LEGAL DIGEST
DATA PROTECTION & CYBERSECURITY

February 14, 2018

Dear Ladies and Gentlemen,

We are pleased to share with you a summary of the most important Data Protection and Cybersecurity topics in Russia of 2017, which shall be of use in 2018 and beyond.

***

DO NOT FORGET TO UPDATE NOTIFICATION PROFILES

Since September 2015, when the requirement on local processing of Russian nationals' personal data came into force, data controllers have been required to notify Roskomnadzor of the location of their databases in Russia.

In 2017, Roskomnadzor was very active in requesting data controllers, who had been registered in the registry of personal data controllers before September 2015, to update their profiles by providing information on location of their databases in Russia.

Roskomnadzor also checked whether the information specified in the registry was correct and up to date.

Data controllers can and should voluntarily update their profiles in the registry of personal data controllers, in order to avoid unexpected checks by the regulator.

***

ROSKOMNADZOR ISSUED GUIDANCE ON PRIVACY POLICIES

Each data controller must have a data processing policy and make it available to data subjects.

In 2017, Roskomnadzor issued guidance on the content and structure of data processing policies.

Although the document has no binding effect, Roskomnadzor expects data controllers' policies to follow the issued guidance. Therefore, data controllers are recommended to check the content and structure of their data processing policies and update them, if necessary.

***

SEPARATE CONSENT FOR EACH PURPOSE

In cases where data processing requires written consent, such consent to the processing of personal data must contain the purpose of such processing. It is quite often, and common practice, to include all relevant purposes of processing in one consent form.

In 2017, Roskonadzor clarified that each written consent shall be specified as much as possible and be dedicated only to one purpose of personal data processing. DPA already has commenced a

practice of fining data controllers for having only one written, multi-purpose consent. Russian courts supported the position of Roskomnadzor.

As the fine for non-compliance with the requirements to written consent has been raised approx. 7 times in 2017, it is expected that Roskomnadzor will actively check compliance of data controllers' consent forms with the "1 consent per purpose" requirement. In this regard data, controllers are recommended to improve their consent forms.

***

INCREASED CONTROL OVER DIGITAL SERVICES

Several important amendments, aimed at regulating the digital services, have been made to the Russian Federal Law "On Information, Information Technologies and Protection of Information" (dated July 27, 2006 No. 149-FZ) in 2017. In particular, the following digital services are already - targets:

Anonymizing services

Russian law provides for a specific procedure to block the websites (e.g. where personal data processing does not meet the requirements of Russian law, etc.). The most well-known case is LinkedIn, which has been unavailable for Russian users since November 2016, for failure to comply with certain Russian data protection requirements. Blocking, however, could be easily bypassed with use of tools called "anonymizers". The amendments were introduced to address this problem. In particular, anonymizers' owners and providers are prohibited from providing any technical opportunities to access the blocked information. In case of non-compliance, the anonymizer will be blocked and therefore unavailable in Russia.

Messengers

Since January 1, 2018, new regulations primarily targeting such services as WhatsApp, Viber, Skype, Facebook messenger and Telegram Messenger came into force. The main result of the newly-adopted regulations is that 'messengers' are officially recognized as moderators of dissemination of information and, for this reason, are already obliged to retain information on facts of users' electronic communications (for 1 year), to ensure users' identification, and to provide access to the retained data to the Russian state authorities upon their legitimate requests. Moreover, from July 1, 2018, they will also have to retain content of such communications for a period of 6 months (based on well-known "Yarovaya Law'' of July 2016).

Audiovisual services / Video-on-Demand services

New rules came into force on July 1, 2017 and apply to the Internet services designed for distribution of audiovisual works through the Internet, that meet certain additional criteria. They, however, do- not apply to search engines, registered online mass media, and services where the content is generated by users.

The amendments have introduced a number of restrictions of foreign capital in the above video services and imposed a number of obligations on their owners (e.g., to publish their contact details for receipt of legal correspondence, to count number of users in Russian, to attribute the content with age rating etc.)

