ALRUD

Newsletter

The major reform of Russian data protection and information laws in July, 2022

July 19th, 2022

Dear Ladies and Gentlemen,

Please be informed that new laws, introducing major reform of Russian data protection and information regulation, have been passed by the Russian parliament and signed by the President of the Russian Federation, in July 2022. The reform covers:

- Significant changes to the Federal Law No. 152-FZ on Personal Data ("**Personal Data Law**"), regarding the scope of its application, new rules for cross-border transfer of personal data, data breach notifications, additional guarantees for data subjects etc.
- New amendments to Unified Biometric System regulations.
- Establishment of a countersanction-information legal regime.
- Introduction of administrative fines for violation of The Federal Law No. 236-FZ on the activities of foreign entities on the Internet in the Russian Federation ("**the Landing Law**").

We would like to present you with the key changes of the newly-passed laws, which should be considered by international companies, when carrying out business activities in Russia.

The reform of personal data laws[1]	
Extraterritorial application	The Personal Data Law will apply to foreign companies, if their processing of personal data of Russian nationals is based on: • An agreement where a Russian national is a party • Consent of a Russian national to processing. Therefore, when a foreign data controller enters into an agreement and/or obtains consent from a Russian data subject, Russian data protection laws are applicable by default, including data localization requirements. For instance, processing of data by an e-commerce platform, even not targeting the Russian market, will be subject to Personal Data Law.
Liability of a foreign data processor	Data controller and data processor both bear equal liability for a violation of Personal Data Law. Additional safeguards can be included into the data processing agreements, to ensure proper distribution of liabilities between a controller and processor, in case of data breach, or other violations.
New rules for	Data controller shall notify and, in some cases, secure permission of the

[1] The Draft Law No. 101234-8 on amendments to the Federal Law on Personal Data, certain legislative acts of the Russian Federation and on repealing part 14 Article 30 of the Federal Law on Banks and Banking Activities. The below-mentioned amendments will come into force on September 1st, 2022, except for the new rules on cross-border data transfer, which will come into force on March 1st, 2023.

cross-border data transfers	Russian data protection authority ("**Roskomnadzor**"), before cross-border, data transfer. There are two regimes of cross-border, personal data transfer in the updated Personal Data Law: a) Transfer to "adequate" jurisdictions: • Personal data may be transferred upon the notification of Roscomnadzor • While the notification is being considered, transfer is not prohibited. b) Transfer to "inadequate" jurisdictions: • Personal data may be transferred upon receipt of the permission of Roscomnadzor • Transfer of personal data abroad is restricted, until the permission is obtained • Personal data may be transferred abroad before permission is obtained, if it is necessary to protect life, health and/or other vital interests of a data subject, or others. Application of a data controller for cross-border, data transfer shall be reviewed by Roskomnadzor, within the statutory term of 10 days.
Data breach notifications	New obligations of data controllers to ensure prevention of data breaches include: • The two-step data breach notification procedure to Roskomnadzor now shall apply: a) Within 24 hours: a notification on: (i) causes of a data breach, (ii) allerged harm, (iii) security measures undertaken and (iv) contact details on authorized official of a data controller, with whom to interact, in relation to data breach. b) Within 72 hours: a notification of: (i) internal investigation results and (ii) persons who caused the data breach. • Data controller ensures interaction with GosSOPKA[2], including providing details of any computer incidents that resulted in unlawful access, publication and/or transfer of personal data.
Restrictions on biometric data processing	A data controller cannot refuse services to customers if they are not willing to provide their biometric personal data, or consent to its processing.
Additional guarantees for data subjects	Data controllers should pay special attention that the following contractual clauses are not included in agreements with data subjects, and conduct a due diligence review covering the restrictions listed below:

[2] The state security system for detecting, preventing and eliminating the consequences of computer attacks on the information resources of the Russian Federation.

	• Contractual clauses that restrict personal data subjects' freedom • Contractual clauses establishing cases of processing minors' personal data • Contractual clauses allowing the omission of the personal data subject, as a condition for the conclusion of an agreement.
Response to requests and enquiries	Statutory terms for response to Roskomnadzor and data subjects' requests have been shortened from 30 days to 10 days.
Privacy policy on the website	Personal Data Law was supplemented with a new obligation of a website owner, as a data controller, to place a privacy policy on each webpage, where personal data is collected.
New amendments to the Unified Biometric System regulation[3]	
Public authorities shall upload biometric personal data, they have collected as part of their activities, to the Unified Biometric System ('UBS') upon informing data subjects. The consent of a data subject is not required for this. Commercial organizations will be able to use biometric data from the UBS to identify data subjects, starting from March 2023.	
Special regime of countersanction information[4]	
The dissemination of countersanction information, i.e., any transactional information, the disclosure of which can entail the introduction of economic sanctions against Russia, is generally prohibited with a few exceptions. We recommend analyzing the existing agreements with Russian entities on the applicability of the new countersanction-information regime and including provisions requiring the parties to disclose whether any information can be considered as countersanction, the procedure on disclosure etc.	
Fines for violation of the Landing law[5]	
The so-called Landing Law entered into force, in full, on January 1st, 2022, that obliges some foreign IT-companies, that meet the criteria set out by the Law, to: • create a branch, a representative office, or an authorized legal entity in Russia, • register a personal account on the website of Roskomnadzor, • place an electronic form, on their resource, for feedback from Russian citizens, or organizations, • install and operate audience counting software.	

[3] The Draft Law No. 946012-7 on Amendments to Articles 14 and 14-1 of the Federal Law on Information, Information Technology and Information Protection and Article 5 of the Federal Law on Amendments to Certain Legislative Acts of the Russian Federation
[4] The Draft Law No. 135977-8 on amendments to certain legislative acts of the Russian Federation and on the suspension of certain provisions of legislative acts of the Russian Federation
[5] The Draft Law N 84631-8 on amendments to the Code of Administrative Offences of the Russian Federation

Administrative liability, for failure to comply with the requirements of the Landing Law, has been finally introduced into the Code of Administrative Offences. Here, we present some examples of administrative fines for IT-companies:

Failure to comply with the landing obligations	Up to 1/10 of the annual revenue, or up to 1/5 of the annual revenue for any repeat offence
Processing of personal data of Russian subjects, in case of a ban by Roskomnadzor	Up to 6 million RUB (approx. 102, 510 USD or 101, 868 EUR) and up to 18 million RUB (approx. 307, 530 USD or 305, 604 EUR) for any repeat offence
Failure to submit, or untimely submission, to Roskomnadzor, the information needed for the maintenance of the register of foreign IT-companies	Up to 700 thousand RUB (approx. 11, 960 USD or 11, 890 EUR)

If any of your colleagues would also like to receive our newsletters, please let us know by sending us his/her email address, in response to this message. If you would like to learn more about our Data Protection and Cybersecurity Practice and TMT Industry Group please let us know in reply to this email. We will be glad to provide you with our materials.

NB: Please note that all information was taken from open sources. Neither ALRUD, nor the author of this letter, is responsible for the consequences that arise as a result of making decisions based on this letter.

If you have any questions, please, do not hesitateto contact ALRUD partner

Sincerely,
ALRUD Law Firm

Maria Ostashenko

Partner
Commercial, Intellectual Property, Data Protection and Cybersecurity

E: mostashenko@alrud.com