GRATA INTERNATIONAL

CLARIFICATIONS OF THE MINISTRY OF TELECOM AND MASS COMMUNICATIONS OF THE RUSSIAN FEDERATION AND THE FEDERAL SUPERVISION AGENCY FOR INFORMATION TECHNOLOGIES AND COMMUNICATIONS ON PERSONAL DATA PROCESSING AND DATABASES LOCALISATION IN RUSSIA

The following documents have been published on the web-portal of the Federal Supervision Agency for Information Technologies and Communications ('Roskomnadzor') focusing on the issues of personal data protection:

- Clarifications on the issues related to processing of personal data of employees, applicants for vacancies, as well as persons included in the employees pool, issued by the Ministry of Telecom and Mass Communications of the Russian Federation and Roskomnadzor;

- Commentaries to the Federal Law No. 242-FZ dated 21 July 2014 'On the Introduction of Amendments to Certain Legislative Acts of the Russian Federation in terms of Clarification of the Procedure for Personal Data Processing in the Information and Telecommunication Networks' (hereinafter - the 'Commentaries').

An overview of the most important provisions of the above documents is provided below.

I. Processing of Personal Data of Employees and Applicants for Vacancies

A. Cases in Which Employees' Consent for Data Processing Is Not Required

As a general rule, the employer may process personal data of an employee without the relevant consent:

- in cases provided for by the collective agreement, internal code of conduct, as well as local acts of the employer; and
- provided that the volume of personal data being processed by the employer does not exceed the respective lists and matches the goals of processing stipulated by the Russian labour legislation and laws on civil service.

In addition, the employer is not required to obtain consent to the personal data processing in the following cases:

1. An obligation to process personal data, including the duty to publish and place employees personal data in the Internet, is provided by Russian legislation: in particular, medical institutions must inform the public in an accessible form, including through the Internet, about the ongoing medical activities and medical staff, their level of education and qualifications[1].
2. The personal data of close relatives of an employee is processed in the volume stipulated by the unified form T-2. In other cases, processing of personal data of close relatives of an employee requires their prior consent.
3. Special categories of employees' personal data are processed, including health information relating to the capability of the employee to perform labour functions under the labour legislation[2].
4. Personal data of an employee is transferred to third parties in cases where it is required to prevent threats to life and health, as well as in other cases provided by the Labour Code of the Russian Federation or other federal laws, in particular:

---

[1] Article 79.1.7 of the Federal Law dated 21 November 2011, No. 323-FZ 'On the Fundamentals of Protection of Public Health in the Russian Federation'.

[2] Under Article 10.2.(2.3) of the Law 'On Personal Data'.

- to the Social Security Fund or Pension Fund of the Russian Federation;
- upon receipt of motivated requests from the prosecutor's office, law enforcement agencies, security agencies, state labour inspectors in the course of the state supervision and control over compliance with the labour legislation, and other bodies authorised to request information about employees.

That said, the employer may transfer personal data of an employee to credit institutions that open and service bank cards for payroll without the employee's consent provided that a contract for the issue of bank cards is entered directly between the employee and the credit institution and provides for the employer's right to transfer the personal data of the employee, or the employer have the relevant power of attorney to represent interests of the employee at the conclusion of a contract with the credit institution.

5. The personal data of an employee is processed for implementation of access control to the territory of the office premises of the employer, provided that the employer independently organises the access control or where such processing complies with the procedure provided for by the collective agreement, local acts of the employer.

   The employer may process personal data of dismissed employees without their consent in cases and within the terms specified by the federal legislation, including for the tax accounting (4 years) and accounting (within the time limits established by the state archiving guidelines, but not less than 5 years).

B. Processing of Personal Data of Applicants for Vacancies

The general rule is that an employer should obtain the consent of applicants for vacancies for their personal data processing for the period of adoption by the employer of a decision to hire or refuse in hiring the applicant.

Exceptions are the cases when:

- an applicant is represented by a recruitment agency under the relevant contract; or
- an applicant independently posted his/her CV in the Internet and made it publicly available.

