About The Authors

Irina Anyukhina is ALRUD coordinating partner of Data protection, Intellectual Property and TMT practice areas. Irina has wide knowledge in protection of IPR in various industries, including in the digital environment, IPR licensing and assignment issues, enforcement in trademarks, patents and other IP-related issues. She specializes in data protection, IT and telecom, entertainment industry.

Irina's practice also covers advising on privacy and security compliance issues associated with cloud computing, mobile applications, big data, advertising and marketing and supply of computer and communications systems and software.

She is a member of the International Bar Association (IBA) and a member of the American Bar Association (ABA).

E-mail: IAnyukhina@alrud.com

Maria Ostashenko advice on personal data protection includes general issues of

Russia - Medical Data Processing

Irina Anyukhina, Maria Ostashenko and Anastasia Petrova

4 March 2016

1. Introduction

The Federal Law 'On personal data' No. 152-FZ dated July 27, 2006 ('the Law') primarily governs personal data protection in Russia. The Law encompasses the purposes, conditions and principles of personal data processing, which are to be observed by data operators, irrespective of the particular area they carry out activities in.

Issues may arise in different spheres such as medicine (which evokes such concepts as medical data and medical secrecy), communications services, employment relations, and so forth. Specifics of the particular data protection are implemented in respective statutory acts, such as the Federal Law N 323-FZ 'On basics of health protection of citizens of the Russian Federation' dd. 21.11.2011, Federal Law N 126-FZ 'On communication' dd. 07.07.2003, Labour Code (Federal Law N 197-FZ dd. 30.12.2001), as well as other specific laws and regulations.

Another integral part of the legal regime are regulatory acts issued by the Russian Government (such as government decrees), as well as regulations and guidance issued by state regulators such as the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications ('the Roskomnadzor'), the Federal Security Service (FSS) and the Federal Service for Technical and Export Control (FSTEC). Regulatory acts, regulations and guidance issued by these authorities are considered as statutory regulations aimed at implementing the provisions of the Law, which often appear to set forth only general principles and thus too broad . Such regulations and guidance must be taken into account since the Roskomnadzor, FSS and FSTEC have also enforcement powers and take part in controlling audits of companies.

Russia is a member of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data elaborated and adopted within the Council of Europe, as well as the Model Law on personal data elaborated and adopted within the Commonwealth of Independent States (CIS). Russian data protection laws and regulations must not contradict these international codes.In light of the statutory acts mentioned above, the Russian regime may be conceptually outlined as follows:

- Processing of personal data is permitted provided that there is a valid legal ground for such processing.
- Processing of personal data must be fair and not excessive; it must be limited by the purposes of processing which shall be defined in advance; and data operators must ensure the accuracy, sufficiency, and actuality for the purposes of processing;
- Storage of personal data in the form allowing identification of the data subject must be no longer than what is required. When the purposes of processing are achieved, personal data must be destroyed or depersonalised.

privacy under the Russian law, confidentiality obligations and disclosures of information under applicable restrictions and binding orders, as well as requirements applicable to data operators and persons involved in processing, structuring data flows within groups of companies among affiliates located in different jurisdictions, registration with the regulatory authorities (filing notifications with the Russian Data Protection Authority (Roscomnadzor), reviewing privacy policies for e-commerce and offline projects, conducting data protection compliance audits of company's activities in Russia, investigations of incidents with disclosure of information with limited access, representing the clients before Roscomnadzor, compliance of clients' IT infrastructure with localization requirements, etc. Maria is a member of the International Bar Association (IBA).

E-mail: MOstashenko@alrud.com

Anastasia Petrova advises foreign and Russian clients on a wide range of issues on maintenance of confidentiality and data protection. Anastasia's advice includes preparing documentation required for protection of confidential information and personal data, consultations on measures to be implemented for protection of personal data, bank secrecy regulations, filing with

2. Applicability of the Law

Russian personal data legislation is not applicable to: 1) the processing of personal data for personal/ household keeping purposes; 2) the processing of personal data in accordance with the Russian legislation on archiving documents; 3) processing of personal data having status of state secrets under the Russian legislation; and 4) processing of personal data in the course of disclosure of information on the courts' activity by competent state authorities.

3. Legal grounds for processing

The Law sets forth a limited list of situations in which personal data may be processed:

- with consent of a data subject;
- if processing is performed in accordance with labour laws, social security laws, pension laws;
- in order to carry out an agreement, to which a data subject is a party, beneficiary or guarantor;
- if processing is required for the protection of life, health, other vital interests of the data subjects, provided that obtaining consent is not possible;
- in order to carry out the rights and legal interests of the operator and third parties, provided that the rights and legal interests of data subjects are not infringed;
- processing for the purpose of mass media and journalism, provided that the rights and legal interests of data subjects are not infringed;
- processing of depersonalised data for statistical or other research purposes, except for marketing and promotion;
- processing of personal data which was made publicly available by a data subject; and
- other cases which are not widespread in practice.

