Main approaches of enforcement practice in the area of data protection and positions of Roskomnadzor: practical guidance

alrud.com

ALRUD

Introduction

Dear Ladies and Gentlemen,

In recent years, the Federal Service for Supervision of Communications, Information Technology, and Mass Media ("**Roskomnadzor"**) and Russian courts have developed many positions and approaches that data controllers should take into account in their activities. Below, you can find some practical recommendations based on these positions and approaches, as well as on the practical experience of our lawyers. This review does not constitute legal advice. However, we believe that it can serve as a practical guidance for companies willing to ensure compliance with Russian personal data laws and to consider the practical aspects of their enforcement.

1. Most companies are obliged to notify Roskomnadzor on personal data processing

Under the Federal Law "On Personal Data", data controllers are obliged to notify Roskomnadzor of their intention to process personal data, except as otherwise provided by law. As a rule, data controllers do not file such notifications, relying on the exception enabling them to process personal data, in accordance with Russian labour laws.

Position of Roskomnadzor: The above-mentioned exception does not apply if the company processes personal data of former employees (for example, stores this data), or applicants for vacant positions.

Position of Roskomnadzor regarding the provision of information on the location of the databases in Russia: Companies that filed notifications to Roskomnadzor before September 1, 2015, shall submit updated information on the location of databases, used for personal data processing in the territory of the Russian Federation, within 10 days, starting from September 1, 2015. Companies, that have not sent updated information on time, shall do this as soon as possible.

2. Third parties, to whom employees' personal data is transferred, should be exhaustively listed in the consent for personal data transfer

In case of employees' personal data transfer to third parties and, if this transfer is not prescribed by law, it is necessary to obtain their written consent. Personal data laws set out requirements both for the form and the content of the consent. In particular, it is required to specify the names and addresses of third parties receiving data.

However, due to certain difficulties (for example, a large number of recipients of this information, frequent changes in their list and, consequently, the necessity to obtain new consents), data controllers indicate only categories of third parties (for example, affiliates, service providers, etc.), without indicating their specific names and addresses.

Position of Roskomnadzor: Any third party, to whom employees' personal data is transferred, shall be directly listed in a consent form, by indicating its name and address.

3. Peculiarities of manual processing of personal data shall be specified in the company's internal regulations

As a rule, data processing implies the use of automated means (e.g., electronic devices). However, some companies also carry out manual processing of personal data, e.g. by way of processing paper forms of potential clients and applications of employees. It should also be taken into account that there are some extra statutory requirements regarding such type of personal data processing.

Position of Roskomnadzor: Companies shall adopt detailed, internal regulations regarding peculiarities of manual processing of personal data, and other documents, required for carrying out such processing under current laws.

4. CVs of the applicants who were not selected for the job cannot be stored longer than 30 calendar days without consent of the data subject

As a rule, companies store information on job applicants who were not offered a job, e.g., for subsequent job opportunities.

Position of Roskomnadzor: Once a company rejects a job applicant, the purposes for which his/her personal data was initially collected are achieved. Therefore, personal data must be destroyed within 30 calendar days (as mandated under the Russian Law on Personal Data).

However, if the company implements internal policy on so-called personnel reserve (a database of applicants for subsequent job opportunities), it can store and process this data longer. In case of inspection, Roskomnadzor will check this policy and if it is not duly implemented, it will prescribe destruction of the data.

Position of the Moscow City Court in case No. 33a-3957 dated June 4, 2018 (McDonald's case): Storage of CV's, and consent on processing of personal data as a part of the employee's personal file, was recognized as a violation of data protection laws.

5. The processing of personal data of employees' relatives, if it exceeds the limits provided by labour legislation, is only allowed with the direct consent of these individuals

Under labour laws, an employer is obliged to inform employee's relatives in the event of an industrial accident. In this context, the employer may lawfully process the contact information of the employee's relatives. However, in practice, employers process a more extended scope of relatives' data (e.g., their occupation, presence/absence of a criminal record, etc.). Processing of this information cannot be justified by the necessity to comply with the requirements of the Labour Code.

Position of Roskomnadzor: If the employer processes a more extended scope of employees' relatives' data than required to fulfil obligations under the law, it is necessary to obtain consent directly from the employees' relatives.

6. If the access system, used in the company, is based on photo identification of employee, the company shall obtain written consent for processing of biometric data

Many companies use electronic access systems, with photo identification of employees (made by comparing the photo displayed on the computer, after the use of the electronic pass by the employee).

Position of Roskomnadzor: Under these circumstances, the photo is considered biometric personal data. In this regard, the employer is obliged to obtain employees' written consents, meeting statutory requirements to their form and content.

Position of the Supreme Court: Photographic images are treated as biometric personal data, because they describe a person's physical and biological characteristics, from which it is possible to identify this person. The order issued in this case, which related to the violation of the procedure for processing biometric personal data, is in line with current laws and does not violate the rights and legitimate interests of the enterprise.

7. Processing of former employee's personal data shall be based on consent

Many companies continue to process their former employees' data in information systems, longer than prescribed by data retention terms set out by law.

Position of Roskomnadzor: Processing of former employees' personal data, when it is not prescribed by law, shall be based on the consent of the data subject. Moreover, the peculiarities of legal grounds for this data processing, specific retention terms and data processing procedure should be governed by the company's internal regulations.