If an applicant sends his/her CV by e-mail or fax, an employer must also take measures to verify whether the CV was sent by the respective applicant. At the same time, if it is impossible to identify an individual who sent the CV, such a CV must be destroyed when received.

If applicants' personal data are collected by means of a standard form questionnaire, such standard form must comply with the requirements of the Regulations on features of personal data processing performed without the use of automation means, as well as provide for the term of its consideration by the employer and taking a decision to hire or refuse in hiring the applicant.

In case of a refusal to hire an applicant, information provided thereby must be destroyed by the employer within 30 days (except for the cases stipulated by the legislation on civil service, where the term of keeping personal data of the applicant is 3 years).

The employer must also obtain an applicant's consent when making requests to other organisations, including former places of work, for obtaining clarification or detailed information on the applicant, except for the cases of recruitment of former state or municipal employees.

II. Processing of Personal Data through Information and Telecommunication Networks

The Federal Law No. 242-FZ dated 21 July 2014 'On the Introduction of Amendments to Certain Legislative Acts of the Russian Federation in terms of Clarification of the Procedure for Personal Data Processing in the Information and Telecommunication Networks' (hereinafter - the 'Law No. 242-FZ') that entered into force on 1 September 2015 established, in particular:

- the obligation of operators collecting personal data of Russian citizens, including through the Internet, to provide for recording, systematisation, accumulation, storage, updating, retrieval of such personal data with the use of databases located in the territory of the Russian Federation, except for certain cases mentioned in the Federal Law 'On Personal Data'[3]('Personal Data Law');
- the procedure for restriction of access to the information processed in violation of legislation of the Russian Federation on personal data[4].

A. Localization of Databases of Personal Data in Russia

In terms of the application of the requirements of the Law No. 242-FZ on the use of databases located in the territory of Russia when performing certain types of processing of personal data of Russian citizens, the Commentary generally repeats the clarifications of the Ministry of Telecom and Mass Communications published in August 2015 on its official web-site: the respective requirements apply to all persons (personal data operators), operating in the territory of the Russian Federation, i.e. to both Russian and foreign companies, including those operating without establishment of representative offices.

Commercial activity is considered to be carried out in the territory of Russia, according to the Commentary, if a foreign company's Internet site, through which it is operating, meets the following criteria:

1) uses the delegated domain name associated with Russia (.ru, .рф., .su); and(or)
2) there is a Russian language version of the Internet site created by the owner of the Internet site or on its behalf by another person (in this case, the use on the site or by the user of plug-ins that provide the functions of automated translators from various languages shall not be taken into account);

[3] Article 18.5 of the Federal Law dated 27 July 2006 No. 152-FZ 'On Protection of Competition'.

[4] Article 15.5 of the Federal Law dated 27 July 2006, No. 149-FZ 'On the Information, Information Technologies and Information Protection'.

3) a contract entered into through such Internet site may be performed in the territory of the Russian Federation (goods are delivered, services are rendered or digital content can be used in the territory of Russia).

According to the Commentary, an **Operator** is a person engaged in the processing of personal data or delegating the processing to a third party under a commission contract.

The Commentary does not provide for the explanation of the concept of 'personal data', indicating only that the information may be deemed personal data subject to compliance with the provisions of the Personal Data Law. However, when collecting publicly available personal data, operator's operations are subject to the requirements for the use of databases localized in Russia.

Database, according to all definitions provided for in Russian laws, is an ordered array of data independent of the type of physical storage media and means used for its processing (archives, filing rooms, electronic databases). A database, in particular, can be an Excel table or Word table, which contains personal data of citizens.

Performance of the 'data collection' obligation means that the operator must receive personal data directly from the subject of personal data or his/her representative. Having received the personal data from the subject, the operator is obliged to arrange recording, systematization, accumulation, storage, updating, modification, retrieval of such personal data with the use of databases located in the territory of the Russian Federation. These types of data processing constitute a single process of formation of and keeping the databases up to date.

