DATA PROTECTION LAWS OF THE WORLD

Russia

DLA PIPER

RUSSIA

Last modified 15 January 2021

LAW

Fundamental provisions of data protection law in Russia can be found in the Russian Constitution, international treaties and specific laws. Russia is a member of the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention) (ratified by Russia in 2006) and the Russian Constitution establishes the right to privacy of each individual (articles. 23 and 24). Most rules are found in specific legislation, particularly the Data Protection Act No. 152 FZ dated 27 July 2006 (DPA) and various regulatory acts adopted to implement the DPA as well as other laws, including the Information, Information Technologies and Information Protection Act No. 149 FZ dated 27 July 2006 establishing basic rules as to the information in general and its protection. In addition, the Russian Labour Code contains provisions on the protection of employees' personal data (Part XIV). Other laws may also contain data protection provisions which implement the provisions of DPA in relation to specific areas of state services or industries.

On 22 July 2014 notable amendments to the DPA were adopted and came into force on 1 September 2015. The amendments require all personal data operators to store and process any personal data of Russian individuals within databases located in Russia (subject to few exceptions). The penalty for violation of this requirement is ultimately the blocking of websites involving unlawful handling of Russian personal data. A Register of Infringers of Rights of Personal Data Subjects shall be established by the *Roscomnadzor* and from there and the *Roscomnadzor* may move to block websites.

As the amendments are newly passed and a track record of enforcement and legal interpretation has not been established, it is still unclear as to how this register and the website blocking would work in practice. According to clarifications of Russian regulators, storing and processing of personal data of Russian individuals outside of Russia can still be compliant with the law as long as primary (often interpreted as initial) storage and processing of data is done in Russia. It is still an open question whether keeping "mirror" databases in Russia and elsewhere would be deemed as compliant.

DEFINITIONS

Definition of personal data

Personal data is defined in law as any information that relates directly or indirectly to the specific or defined physical person (the data subject). This can be widely interpreted in various contexts, so it is important to consider each situation carefully.

Definition of sensitive personal data

Sensitive personal data is defined as special categories of personal data in Russian legislation. Such special categories include data related to race, national identity, political opinions, religious and philosophical beliefs, health state, intimacies and biometrical data.

NATIONAL DATA PROTECTION AUTHORITY

Federal Service for Supervision of Communications, Information Technologies and Mass Media or, in short, *Roscomnadzor*

('Agency')

Build. 2, 7, Kitaigorodskiy proezd
Moscow, 109074

T +7 495 987 6800
F +7 495 987 6801

http://www.rsoc.ru/

REGISTRATION

The Agency is in charge of maintaining the Registry of Data Controllers.

Any data controller shall notify the Agency in writing about its intention to process personal data, unless one of the following exclusions applies:

- the personal data is exclusively data about employees;
- the personal data was received in connection with a contract entered into with the data subject, provided that such data is not transferred without the consent of the data subject, but used only for the performance of the contract and entering into contracts with the data subject (for example, data provided by a customer purchasing a product online and the data is used only to fulfil the order);
- the personal data is the data about members of a public or religious association and processed by such an organisation for lawful purposes in accordance with their charter documents, provided that such data is not transferred without the consent of the data subjects;
- the personal data was made publicly accessible data by the data subject;
- the personal data includes the surname, name and father's name only (Russia uses patronymic references in place of "middle" names);
- the personal data is necessary in order to give single access to the premises of the data controller or for other similar purposes;
- the personal data is included in state automated information systems or state information systems created for the protection of state security and public order;
- the personal data is processed in accordance with the law without any use of automatic devices; or
- the personal data is processed in accordance with transportation security legislation for the purposes of procurement of stable and secure transport complex and personal, community and state interests protection.

The notification letter shall contain information about:

- the full name and address of the data controller;
- the purpose of the processing;
- the categories of personal data processed;
- the categories of the subjects whose personal data is processed;
- the legal grounds for processing;
- the types of processing of the personal data;
- the measures of protection of personal data;
- name and contact information of the physical person or legal entity responsible for personal data processing;
- the commencement date;
- information on occurrence of cross border transfer of personal data;
- the term of processing or the conditions for termination of processing the personal data; and
- information on personal data security provision.

DATA PROTECTION OFFICERS

If the data controller is a legal entity, it is required to appoint a data protection officer. Such an appointment is considered to be a personal data protection measure. The data protection officer oversees compliance by the data controller and its employees

regarding the data protection issues, informs them of statutory requirements and organises the receiving and processing of communications from data subjects.

There are no legal restrictions as to whether the data protection officer should be a citizen or resident of the Russian Federation, however, it is adviseable that the data protection officer is available in case there is an inspection or other communication from the authorities.

Non-appointment or improper appointment of the data protection officer is a violation of the data protection regime and may result in the imposition of penalties and enforcement protocols, as described below.

COLLECTION & PROCESSING

Data controllers may collect and process personal data where any of the following conditions are met:

- the data subject consents;
- the processing is required by a federal law or under an international treaty;
- the processing is required for administration of justice, execution of a court order or any other statements of public officers to be executed;
- the processing is required for provision of state or municipal services;
- the data controller needs to process the data to perform or conclude a contract to which the data subject is a party or beneficiary party or guarantor;
- the processing is carried out for statistical or scientific purposes (except where processing is used also for advertising purposes) provided that it is impersonalised;
- the processing protects the data controller's vital interests and it is impossible to have the data subject's consent;
- the processing is required for execution of statutory controller's or third parties' rights or for purposes important for the community provided the data subject's rights are not in breach;
- personal data that is processed was publicly made accessible by the data subject or upon his or her request;
- the processing is carried out by a journalist or mass media as a part of its professional activities or for the purposes of scientific, literary or other creative activities, except if the processing would damage the data subject's rights and freedoms; or
- personal data that is processed is subject to publication or mandatory disclosure under law.