The most common grounds for processing of personal data are processing with the consent of a data subject, in accordance with Russian labour laws, or in order to carry out an agreement, to which the data subject is a party, beneficiary or guarantor.

4. Specifics of data processing

Medical data implies information related to facts about an individual applying to medical institutions, information on an individual's state of health, diagnostics, and any other information obtained in the course of medical examinations and treatment. Such data is covered by the regimes of medical secrecy under the Federal Law N 323-FZ 'On basics of health protection of citizens of the Russian Federation' dd. 21.11.2011 ('the Law on Health Protection') and sensitive personal data under the Law which means stricter rules of confidentiality in comparison with ordinary personal data.

Medical data can be processed for limited number of purposes, namely for medical and prophylactic purposes, in order to establish a medical diagnosis, for the provision of health and medical and social services, provided that the processing of personal data is carried out by a healthcare professional who is obliged to maintain medical secrecy.

Disclosure of of medical data to third parties is subject to data subject's written consent and is possible only for the purposes of medical diagnosis and treatment, scientific

Regulatory authority, regulating data protection aspects in employment relations, including in international group of companies, adapting of foreign data processing and data transfer agreements, as well as policies for implementation and use in Russia, legal audits of compliance with data protection requirements. Anastasia also advices on recent Russian Data Localization Law and Right to be Forgotten Law.

Anastasia is a member of the International Bar Association (IBA).

E-mail: apetrova@alrud.com

researches, publishing in scientific media, use in educational processes and other similar purposes. However, this rule is subject to certain exceptions. Processing of medical data without the subject's consent is possible:

- in case of reasonable threat of dissemination of diseases, massive intoxications and large-scale damages;
- for the purpose of investigating industrial accidents as well as occupational illnesses;
- for the purpose of supervision and control of obligatory social insurance;
- for the purpose of controlling the quality and safety of rendered medical services;
- in the course of information exchange between medical institutions for the purpose of rendering medical services;
- upon request of the authorised Russian state authorities and courts and for the purpose of performance of their authorities;
- for the purpose of informing of parents or legal representatives of juniors who are provided with medical treatment
- for the purpose of informing state authorities, on the admission of a patient to a medical institution, provided that there is reasonable ground to assume that the damage to the patient's health is caused by the wrongful acts; and
- for the purpose of urgent medical treatment of an individual who, due to his/her state of health, cannot express his/her will and does not have any legal representative.

Information on the individual's state of health is deemed as 'sensitive personal data' in the context of the Law.

Special requirements for processing other specific categories of data Russian legislation provides for the protection of sensitive personal data (in terms of Russian legislation, 'special categories of personal data'), which implies all information concerning an individual's health, nationality, race, political/religious/ philosophical commitments, facts of private life and so forth.

This category of data may only be processed if:

- the data subject provided his/her written consent;
- the data subject made his/her personal data publicly available;
- processing is performed pursuant to an employment, pension, social security legislation, or other Russian legislation;
- processing is indispensable for the protection of life, health and legitimate interests of the data subject, provided that it is impossible to obtain the subject's consent and in some other specific cases;
- processing for medical and prophylactic purposes, in order to establish a medical diagnosis, for the provision of health and medical and social services, provided that the processing of personal data is carried out by a person professionally engaged in medical activities who is obliged to maintain medical secrecy regime; and

- other cases.

Biometric personal data is subject to a higher level of protection. This category of data is defined as information pertaining to the physical or biological characteristics of a person which makes it possible to identify a particular individual, and which is processed by an operator for the purpose of identification.

Biometric personal data may be processed only upon the written consent of the data subject, or without it if required by Russian laws or international treaties to which Russia is a party or, in some other cases, as directly prescribed by Russian laws.

5. Consent

Consent of a data subject shall be informed, clear and explicit. The data operator must be able to prove that consent has been obtained.

In certain cases, consent for processing of personal data must be obtained strictly in writing. ritten consent shall be executed in the form of a hard copy and contain the signature of the data subject, or it may be executed in an electronic format, provided that it is signed by digital signature.

Written consent must contain specific information prescribed under Russian data protection laws.

6. Additional requirements around consent

One of the areas, where additional requirements related to the form of consent are applicable, is the conduct of clinical trials. There are certain national standards and regulations which primarily set forth the obligation of the trial investigator to obtain the so-called informed consent of trial subjects. Such consent should contain certain information, including, for example, information on medication and key points of the clinical trial of the medication, expected efficiency of the medication, risks for the trial subjects, the terms of the insurance of trial subjects, and so forth.

