The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

B2B: Implementing Data Protection Policies in Russia: Hidden Issues

By Pavel Karpunin

May 13, 2013

The MT Conferences section did not involve the reporting or the editorial staff of The Moscow Times.

Pavel Karpunin
Partner
Capital Legal Services

Companies operating worldwide generally adopt data protection policies to be implemented by all of their offices. For instance, many foreign companies operating in Russia require that certain data be transferred from their Russian offices to the headquarters located abroad. As an alternative, some transnational companies use special data centers to store the information produced by their offices worldwide. The data to be transferred by a Russian company abroad typically includes commercial information, as well as personal data of employees and, for companies operating in certain industries (insurance, tourism, air transportation, etc.), also personal data of clients.

Likewise, many companies require that equipment and software of a certain type be used by all of their offices in order to provide a certain security level and simplify the document workflow.

Yet, certain factors need to be taken into account when making a decision on whether to implement the data protection policies developed by the company's head office, especially if such policies involve transferring data used by a Russian company abroad.

Legal restrictions on transferring certain categories of data abroad

Russian legislation establishes some cases when companies may process personal data without obtaining consent from the subjects of the personal data. Such cases include, for example, processing personal data of the company's employees and processing personal data for the purpose of performing a contract to which the subject of personal data is a party.

However, it is important to note that such cases cover only situations where personal data is transferred by the Russian company itself, and do not extend to personal data processing by the headquarters or by affiliated companies of the Russian company or by a data center.

Furthermore, under Russian legislation, a company that plans to transfer personal data abroad must ensure that laws of the relevant country provide for adequate protection of personal data. At present, only the countries that are parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data are deemed by Russia as providing adequate protection for personal data. In order to transfer personal data to other countries (for example, the U.S.), Russian companies must obtain a written consent from the subject of personal data.

In view of the above, Russian companies may be unable to legally transfer personal data abroad due to the refusal of some subjects of personal data to grant consent for such transfer.

It is also worth mentioning that the transfer of other categories of confidential information, including commercial secrets, to third parties, requires consent of the owner of such information. Therefore, a Russian company that intends to transfer confidential information that this Russian company does not own (for instance, information of its business partners), to third parties, must obtain consent from the owner of the information in question. The requirement to obtain such consent likewise applies to the transfer of confidential information to the headquarters of the Russian company or data center.

Liability for disclosure of information

Despite the fact that data centers usually provide certain guarantees with respect to the security of the data they store, the recipient of confidential information remains liable before its owner for non-disclosure of such information. This means that if confidential information is disclosed due to the fault of the data center where it is stored, the owner of confidential information may request that the recipient of the information compensate the damages caused by such disclosure. It is therefore advisable to ensure that the agreement with the data center stipulates the data center's obligation to compensate the user of the data center for any damages (including compensation paid to the owners of confidential information) caused by the disclosure of the information stored at the data center due to the data center's fault.

Requirements for equipment and software

As many companies operating worldwide tend to require that standard equipment and software be used by all of their offices, it is also worth mentioning that the equipment and software used in Russia to process personal data must comply with certain requirements established by Russian legislation.

The requirements depend on the type of personal data processed, as well as the amount of such data, with requirements being stricter for companies that process personal data of a large number of persons and for companies that process special categories of personal data, such as medical information, information on religious views, private life, etc.

Thus, prior to acquiring equipment and software to be used to process personal data in Russia, it is advisable to ensure that such equipment and software guarantee the level of security required by the Russian legislation.

In addition, companies that use encryption tools to protect their data must keep in mind that in order to import into Russia equipment containing encryption tools, a special procedure has

to be followed, which may include obtaining a permit from the Federal Security Service of Russia.

In conclusion, before implementing data protection or data transfer policies in Russia, it appears reasonable to consider the restrictions established by the Russian legislation in view of the types of data used by the Russian company.

If a decision to transfer some data abroad is adopted, it is necessary to allow enough time for its implementation in order to ensure that the requirements of the Russian legislation are met.

The MT Conferences section did not involve the reporting or the editorial staff of The Moscow Times.

Original url:
https://www.themoscowtimes.com/2013/05/13/b2b-implementing-data-protection-policies-in-russia-hidden-issues-a23986