As a general rule, consents by a data subject may be given in any form, but it is the data controller's obligation to provide proof that he has the data subject's consent. Because of this burden of proof, it is important to keep careful records of consents.

In the following cases, the DPA requires that the data subject's consent should be in writing (preferably in hard copy form):

- where the personal data is collected to be included within publicly accessible sources;
- where sensitive or biometrical data is processed;
- in the case of the cross border transfer of personal data, where the recipient state does not provide adequate protection of personal data; or
- where a legally binding decision is made solely on the grounds of the automated processing of personal data.

Consent is deemed to have been given in writing where it is signed by hand or given in an electronic form and signed by an electronic signature.

Consent may be revoked.

Consent in writing must contain the following information:

- the identity of the data subject, his/her address and passport details and identity of the subject;
- data representative (if any);
- the identity and address of the data controller or the entity that processes personal data on behalf of the data controller (if any);
- the purpose of the processing;

- the list of personal data that may be collected and processed;
- the types of processing that are authorised;
- the term for which the consent, remains valid and way of revocation; and
- the data subject's signature.

The data controller shall ensure the confidentiality of personal data. The data controller and other persons who have access to the personal data, shall not disclose any information to a third party without the prior consent of the data subject.

TRANSFER

Prior to a transfer of personal data out of Russia, the data controller must ensure that the recipient state provides adequate protection of personal data. The fact that the recipient state ratified the Convention is sufficient grounds to deem that the state provides adequate protection of personal data for the purposes of the DPA.

Where there is no adequate protection of personal data, a cross border transfer is permitted if one of the following conditions is met:

- the data subject consents;
- the transfer is provided for under an international treaty to which Russia is a signatory;
- the transfer is necessary in accordance with federal laws for protection of the Constitution, state defence, security and transport system;
- for the purposes of performance of a contract to which the data subject is party; or
- the transfer protects the data subject's vital interests where it is not possible to get the written consent of the data subject.

In addition to the above, the *Roscomnadzor* issued the Order No. 274 of 15 March 2013 '*On endorsement of the List of the Foreign States Which are Not Parties to the EC Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data*'. The Order contains the list of countries which are officially recognized by Russian authorities as 'ensuring adequate protection'. Apart from the Member States of the Convention, there are 23 so 'white-listed' states as of today.

SECURITY

Data controllers are required to take appropriate technical and organisational measures against unauthorised or unlawful processing and accidental loss, changing, blocking or destruction of, or damage to, personal data.

A recent special regulation sets forth certain measures that the data controller should undertake to ensure security of personal data, data systems, carriers of biometrical information and technologies.

BREACH NOTIFICATION

There is no mandatory requirement to report data security breaches or losses to the Agency or to data subjects.

ENFORCEMENT

In Russia, the Agency is responsible for the enforcement of the DPA. The Agency is entitled to:

- carry out checks;
- consider complaints from data subjects;
- require the submission of necessary information about personal data processing by the data controller;
- require the undertaking of certain actions according to the law by the data processor, including discontinuance of the processing of personal data;
- file court actions;
- initiate criminal cases; and
- impose administrative liability.

If the Agency becomes aware that a data controller is in violation of the law, he can serve an enforcement notice requiring the

data controller to rectify the position.

A data controller can face civil, administrative or criminal liability if there is a violation of personal data law. Officers of the data controller responsible for the offence may also face disciplinary action.

Usually, in the case of violation of data protection law, the Agency will serve an enforcement notice requiring the position to be rectified and may also impose an administrative penalty and/or recommend imposing disciplinary action on the officers of the data controller who are responsible for the offence.

The maximum administrative penalty that can be imposed, as at the date of this review, is RUR (Russian Rubles) 75,000.

ELECTRONIC MARKETING

Electronic marketing activities are subject to limitations set by the Russian Law on Advertising No. 38-FZ dated 13 March 2006, under which the distribution of advertising through telecommunications networks, in particular, through the use of telephone, facsimile and mobile telephone communications, is allowed only subject to preliminary consent of a subscriber or addressee to receive advertising.

Advertising is presumed to be distributed without preliminary consent of the subscriber or addressee unless the advertising distributor can prove that such consent was obtained. The advertising distributor is obliged immediately to stop distribution of advertising to the address of the person who made such a demand.

ONLINE PRIVACY

Russian law does not specifically regulate online privacy. The definition of personal data under the DPA is rather broad and there are views that information on number, length of visits of particular web-sites and IP address (in combination with other data allowing the user to be identified) could be considered personal data.

KEY CONTACTS

Michael Malloy
Counsel and Head of Intellectual Property and Technology Practice
T +7 495 221 4400
michael.malloy@dlapiper.com

Pavel Arievich
Legal Director
T +7 495 221 4472
pavel.arievich@dlapiper.com

Ekaterina Golodinkina
Associate
T +7 495 221 4546
ekaterina.golodinkina@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.