

July 14, 2016

OVERVIEW OF LANDMARK LEGISLATIVE NOVELTIES IN THE AREA OF DATA PROTECTION AND PRIVACY

Dear Sir or Madam,

We are pleased to provide you with a brief overview of some recent significant amendments to the legislation in the area of data protection and privacy. The said amendments relate to **counterterrorism set of bills** (so-called “Yarovaya” law), introduction of the notion of **news aggregators** as well as restrictions on the activity of **debt collectors**.

COUNTERTERRORISM PACKAGE OF AMENDMENTS: NEW OBLIGATIONS DESIGNED TO EXPAND INTERNET SURVEILLANCE THAT MAY BE APPLICABLE TO YOUR BUSINESS

Counterterrorism package of amendments¹ has been recently adopted and sparked extensive public debate (“Counterterrorism Law”). For the last few years, this is a second anti-terrorism set of bills. The first one (adopted in 2014) laid down some statutory obligations that now have been expanded.

Key changes introduced by the Counterterrorism Law

The Law amends a dozen of laws relating to a new scope of obligations imposed on post offices, shipping agents and so on. The most crucial amendments in the area data protection and privacy are new obligations imposed on telecom operators (principally, they are now obliged to retain in the territory of Russia content of users’ communication for a period up to 6 months as well to retain information on receipt, delivery of such communications for a period of 3 years) and so-called **moderators of dissemination of information in the Internet** (“moderator(s)”). The formers are now obliged retain not only metadata and some types of personal data of users (as prescribed by 2014 anti-terrorism bill), but to retain also communications of users (content of messages) as well as enable state authority to decypher messages if moderator applies encryption (cryptographic) security tools. Failure to comply with the said obligations may result in imposing fine up to RUR 1 million (approx. EUR 14,000).

At what point compliance risks for your business emerge

Whereas new obligations imposed on telecom operators are relevant for quite restricted scope of companies, the notion of moderator due to its broad meaning and new scope of their obligations may imply some risks for quite large number of entities.

What companies shall be considered as moderators and therefore fall into the scope of the Counterterrorism Law

Statutory definition of moderators is indeed quite broad. They are defined as entities maintaining information systems and/or software, which are designed and/or used for the receipt, transfer, delivery and/or processing of e-messages in the Internet.

At first sight, such notion applies mainly to instant messaging, blogging, social media, public e-mails, etc. However, the broad and ambiguous definition makes it possible to apply the law to every website having forum or option of providing feedback for its users as well as companies maintaining corporate communication systems.

¹ Federal Law No. 374-FZ dd. 6 July 2016 “On making amendments to the Federal Law “On countermeasures against terrorism” and other legislative acts of the Russian Federation in part of establishing additional countermeasures against terrorism and measures for ensuring public security”

Some considerations on current industry practice

As current practice demonstrates, companies deemed moderators and falling into the scope of relevant statutory obligations are:

- Those who declared themselves as moderators (by way of filing notification with the Data Protection Authority) upon their own initiative and therefore included into the state register of moderators;
- Those who received from the Data Protection Authority a request to declare themselves as moderators and upon such declaration included into the state register of moderators. For the moment, such companies are mainly social networking website, blogging and public email services.

Due to this, it is unclear whether companies in essence meeting criteria set out in the statutory definition of moderators but not included into the state register, shall perform obligations imposed on moderators. In practice the companies concerned prefer waiting for receipt of the Data Protection Authority's request and do not perform any obligations until they are included into the register of moderators. At the same time, please pay attention to the fact that internal regulations of the Data Protection Authority allow it to hold an inspection of the companies who are not included into the state register (*de facto* moderators). This is possible mainly under the request of authorities in charge of carrying out operational investigation and responsible for the state security.

THE NEW LAW ON TAKING CONTROL OVER NEWS AGGREGATORS: WIDE-REACHING REGULATIONS

Russian lawmakers adopted rather controversial law² aimed at taking control over certain online information resources ("**Law**"). The Law introduces notion of so-called News Aggregators and impose on their owners a number of obligations. Below you may find a brief overview of the Law.

Who shall be considered as a News Aggregator?