The draft of the informed consent should be preliminarily approved by an ethics committee that should be formed as an independent expert body. All information indicated in such informed consent should be clear and comprehensive. It must contain a minimum of specialised terminology. It must not contain any statement restricting the scope of liability of trial investigators, or any statement forcing trial subjects to waive their statutory rights.

Informed consent can be amended in the course of the trial and this new version must be communicated to trial subjects.

All data on trial subjects should be systematised in the so-called 'individual record book of the trial subject'. All trial subjects are assigned a special identification code to protect their anonymity. These codes are used in the trial reports.

Please note that consent for processing sensitive personal data (including medical data) must be obtained strictly in writing.

Written consent is also required in the following cases:

- transfer of employees' data to third parties;
- processing of biometric data;
- transfer of personal data to countries which do not provide adequate protection of personal data; and

- implementation of a decision taken according to a result of automated processing of personal data, provided that such decision entail certain legal consequences for a data subject.

7. Engaging third parties

With the consent of data subjects, data operators can transfer personal data to a person processing such data on behalf of the data operator (upon assignment of data operator) based on the agreement concluded with such person. Such agreement and/or data operator's assignment must contain specific information, provided for under the Law, in particular, on the confidentiality and security obligations of the data processor, the obligation of the data processor to ensure a level of protection as required by the Law, categories of processed data, actions with such data, and other information. The data operator is liable for the actions of its data processors vis-a-vis the data subjects, while data processors may be held liable in front of data operators on a contractual basis.

8. Specific requirements around cross-border data transfers

Transfers are considered as data processing and, by general rule, require the prior consent of the data subject.

Requirements around consent forms depend on the country to which data is transferred. The key criterion in this regard is the adequacy of the protection applied to the data. In the absence of adequate protection, cross-border transfers may be allowed if it is performed based on the agreement concluded with a data subject.

If personal data is transferred to countries not considered as providing adequate protection, the consent for such transfers must be obtained strictly in writing. According to the Law, countries providing adequate protection of personal data are parties to the Convention of the European Council on Protection of Rights of Individuals in case of Automated Processing of Personal Data, as well as other countries approved by the Roskomnadzor (for example, Switzerland, Australia, Israel, Korea and Chile, among others). If personal data is transferred to countries considered as providing adequate protection, consent may be obtained in any form subject to certain conditions (except for cases of processing employee data).

In order to transfer data for processing by the third parties, the operator must conclude contracts with such third parties (e.g., through data processing or data transfer agreements - the EU standard contractual clauses may be used after some adaptation to the Russian law). Security measures must be implemented in order to protect data in the course of those transfers.

Transfers of medical data require mandatory written consent of data subjects, irrespective of the country to which data is being transferred. It is also recommended to be more prudent with regards to ensuring security and confidentiality of such data in the course of its transfer.

9. Data Security

Information systems used by data operators to process data must ensure the confidentiality and security of the data, and comply with the requirements of Russian laws. Operators must adopt legal, organisational and technical measures necessary to protect personal data against unlawful or accidental access and destruction, alteration, blocking, copying, provision or dissemination of personal data and against other unlawful actions in relation to personal data. Russian personal data laws provide for a list of particular measures to manage the security of data.

Additionally, the legislation sets forth the four levels of data protection processed within information systems. Each level determines the particular security measures which must be adopted. The required level of protection must be determined upon legal and technical audit of IT system and personal data processing existing in a company. Specialists are required in order to determine the required level of protection in terms of IT or information security.

10. Notification

All data operators must be registered as data operators as part of the register maintained by the Roskomnadzor. For this purpose, they must file a notification to the Roskomnadzor, prior to the commencement of processing (this obligation is subject to certain exceptions). Notification must take place in accordance with the statutory form and signed by the head of a company.

The Roskomandzor has 30 days for considering the application and may request additional information from the operator (if the provided data is not sufficient) before including it in the register.

11. Data localization requirements 15

Requirements on processing of personal data of Russian citizens in Russia (hereinafter – the "**Localization Law**") came in force on September 1, 2015.

The Localization Law covers processing of personal data belonging to Russian citizens, including medical data. It requires operators of personal data to ensure that certain types of processing of personal data relating to Russian nationals (including the collection of such data via the Internet) is conducted using databases located in the territory of Russia. Russian data operators must inform Russian data protection authority (Roskomnadzor) on location of databases processing Russian citizens personal data.

Transfer of personal data outside of Russia (which is subject to compliance with Russian cross-border data transfer requirements) is not prohibited by the Localization Law which requires that the primary database of personal data relating to Russian citizens is kept in Russia without restrictions for copying data and sending abroad subject to the rules applicable to cross-border transfers of data and disclosures of medical data.

Obligations to keep personal data in Russia cannot be contracted out of, even with data subject's consent.