A database formed by means of the collection of personal data shall be located as well as updated in the territory of Russia. This requirement applies in collecting personal data of Russian users within international geographically allocated systems, in particular, in the course of outsourcing services for human resource recordkeeping and accounting (i.e. by multinational corporations).

Thereat, when personal data collected is entered simultaneously (in parallel) into the Russian information system and the system located in the territory of a foreign state, the requirements of the Law No. 242-FZ are deemed not complied with.

If the personal data from the database (databases) located in the territory of Russia is transferred to another database (databases) located in a foreign country, it constitutes a cross-border data transfer. Such a transfer should be made in compliance with the requirements of Article 12 of the Personal Data Law: in particular, it should be made with specific and legitimate purpose and subject to the consent of the personal data subject, if necessary, provided in writing.

B. Restriction of Access to the Information Processed in Violation of the Personal Data Laws

Following the entry into force of the Law No. 242-FZ, an automated information system 'Register of Persons Violating the Rights of Personal Data Subjects' started operating in Russia' (the 'Register'). The Register includes domain names, URL-addresses of web pages of Internet resources that process personal data of Russian citizens in violation of the Russian legislation on personal data. The ground for inclusion of violators into

the Register is an effective judgement recognising the dissemination of information containing personal data as violation of the requirements of the Personal Data Law. In the practice of Roskomnadzor, defendants under the relevant claims are mainly determined through public whois-service in the Internet.[5]

When the violator eliminates voluntarily the respective breaches of the Russian legislation on personal data, the respective information is included into the Register. Otherwise, Roskomnadzor forwards to the operators the information on the respective Internet resource for the purposes of blocking access thereto, and the date and time thereof is also included into the Register.

The procedure for blocking access to an Internet resource may commenced not only on the ground of collection of personal data in violation of the Personal Data Law in terms of databases localization in Russia, but also due to:

- processing of personal data without legal grounds: an operator failed to obtain consent of the personal data subject to the processing; the operator is not legally entrusted with the functions, powers and duties for the dissemination of personal data through the Internet; the operator provides access to the public to publicly available personal data for the purposes and in the scope different from the purpose and scope of the initial collection of such data;
- an operator failed to place in the Internet the documents defining the operator's policy in relation of personal data processing and regulating the processing procedure and conditions.

According to the Commentaries, the Personal Data Law applies in full to the activities on dissemination through the Internet of personal data contained in archive documents.

The law provides for two legal grounds for exclusion of Internet resources from the Register:

- taking measures by an Internet site owner, hosting provider or operator to eliminate violations of the legislation on personal data;
- the entry into force of a court decision on cancelation of the previous court decision on the basis of which the information on the Internet resource was included into the Register.

Thereat, termination of an Internet site is not a legitimate ground for its exclusion from the Register.

Please note that the Commentaries, as they expressly state, are not of binding or advisory nature, but may be used in the course of activities of operators engaged in processing of personal data of Russian citizens.

[5]The first precedent for inclusion into the Register of persons violating the right of personal data subjects of a foreign social network and imitation of access thereto was the decision of the Tagansky Court of Moscow dated 4 August 2016 on the claim of Roskomnadzor against LinkedIn Corporation (USA), which is an administrator of the Internet - resources http: / /www.linkedin.com, http://linkedin.com. The decision was upheld by the appellate ruling made by the civil board of the Moscow City Court dated 10 November 2016.

****

Best Regards,

GRATA International Law Firm (Moscow)

This information is provided for your convenience and does not constitute legal advice. It is prepared for the general information of our clients and other interested persons and it may include links to websites other than the GRATA International website. This information should not be acted upon in any specific situation without appropriate legal advice.

What we do (in conjunction with a licensed provider in the area of information technology and personal data protection):

- comprehensive audit of information systems of personal data;
- development of the personal data protection system and recommendations to optimise data processing and protection;
- development of a set of organisational and administrative documentation on personal data protection;
- representation of client's interests during Roskomnadzor inspections.

Contacts:

Yana Dianova

Director of the Corporate and Commercial Law Department

GRATA International (Moscow)

Tel: +7 (495) 660 11 84

E-mail: ydianova@gratanet.com