types of personal data processing:

1. making decisions based on the data
2. transmitting data (including cross-border transfers)
3. depersonalizing data
4. blocking data
5. erasing data.

More importantly, the Ministry expressed the view that the Localisation Law does not apply to the companies that obtain personal data "without solicitation." For example, according to the Ministry, processing of contact details of a designated representative provided in a contract is exempted from the Localisation Law as "acquired from a second legal entity in the course of lawful business activity."

Finally, the Ministry confirmed that the Localisation Law is not applicable if personal data was collected before the Law came into force. This being said, the Ministry added that if personal data collected before 1 September 2015 is updated or changed now that the law is in effect, that data will be subject to localisation requirements.

Unfortunately, the Ministry did not define the above exemptions in detail and thus left room for further broad interpretation of the exempted data processing activities while enforcing the Localisation Law by Roskomnadzor.

What obligations does the Localisation Law impose?

Generally speaking, the Localisation Law imposes two new major obligations on the affected companies that process Russian citizens' personal data.

First, unless one of the exemptions applies, a data operator must collect and store the personal data of Russian citizens on the databases on servers that are physically located in Russia. Such databases are called 'primary databases'. A data operator is required to ensure that the recording, systemisation, accumulation, storage, clarification (updating, modification) and retrieval of Russian citizens' personal data is conducted only in the primary database.

The good news is that once the data is collected in the primary database, it may be further transferred to any third party, including those located outside of Russia (provided that the data subject has consented and such transfer is otherwise compliant with Russian data protection legislation).

Interestingly, in its clarifications the Ministry explained that if the personal data of Russian citizens is processed using paper records only (rather than in an electronic database), and then sent to a foreign-based database via electronic means, the Localisation Law would not require the data processor to have a separate electronic Russian database, as retaining the paper records in Russia would satisfy the localisation requirement. Additionally, the Ministry explained that the Localisation Law does not prohibit remotely accessing the primary database from abroad.

Secondly, in addition to the requirement to notify Roskomnadzor on processing personal data, a data operator must notify the location of servers with databases containing personal data of Russian citizens. However, there is still no form of such notification approved by Roskomnadzor, so at this stage the data operators are free to use any format they want to notify Roskomnadzor.

What are the penalties for non-compliance?

Failure to comply with the Localisation Law may lead to administrative fines for data operators of up to 10,000 rubles (approximately US $135 or 120 Euros). Since late 2014 the Russian Parliament has been considering a draft law to increase liability for failure to comply with the Russian data protection legislation up to 50,000 rubles (approximately US $650 or 582 Euros) for general cases of violations of personal data processing. It is also suggested that violations related to sensitive or biometric personal data will be fined up to 300,000 roubles (approximately US $4,000 or 3,600 Euros). The draft law has not yet been approved but is supported by Roskomnadzor.

Roskomnadzor has the right to carry out inspections on-site, scheduled or without warning, as well as to request documents regarding data processing activities conducted by data operators. Usually Roskomnadzor's representatives recommend that data operators are prepared to show evidence that there are agreements with Russia-based data centres or documents substantiating that a data operator has its own data storage hardware and facilities in the territory of Russia. According to Roskomnadzor, the company can also show its intention to comply with the Localisation Law by:

1. preparing documents demonstrating how it is changing internal data processing procedures aimed at compliance and data protection
2. the company's discussions with potential IT service providers
3. data transfer
4. storage plans and other evidence.

Roskomnadzor also shows leniency towards companies initiating a direct dialogue on the steps that are needed to comply with the localisation requirement. Reportedly, a number of big multinational companies (such as Facebook, Twitter and Google) have already had meetings with Roskomnadzor and discussed the data migration plans and procedures compliant with the localisation requirements.

According to the Localisation Law, Roskomnadzor is entitled to block access to information resources (websites) that are processing personal data in breach of the Russian data protection legislation, including the Localisation Law. Arguably, Roskomnadzor may block access to the websites in any Internet zone irrespective of the location of the data operator or the website administrator.

According to recently published Roskomnadzor's statistics, so far Roskomnadzor has blocked 28 websites in .ru and .su zones only and made 108 entries to the special register of violators of personal data subjects' rights. The register is maintained by Roskomnadzor but Roskomnadzor is entitled to make any entries only on the basis of a court decision. The register contains information about the domain names or other links to website pages on the Internet containing personal data processed in violation, network addresses which enable the identification of such websites, and certain other information.

The Localisation Law has been effective for more than five months, but there are still many questions as to its interpretation and enforcement by Roskomnadzor. Businesses that offer goods and services to Russian citizens and collect their personal data are encouraged to keep a close eye on the developments in this sphere in the coming months and consider auditing and re-structuring their data flows and IT procedures sooner rather than later, seeking further assistance where needed.

AUTHORS

Brian Zimbler, Partner, Morgan Lewis, Moscow: bzimbler@morganlewis.com and Ksenia Andreeva, Associate, Morgan Lewis, Moscow: kandreeva@morganlewis.com
Website: www.morganlewis.com