Position of the Moscow City Court in case No. 33a-3957 dated June 4, 2018 (McDonald's case): The absence of the company's internal personal data processing regulations, on the inclusion of rejected job applicants' and former employees' data in personnel reserve, as well as the absence of a separate written data subject's consent on the inclusion of the information, relating to them to the personnel reserve, constituted a violation of laws.

8. The company shall adopt rules for destruction of personal data

In practice, companies use shredders and some other similar means for destruction of documents. However, as a rule, companies do not have any detailed guidance on the destruction procedure for various types of personal data (including information stored in electronic information systems).

Position of Roskomnadzor: It is necessary to have internal regulations approving the procedure for destruction of personal data, depending on their type and means of processing, as well as special acts confirming the fact of their destruction.

9. Data subject's consent should cover only one purpose

Companies often indicate several purposes of processing in a written consent for personal data processing.

Position of Roskomnadzor and courts: According to the clause 4, part 4, art. 9 of the Federal Law "On Personal Data", written consent shall include "the purpose of personal data processing". Consequently, if the data controller processes personal data of one data subject for several purposes, and such processing requires written consent, it is necessary to request a separate data subject's consent for each purpose of processing.

10. The processing of data taken from social networks shall be compatible with the purposes of displaying such information in the social network

Many companies process personal data from social networks, considering that it is publicly available. However, such processing, in isolation from the purposes of the initial data collection, is considered a violation of personal data laws.

Position of Roskomnadzor and courts:
under personal data laws, information posted by users, on social networks, is not recognized as publicly available. Such data is processed on the basis of the user agreement between the data subject and the social network.

11. Although a telephone number is not considered personal data, advertising laws restrict usage of telephone numbers

Sometimes companies process only customers' and contractors' telephone numbers.

Position of Roskomnadzor: a telephone number, without additional information about the data subject, relates to the device, but not to the data subject, and its use, without additional information about the data subject, is not considered personal data processing.

The FAS position: It is not allowed to distribute advertising in communication networks, including telephone communications, in the absence of the subscriber's prior consent to receiving marketing messages. Violation of this requirement may entail an administrative fine of up to 500 thousand rubles.

12. Information contained in cookies, and in other analytical data, is considered personal data

Many companies automatically collect analytical data (cookies, MAC address, IP address). Sometimes, they believe that such information does not allow to identify a person and, therefore, it does not fall within the scope of personal data laws.

Position of Roskomnadzor and courts:
Automatically-collected data (cookies, MAC address, IP address) is considered personal data. It is necessary to comply with the personal data laws, when processing such data.

Position of the Tagansky District Court of Moscow in case No. 2-4261/18 dated December 19, 2018 (the website https://2019.vote/): The use of Google Analytics and Yandex Metrika services is considered to be the collection and processing of personal data. Information, about their use, shall be included in the privacy policy of data controller.

13. The processing of pseudonymized, personal data should be carried out in compliance with the requirements of personal data laws

Many companies pseudonymize personal data, in order to exclude such data from the scope of data protection laws and commercialize this data.

Position of Roskomnadzor and courts: processing of pseudonymized personal data allows indirect identification of the data subject. Pseudonymized personal data is still personal data, and processing of this data shall be carried out in accordance with the law.

14. Written consent may be obtained with the use of simple electronic signature

Position of Roskomnadzor: According to the position of Roskomnadzor's officials, which has been articulated in several public events in 2018 - 2019, a written consent may be obtained with the use of simple, electronic signature. At the same time, it is necessary to conclude an agreement on the use of a simple, electronic signature in advance.

In addition to the above-mentioned approaches of Roskomnadzor, we would also like to draw your attention to the following recommendations:

- In the course of audits/inspections, companies should be capable to prove that data processing procedures (for example, retention terms, pseudonymization procedures, destruction of data etc.), outlined in their internal policies, are actually being applied in practice.
- If a company has filed a notification on personal data processing, Roskomnadzor, in the course of audit/inspection, will verify whether information indicated in the notification is in line with actual data processing activities of that company. It is unacceptable to list, in the notification, all types of information contained in the law, in isolation from the actual activities of the company.
- Roskomnadzor will rely on the information specified in the company's internal documents on the processing of personal data, even if the company does not actually take any actions that are listed in these documents. For instance, if company's website indicates that data can be transferred to the United States, Roskomnadzor will assume that this processing actually takes place, and, therefore, may give rise to questions regarding legal grounds of such transfer.
- Roskomnadzor treats such information as IP addresses, information obtained via cookies, etc. as personal data (even if the company does not process any other additional information regarding individuals). In this regard, if the privacy policy on the website contains provisions related to the pseudonymized nature of the said data, these provisions should be changed. When developing internal documentation on the data processing, the company's website users should be considered to be data subjects whose personal data is processed by the company. It also applies to those visitors who do not have personal accounts on the website and do not provide their names and email addresses, since companies anyway are able to obtain their IP addresses.

Maria Ostashenko

Partner

mostashenko@alrud.com

We hope that the information provided herein will 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.

Please be aware that all information provided in this brochure was taken from open sources. Neither the ALRUD Law Firm, nor the authors of this brochure, bear liability for consequences of any decisions made in reliance upon this information

ALRUD Law firm
Skakovaya st., 17, bld. 2, 6th fl.
Moscow, Russia, 125040

T: +7 495 234 96 92
+7 495 926 16 48
F: +7 495 956 37 18
E: info@alrud.com

ALRUD