Russian Data Protection Updates: Key Points for International Businesses

September 13, 2022

Russia has enacted amendments to its Personal Data Law (the "Amendments") that may have a significant impact on companies operating in Russia. The Amendments became effective on September 1, 2022, save for certain provisions that will become effective on March 1, 2023.

This Debevoise In Depth addresses key aspects of the Amendments that impact multinational companies: (i) expanded extraterritorial effect; (ii) enhanced cross-border data transfer restrictions; and (iii) mandatory data breach notification.

The penalties for noncompliance are relatively modest in comparison to those in the European Union and the United Kingdom. However, the increased likelihood of investigations by Russian authorities, which can be disruptive and time-consuming, coupled with potential sanctions concerns when dealing with Russian government authorities, are further reasons for companies to take note of the new requirements and to carefully assess the attendant risks. You can read more about recent Russia-related sanctions developments here.

Expanded Extraterritorial Effect

As amended, the Personal Data Law has extraterritorial effect and applies to any processing of personal data by foreign persons (including corporate entities): (i) pursuant to a contract with a Russian citizen; (ii) pursuant to other agreements between foreign persons and Russian citizens; or (iii) if a Russian citizen consented to having their personal data processed by a foreign person.

Previously, the Personal Data Law had no express extraterritorial effect and, per prior regulatory guidance, was limited to processing of personal data that took place in Russia or in connection with Internet services aimed at individuals located in Russia. The Amendments therefore significantly expand the Personal Data Law's scope. Companies processing personal data of Russia-based individuals may want to assess (or reassess) whether they are subject to the Personal Data Law.

Enhanced Cross-Border Transfer Restrictions

From March 1, 2023, companies transferring personal data outside of Russia will face significantly increased compliance hurdles. Generally, companies will have to notify, and in certain circumstances obtain approval from, the Russian Federal Service for Supervision of Communications, Information Technology and Mass Media ("Roskomnadzor") before transferring personal data outside of Russia. Companies will also be required to conduct a cross-border data transfer risk assessment. Companies subject to the EU General Data Protection Regulation (the "GDPR") may be able to repurpose existing data transfer risk assessment policies and procedures to address the new Russian requirements.

Companies will not have to submit their risk assessment reports to Roskomnadzor, but they will have to include the date of the assessment in the cross-border data transfer notification submitted to Roskomnadzor, which can subsequently request the full assessment.

Risk Assessment

In conducting the risk assessment, companies will need to consider the level of protection offered to the Russian personal data post-transfer. This should include an assessment of:

- information about the recipient of the data;
- measures the recipient will have in place to protect the transferred personal data; and
- laws in the jurisdiction where the recipient is located and the level of protection they afford to personal data. This legal assessment is not required if the jurisdiction of the recipient (i) is a party to the 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (which includes all EU Member States and the United Kingdom) or (ii) is included in Roskomnadzor's list of jurisdictions providing adequate protection to personal data (collectively, "Permitted Jurisdictions"). The United States and China are not among the Permitted Jurisdictions at this time.

Roskomnadzor Notification and Approval

As of March 1, 2023, companies will have to notify Roskomnadzor prior to transferring personal data outside of Russia, except in certain narrow circumstances. If personal data is to be transferred to a Permitted Jurisdiction, the transfer may proceed after the Roskomnadzor notification is made, without awaiting Roskomnadzor's response. For

transfers to Non-Permitted Jurisdictions, Roskomnadzor's approval must be obtained before the transfer.

Roskomnadzor generally must respond to cross-border transfer notifications within 10 business days. Based on its own assessment of the transfer, Roskomnadzor can prohibit or otherwise restrict the transfer to Permitted or Non-Permitted Jurisdictions if it determines that doing so is necessary to protect morality, health, rights, and legal interests of individuals.

In addition, upon application of other Russian authorities, Roskomnadzor may restrict or prohibit any cross-border transfers of personal data to Permitted or non-Permitted Jurisdictions for the purposes of:

- protecting the constitutional order of Russia, upon a request of the Federal Security Service (the "FSS");
- national security, upon a request of the Russian Ministry of Defense;
- protecting Russia's economic and financial interests, upon a request of the regulatory bodies authorized by the president or government of Russia; and
- ensuring the protection of rights, liberties and interests of Russian citizens, sovereignty, security and territorial unity of Russia, and other interests of Russia, upon a request of the Russian Ministry of Foreign Affairs.

If Roskomnadzor prohibits or restricts a cross-border transfer and the data has already been transferred, the transferee will have to procure the deletion of all previously transferred personal data by the foreign recipient in accordance with Roskomnadzor's directive.

The fines for failure to submit a cross-border data transfer notification to Roskomnadzor can result in fines ranging from RUB 10,000 (approx. $164) to RUB 300,000 (approx. $4,896), substantially lower than the fines that multinational companies face under other privacy laws, including the GDPR. That said, noncompliance with the notification regime may lead to regulatory scrutiny from Roskomnadzor, which can be disruptive and costly.

The new cross-border transfer restrictions are likely to have a significant impact on multinational companies that continue to operate in Russia or that receive data from Russia, including in the context of regular business practices and in the context of internal investigations, cross-border regulatory actions or litigation.

Data Breach Notification

The Amendments introduce a two-track data breach notification framework.

First, companies will need to take part in the State System for Detection, Prevention and Liquidation of Consequences of Cyber Attacks. Through this scheme, companies will be required to report activity related to personal data to the FSS, including cybersecurity attacks that lead to personal data breaches. This requirement came into force on September 1, 2022, but, to date, the FSS has not implemented any regulation or guidance regarding the process.

Second, in addition to any notifications made to the FSS, companies will need to notify Roskomnadzor about personal data breaches. The first notification must be made within 24 hours of the discovery of the breach and should include an overview of the breach, its suspected cause, the harm caused, the measures the company had in place to prevent the breach, and details of the person responsible for interactions with the regulator. The second notification must be made within 72 hours of discovering the breach and should include any additional available information regarding the breach. From March 1, 2023, Roskomnadzor will maintain a personal data breach register and will share the information on data breach incidents with the FSS. The 24-hour initial notification period is considerably stricter than the GDPR's 72-hour notification period.

Penalties for failure to comply with the data breach notification framework have not been set out in the Amendments. According to a press release by the Russian Ministry of Digital Development, Communications and Mass Media, fines for personal data breaches are in the process of being reviewed and may be significant (*e.g.*, taking into account a company's revenue).

Multinational companies operating in Russia will have to comply with these new notification obligations and may wish to update their existing incident response procedures to reflect them and the short notification timeline.

The authors would like to thank Debevoise Trainee Associates Maria Epishkina and Aleksei Shapovalov for their work on this Debevoise Data Blog.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Alan Kartashkin
akartashkin@debevoise.com

NEW YORK / LONDON

Jane Shvets
jshvets@debevoise.com

LONDON

Konstantin Bureiko
kbureiko@debevoise.com

LONDON

Robert Maddox
rmaddox@debevoise.com