

■ **INDEPTH FEATURE** Reprint November 2020

DATA PROTECTION & PRIVACY LAWS

Financier Worldwide canvasses the opinions of leading professionals around the world on the latest trends in data protection & privacy laws.





RUSSIAN FEDERATION

Gorodissky & Partners

Respondent



SERGEY MEDVEDEV

Partner

Gorodissky & Partners

+7 495 937 6116

medvedevs@gorodissky.com

Sergey Medvedev is a partner in Gorodissky & Partners' Moscow office, where he works in the intellectual property (IP) and technology, media and telecommunications (TMT) group. With more than 12 years of professional and profound legal experience, he advises clients on all aspects of Russian law associated with IP and TMT, internet and e-commerce, data protection and privacy, software development and protection, licensing and outsourcing, franchising and distribution, TMT dispute resolution and IP litigation. His clients are global corporations and big multinational companies. He is the accredited and regular DataGuidance and Practical Law contributor and a recognised PrivacyRules expert.

Gorodissky & Partners

Q. In your experience, do companies in the Russian Federation need to do more to fully understand their data privacy and protection duties in the digital age?

A: Globally, data privacy and protection have become one of the most discussed topics in the information technology (IT) legal sector in the last couple of years, and the Russian jurisdiction is no exception in this regard. In the digital age and with the constant evolution of e-commerce, companies currently operating in Russia should carefully assess not only their international, but also their national data protection strategies, especially when they overlap and proceed with local data privacy compliance, in order to mitigate the associated risks. However, not all companies are fully aware of their main rights and general obligations under Russian laws and regulations, which have a lot of specifics and technical details. This may lead to a big challenge for global or multinational companies following the enactment of tougher sanctions and fines for data breaches on a local and global level.

Q. Could you outline the latest legal and regulatory developments affecting corporate storage, handling and transfer of data in the Russian Federation?

A: When collecting personal data, the data operator must provide the data subject, at his or her request, with certain required pieces of information, including but not limited to, the legal grounds and purposes of data processing, methods and duration of data processing, as well as the information on cross-border data transfer, if planned. If the provision of personal data is mandatory under the Russian law, the data operator is required to explain to the data subject the legal consequences of refusing to provide such information. In cases where personal data is collected through the internet, the data operator is obliged to ensure that the recording, systematisation, accumulation, storage, clarification and extraction of personal data, which is related to citizens of the Russian Federation, is made through the use of databases located in the territory of the Russian Federation. In the event of a cross-border data transfer, the data operator must ensure, before such transfer is made, that the rights and interests

Gorodissky & Partners

of the respective data subjects are fully protected in an ‘adequate manner’ in the corresponding foreign country. Cross-border data transfers to countries that do not provide a level of ‘adequate protection’ is permitted, if the written consent of respective data subjects has been received, or it is made for the performance of the contract to which the data subject is a party.

Q. In what ways have the authorities increased their monitoring and enforcement activities with respect to data protection and privacy in recent years?

A: Local data privacy laws have been enforced quite heavily in recent years, and the Russian Data Protection Authority (Roskomnadzor) is quite active in terms of monitoring national data protection compliance. There has been a growing number of cases for data breaches of late, and the local court practice devoted to data privacy enforcement is developing constantly. On 1 July 2017 the administrative sanctions for different privacy violations were increased substantially. For example, data processing, which is not in line with legal

requirements toward the volume of data provided in the written consent of data subject, may eventually lead to a fine of RUR 75,000 for a business entity acting as the data operator. Also, in case of illegal data processing on the web, access to the infringing website may be blocked under the effective court decision in Russia. Criminal prosecution is available for certain specific categories of privacy violations. Roskomnadzor is empowered to carry out planned and random inspections of data privacy compliance. If data breaches are uncovered, it can investigate and move infringement cases to local courts, if applicable.

Q. What insights can we draw from recent high-profile data breaches? What impact have these situations had on the data protection landscape?

