Law on Security of Critical Information Infrastructure: implications for players of finance, banking, transport, health, telecom and other industries.

July 20, 2017

Dear Ladies and Gentlemen,

We would like to inform you of the recent developments of Russian cybersecurity legislation. The draft law "On Security of Critical Information Infrastructure" has passed the third (final) reading at the Lower Chamber of the Russian Parliament and has been sent to the Upper Chamber for final approval. Afterwards Russian President will likely sign the document. The draft law defines critical information infrastructure ("**CII**"), industries of CII, responsibilities of their owners, enforcement powers of state authorities, etc.

Amendments proposed under the draft law will come into force on January 1, 2018.

Who will be on the radar?

The draft law targets the state authorities, Russian legal entities and individual entrepreneurs owning and otherwise possessing IT and telecom systems, automated control systems as well as electronic communications networks applied in the following industries: healthcare, science, transport, communications, defense, energy, banking and finance, nuclear energy, mining, chemicals, space-rocket, metallurgy, fuel ("**CII Subject(s)**"). The draft law also applies to the Russian entities and individual entrepreneurs ensuring connectivity between CII Subjects.

State register of crucial CCI

Information systems of the CII Subjects shall be assigned a category (one of three) in accordance with their social, economic, political, ecological and public security weight.

The CII Subject itself shall make decision on assigning particular category to its system or decision not to assign it at all. The decision made shall be communicated to a competent state authority, which will verify or challenge it.

If CCI is assigned a category and the state authority approves it, the information on such CII is inserted into the special register ("**Crucial CII Subjects**").

Responsibilities of CII Subjects

The key obligations are as follows:

- Notify immediately the state authorities of a computer incident;
- Cooperate with the state authorities in detecting, preventing, investigating computer incidents and mitigating their negative consequences;
- Comply with technical requirements concerning antiviruses and other technical means installed to detect computer attacks.

Additional obligations are imposed on Crucial CII Subjects, such as:

- Comply with special security requirements;
- Comply with the orders of the competent state authorities with respect to security requirements;

- Respond to compute attacks as required by applicable regulations, mitigate consequences of the attacks;
- To ensure easy access to Russian authorities to crucial CII.

Application of state secrecy laws

Under the draft law the information on security measures applied to the CII constitute state secrecy. Please note that information system containing state secrecy is subject to specific statutory requirements (e.g., only certified security tools can be used; specific IT contractors can be engaged, etc.).

Liability issues

The draft law supplements Russian Criminal Code with a number of crimes in the area of cybersecurity. In particular, it introduces criminal liability for non-compliance with rules on handling means for storage, processing and transfer of information contained in the CII (up to imprisonment).

Hope that the information provided herein would be useful for you. 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, please let us know about it in reply to this email. We will be glad to provide you with our materials.

If you have any questions, please, do not hesitate to contact the Partner of ALRUD Data Protection and Cybersecurity Practice **Maria Ostashenko** at MOstashenko@alrud.com.

Kind regards,

ALRUD Law Firm

Note: Please be aware that all information provided in this letter was taken from open sources. The author of this letter bears no liability for consequences of any decisions made in reliance upon this information.