***

ADMINISTRATIVE FINES FOR DATA BREACHES HAVE BEEN RAISED

Before July 1, 2017, the Russian Code of the Administrative Offences (dated December 30, 2001) implied that the maximum fine imposed on legal entities for any violation of personal data laws and

regulations could be only RUR 10 000 (approx. EUR 145, USD 180). Since this date, the so-called *per breach approach* has been introduced and maximum limits of imposed fines have been raised.

At the moment, administrative fines are imposed based on the seven types of violations, and the maximum fine of RUR 75 000 (approx. EUR 1 100, USD 1 330) may be imposed on a legal entity processing personal data without data subject's written consent, where such consent is however required in accordance with the law (e.g. in case of cross-border transfer to "inadequate" jurisdiction, processing of sensitive and biometric data etc.). The fines are imposed in accordance with "per breach" approach.

****

CRITICAL INFRASTRUCTURE: WHAT IS THE LAW?

The Federal Law "On Security of Critical Infrastructure of the Russian Federation" (dated July 26, 2017 No, 187-FZ) came into force since January 1, 2018. It is expected that implementing regulations will be adopted later in 2018.

The key purpose sought by the Russian legislator, when adopting the law, was to ensure that private and publicly-owned facilities having social, economic, political, ecological and public security importance and operated in the specific industries (healthcare, science, transport, communications, defense, energy, banking and finance, fuel etc.) are effectively protected from cyber-attacks. For this reason, owners of such facilities will be subject to certain security standards and obligations to ensure lawful interception capabilities.

***

OUTSTANDING COURT CASES

Vkontakte vs. Double Data

The social network Vkontakte vs. Double Data case confirmed the position that personal data from public sources (e.g. social media) can be collected and used only for the purpose for which they were provided by a data subject. This means that using personal data from public sources, such as social media, for marketing, recruiting, automatic decision making, etc. is illegal without a separate, explicit consent of a data subject, or existence of other legitimate basis of data processing.

Telegram vs Federal Security Service

Earlier this year, Federal Security Service (FSS) requested, from the popular messenger Telegram, keys for decoding user messages.

Telegram refused to provide these codes and the FSS recorded this as an administrative offense. The company believes that the requirements of the FSS contradict the Russian Constitution and are technically unrealizable. It called the FSS's desire to gain access to personal correspondence "an attempt to expand its influence through the constitutional right of citizens."

FSS, in its reply to Telegram, referred to the Russian Law on information, according to which companies, included in the register of information dissemination, organizers (moderators) must share keys with the FSS to decode messages.

The court of first instance fined Telegram for RUR 800,000 (approx. USD 14 300 or EUR 11 600). The Appeal Court approved this decision.

This case is notable, due to the fact that Telegram has no legal presence in Russia and enforcement actions are aimed at a foreign legal entity.

Job applicants' data is covered by employment purposes

The Arbitrage Court of the Irkutsk Region has confirmed that the collection of job applicants' data is covered by employment purposes (and such purposes allow an exemption from the requirement on registration with Roskomnadzor) and no registration with Roskomnadzor is necessary.

Data processing consents need to be specific. Too general language should be avoided

The court confirmed that consents allowing the transfer of personal data to third parties must be sufficiently specific. In other words, it is not allowed to stipulate, for instance, that 'the controller is allowed to transfer personal data to third parties'. It is necessary to specify the relevant third party recipients with their full names and legal addresses, so that individuals can refuse to authorize such transfers.

Photos on ID documents are considered biometric personal data

Companies should take a closer look at the data they are collecting. Potentially, the companies may delete, or destroy, any documents with photos from ID documents as, otherwise, such processing requires the implementation of additional compliance measures, applicable to processing of biometric personal data.

***

ROSKOMNADZORINSPECTIONS IN 2018

Under the published list of scheduled inspections of Roskomnadzor in 2018, the main subjects of inspections are financial and credit organizations, as well as communication operators.

We hope that the information provided herein will be useful to 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 & Cybersecurity practice, please let us know 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 Maria Ostashenko, Partner of ALRUD Law Firm, at MOstashenko@alrud.com.

Sincerely,

ALRUD Law Firm

Note: Please be aware that all information provided in this letter was taken from open sources and does not constituent legal advice. The author of this letter and ALRUD Law Firm bear no liability for consequences of any decisions made in reliance upon this information.