A: There have been quite a few high-profile data breach cases in Russia in recent years. All of them are surrounded by different background, circumstances, outcome and court decisions. For instance, in *Telegram*, the Russian Court of General Jurisdiction fined instant messaging service Telegram RUR 800,000 for a



Gorodissky & Partners

failure to provide the Federal Security Service (FSS) with its decoding keys, as prescribed by Article 10.1 (4.1) of the Russian Data Protection Act. On 22 October 2018 Telegram's appeal was rejected, and the administrative fine was enforced under Article 13.31(2.1) of the Russian Code of Administrative Offences. Russian law requires all messaging services to ensure the confidentiality of their users' communications. In this case, the FSS, although entitled to see such communications by operation of law, was refused access by Telegram, which argued that it lacked control over the encoding and decoding processes. Eventually, Telegram lost this particular court case. Telegram clearly demonstrates that if the technology of the messenger does not grant Russian state authorities to get an access to the decoded information, including personal data, this may be deemed a data breach under the Russian law and local practice.

Q. What steps can companies take to mitigate data risks arising from the use of third parties, such as consultants, agents and distributors?



Companies currently operating in Russia should carefully assess not only their international, but also their national data protection strategies, especially when they overlap and proceed with local data privacy compliance in order to mitigate the associated risks.

Gorodissky & Partners

A: Third parties, including consultants and agents, are basically subject to the same legal requirements as data operators, and they must comply with general data processing and certain compliance rules established by Russian law. Usually, such third parties will be acting under data processing agreements, and data operators will be liable for all acts or omissions of data processors in front of data subjects, while respective data processors must take responsibility and the associated risks before data operators. Of course, data subjects must provide their consent to the transfer of their personal data to third-party processors.

Q. What can companies do to manage internal data privacy risks and threats, such as liabilities arising from lost devices or the actions of rogue employees?

A: Certain legal, technical and organisational steps must be undertaken in terms of overall data processing compliance and privacy management, including against data theft risks and threats, or actions or omissions of rogue employees. In practice, compliant companies would develop appropriate and


efficient data enforcement programmes, as well as unique ‘models of threats’, against actual or potential data breaches to manage the associated risks. Special training and privacy-related sessions are usually conducted for employees on a regular and professional basis. Certain technical means and data security solutions would be applied for special cases.

Q. What essential advice can you offer to companies in the Russian Federation on managing data risk and maintaining regulatory compliance going forward?

A: When doing business in Russia it is essential to manage data risks and maintain regulatory and regular privacy compliance on a proper and legitimate basis. The appointment of local data protection officer (DPO), the adoption of local data protection policy and other required privacy documents, as well as the implementation of appropriate security measures, will be the first key things to do, among other actions, in addition to defining the overall business processes, data flows and relevant data categories. Of course, the underlying agreements with all third parties and data processors must be



Gorodissky & Partners

made in place. Again, if the personal data of Russian individuals is collected online, the ‘localisation’ of the corresponding database or IT system in the territory of Russia is a must. Finally, we would recommend conducting periodic data protection audits and ensuring ongoing data privacy compliance with national data protection requirements and regulations, including when they are amended or updated. 

www.gorodissky.com

A home-grown and full-service Russian IP and TMT boutique, **GORODISSKY & PARTNERS**, with its headquarters in Moscow, 12 branch offices in Russia and one in Ukraine, is a leading firm in every aspect of the protection, disposal, management and enforcement of IP and IT rights. Though the firm’s main jurisdictions are Russia and Ukraine, thanks to its trusted network, Gorodissky & Partners represents national and international clients around Eurasia and CIS countries. It is the largest legal practice in Russia and among the top 10 biggest IP/IT law firms in Europe. The firm was originally founded in 1959.

SERGEY MEDVEDEV Partner
+7 495 937 6116
medvedevs@gorodissky.com

GORODISSKY