The law defines News Aggregators as computer programs or web sites ("information resource(s)"), corresponding to the following features: (a) designed to process and distribute news via the Internet in Russian or other state languages of the Russian Federation, (b) may be used for disseminating advertisement targeting Russian consumers, and (c) have more than a million users (visitors) per day. Please note that foreign citizens and legal entities are prevented from owning a News Aggregator.

News Aggregators meeting the said criteria shall be included in the official register maintained by the Russian Federal Service for Supervision of Communications, Information Technology and Mass Media ("**Roskomnadzor**"). Once an information resource is registered as a News Aggregator, its owner shall be informed accordingly.

Obligations imposed on the owners of News Aggregators

The Law specifies a number of obligations, such as:

- To distribute information in accordance with mass media and other relevant Russian laws (e.g., to prevent violation of individuals' privacy as well as reproducing defamatory information, etc.);
- To prevent using News Aggregator for illegal purposes;
- To verify accuracy of the information on socially relevant topics (information of public importance) before uploading it (except for the information reproducing publications of duly registered mass media);
- To store information uploaded on News Aggregator, sources of such information and some other details within 6 months as well as to ensure provision of the access to such information for Roskomnadzor.

Roskomnadzor is authorized to monitor compliance with the Law (jointly with other competent state authorities) and may issue an order on immediate ceasing of dissemination of information and bring the owner of News Aggregator to liability (e.g., if information of socially relevant topics has been falsified or inaccurate information has been disseminated via News Aggregator, etc.).

Liability issues

The Law introduced some new types of administrative offences. E.g., failure by a News Aggregator to retain information a mandated by the Law may entail liability in the form of fine up to RUR 500,000 (approx. EUR 7,000). Non-compliance with the order of Roskomnadzor on ceasing dissemination of information may result in administrative fine up to 1 million RUR (approx. EUR 14,000). In the event of repeated violations, the fines may be increased up to 3 million RUR (approx. EUR 42,400).

² Federal Law No. 208-FZ of June 23, 2016 "On amending the Federal Law on Information, Information Technology and Protection of Information and the Code of Administrative Offences of Russian Federation" coming into force on 1 January, 2017

NEW RESTRICTIVE LEGAL FRAMEWORK ON ACTIVITY OF DEBT COLLECTORS

With increasing violence of debt collectors and in awake of some outrages allegations of the abuse on their part, Russian Parliament came up with the comprehensive law containing a number of restraints relating to activity of debt collectors³ (“Law”).

General overview of the key novelties

- The Law specifies that under general rule debts may be collected either by the creditors themselves or by special debt collection agencies, whose core activity shall be debt collection and who shall be included into the special state register.
- The Law explicitly set outs appropriate ways of communications with debtors (such as personal meetings, telephone conversations, e-mails, etc.) along with limiting the amount of those communications (e.g., not more than one personal meeting per week). Additional forms of communication may be implemented only if debtors agree.
- Under the Law, some forms of communication with debtor are prohibited (e.g. those relating to intimidating, endangering methods and so on).
- The Law prevent debt collectors (creditors) from liaising with third parties with regard to debt collection (including relatives and colleagues) without written consent of a debtor.
- It is also worth mentioning that under the Law disclosure of the information relating to a debtor (including, information disseminated via the Internet) is prohibited even if there is a consent of the debtor to such disclosure.
- Processing of personal data in accordance with the Law is a separate legitimate ground of data processing (unless Law requires obtaining consent of debtors).

Liability issues

Failure to comply with the Law by the creditor may trigger a fine for the entity up to RUR 200,000 (approx. EUR 2,828). The increasing fines would be applied to the debt collection agencies (up to RUR 500,000 (approx. EUR 7,063) or even administrative suspension of their business activity for a period of up to 90 days). Collecting debts by entities, which are not creditors or entities registered as debt collection agencies would trigger a fine up to RUR 2,000,000 (approx. EUR 28,285).

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 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 Law Firm – Maria Ostashenko (MOstashenko@alrud.com) or Irina Anyukhina (IAnyukhina@alrud.ru).

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.

³ Federal Law No. 230-FZ of July 3, 2016 “On protection of rights and legitimate interests of individuals” and on amendments to the Federal Law “On microfinance and microfinance organizations” came into force on July 3, 2016 and Federal Law No. 231-FZ of July 3, 2016 “On amendments to certain legislative acts of the Russian Federation related to the adoption of the Law” comes into force on January 1, 2017