The Localization Law is applicable to the following methods of processing of the personal data at the moment of their collection, namely:

- Recording;

- Systematization (or organization);
- Accumulation (or aggregation);
- Storage;
- Clarification (update and amendment);
- Extraction

A. (hereinafter together referred to as the "target types of processing").
B. The Localization Law applies only to Russian citizens' personal data collected by directly from data subjects or collected through third parties engaged for processing of these data on behalf of the data operator. The Localization Law does not apply to the data obtained by data operators from third parties where those third parties collected the data from Russian citizens on their own behalf.
C. Personal data must be initially collected in a so-called "primary database", which must be located and maintained (to the extent maintenance involves the target types of processing), in Russia. Personal data contained in the primary database may be transferred abroad into other databases (secondary databases) if Russian cross-border transfer rules are complied with.
D. The Localization Law does not apply to data collected in databases abroad before the 1 September 2015 as long as such data remains unchanged and is not subject to the target types of processing outside Russia. If the target types of processing are carried out with such data as of the 1 September 2015, data operators must comply with their obligations under the Localization Law by moving the data to Russia to be maintained in a Russian database.

12. Enforcement actions

Russian legislation provides for a range of penalties and adverse consequences for those violating the legislation.

Criminal liability is established as follows:

Violation of the right to privacy (which is the illegal collection or dissemination of information on the private life of an individual, which constitutes his/her personal or family secrecy, without his/her consent, or the distribution of this information in a public performance, in a publicly performed work, or in the mass media) will result in:

- fine in the amount of up to 200,000 RUR, or in the amount of the salary or other income of the convicted person for a period of up to 18 months;
- obligatory work for a term of up to 360 hours;
- corrective work for a term of up to one year;
- compulsory work for a term of up to two years accompanied by deprivation of the right to hold certain positions or be engaged in certain activities for a term of up to three years or without such;
- detention for a term of up to four months; or
- imprisonment for a term of up to two years along with deprivation of the right to hold certain positions or be engaged in certain activities for a term of up to three years.

Violation of the privacy of correspondence, telephone communications, mail, cables, or other communications of individuals, will result in:

- a fine of up to 80,000 RUR, or in the amount of the salary or any other income of the convicted person for a period of up to six months;
- obligatory work for a period of up to 360 hours; or
- corrective work for a term of up to one year.

Illegal access to computer information protected by law if such access resulted in destruction, blocking, modification or copying of computer information will result in:

- a fine in the amount up to 200,000 RUR, or in the amount of the salary or any other income of the convicted person for a period of up to 18 months;
- corrective work for a term of up to 1 year;
- custodial restrain for a term of up to 2 years;
- compulsory works for a term of up to 2 years;
- imprisonment for a term of up to 2 years.

Criminal liability is not applicable to legal entities, only to individuals.

Violation of personal data legislation further carries administrative liability as follows:

- Violation of an established order on processing, storage, use and dissemination of data will result in an official warning and administrative fine for a company, as well as its officers, of up to 10,000 RUR.
- Use of non-certified information systems, databases and technical means of information protection (if those are subject to an obligatory certification requirement) will result in an administrative fine for a company as well as its officers, with a fine of up to 25,000 RUR.
- Failure to perform statutory requirement to provide information to a state authority will result in an official warning and administrative fine for a company and its officers, with the amount of fine set at 5,000 RUR.
- Violation of employment legislation (if personal data of employees are processed) will result in an administrative fine for a company and its officers, with the amount of fine set at 50,000 RUR.

Breaches may also lead to civil litigation since subjects are entitled to claim reimbursement of damages incurred - including moral damages - due to the unlawful processing of their data, as well as requiring removal, destruction, elimination and ban of further dissemination of information related to non-monetary personal benefits.

In addition to the above, the Roskomnadzor is entitled to restrict access to the information resource of an operator (if any) who is violating the personal data legislation, effective as of Semptember 2015.

13. Conclusion

Russian personal data regulation is rather extensive. We would like to outline the key legal considerations which shall be taken into account by the entities in the course of processing of medical data:

- Generally speaking, the processing of medical data shall be lawful and proportionate (not extensive). Such data will be processed for specified purposes only and will not be processed in any manner incompatible with such purposes.
- As a general rule, transfers of medical data to third parties require the written consent of data subjects or other legal grounds, as provided for under applicable law.
- In the course of medical data processing, especially transfers of data to the third parties, the increased level of security and confidentiality of personal data must be maintained since a violation of medical data confidentiality may also be deemed as the violation of an individual's privacy. This may entail criminal liability.
- When transferring data abroad, the operator must comply with the Russian data localization requirements effective as of the 1 September 2015 and Russian cross-border transfer rules.
- When organising clinical trials, the operator must obtain informed consent from trial subjects, depersonalise data obtained, as well as follow other requirements established under the special statutory regulations applicable to clinical trials.