DATA PROTECTION LAWS OF THE WORLD

Russia

DLA PIPER

RUSSIA

Last modified 17 January 2024

LAW

Fundamental provisions of data protection law in Russia can be found in the Russian Constitution, international treaties and specific laws.

Key legislation includes (but is not limited to):

- Federal law No. 152 FZ of 27 July 2006, “On Personal Data” (the Data Protection Act or DPA);
- Federal law No. 149-FZ of 14 July 2006, “On Information, Information Technologies and Protection of Information” (the Information Law); The Labor Code of the Russian Federation; and The Constitution of the Russian Federation.

The DPA is the most comprehensive source for Russia data protection rules and contains most of the provisions setting forth most of the provisions discussed herein. The Information Law sets forth rules related to information in a broader context and the Constitution provides for even broader rights to privacy (Articles 23 and 24). The Labor Code contains specific provisions for data protection in employment relationships.

Russia is a member of the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the Convention) (ratified by Russia in 2006).

DEFINITIONS

Definition of personal data

Personal data is defined in law as any information which relates directly or indirectly to a 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. While not specifically included as “sensitive” personal data, there are special rules for handling criminal records, so this should also be considered as sensitive.

Definition of biometric personal data

Biometric personal data is defined as information on physiological and biological features of a person, on the basis of which it is possible to and is used to establish the data subject’s identity. The definition of biometric personal data requires the data operator’s use of the information to identify the data subject.

Definition of personal data authorized by the personal data subject for dissemination

Intended to capture circumstances where a data subject has provided information or has given authorization for the dissemination of information to the public (mainly online), Russian law features a defined type of personal data as "personal data authorized by the personal data subject for dissemination.” The focus of the definition is not so much on the nature of the personal data itself, but the data subject’s authorization for its dissemination.

Data Operator

Russian law does not distinguish between “data controllers” and “data processors” in nearly all circumstances. Instead, the reference is to “data operators”.

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

Telephone

+7 495 987 6800

Fax

+7 495 987 6801

Website

rsoc.ru/

REGISTRATION

Russian law requires all data operators to notify the data regulator in writing about its intention to process personal data, unless very few narrow exclusions apply. The Federal Service for Supervision of Communications, Information Technology and Mass Media or “*Roskomnadzor*” (the Agency) is the data regulator for Russia.

The notification is made in a letter format and should contain the following information:

- the name and address of the data operator;
- the purpose of the processing;
- the measures of protection of personal data;
- name and contact information of the physical person or legal entity responsible for personal data processing;
- the data processing commencement date;
- information on occurrence or absence of cross border transfer of personal data;
- the term of processing or the conditions for termination of processing the personal data;
- information on personal data security provision;
- information on location of the database containing personal data of Russian citizens; and
- the name of the person or legal entity having access to and (or) carrying out the processing of personal data (based upon a contract) contained in state and municipal information systems.

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

- The data subject consents;
- The processing is required by 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 operator needs to process the data to perform or conclude a contract to which the data subject is a party, a 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 depersonalized;
- The processing protects the data subject’s vital interests and it is impossible to obtain the data subject’s consent;
- The processing is required for execution of the data operator’s or third parties’ rights or for purposes important for the community, provided the data subject’s rights are not infringed;
- The processing is carried out by a journalist or media organization as a part of its professional activities or for the purposes of scientific, literary or other creative activities, except if the processing would infringe upon the data subject’s rights;
- The personal data is subject to publication or mandatory disclosure under law; or
- The personal data that is processed by participants under the conditions set forth in an experimental regulatory regime (sometimes referred to as a “regulatory sandbox") in depersonalized form.

Consent by the data subject is by far the most common legal basis for data processing in Russia. In most cases, consent may be given in any form, but it must be in some tangible format, as the data operator bears the burden of proof to show that consent was given, so, it is important to keep careful records of consents.

In some cases, however, DPA requires an explicit written consent:

- where the personal data is allowed by the data subject for dissemination;
- where sensitive or biometrical data is processed;
- where a legally binding decision is made solely on the grounds of the automated processing of personal data; or
- where employee personal data is transferred to third parties.

Consent is deemed to have been given in writing where it is signed by hand or in electronic form with a digital signature.

Written consent (except personal data allowed by the personal data subject for dissemination – there are special rules for this) must contain the following information:

- The identity of the data subject, (which can be made by reference to residential address and passport details);
- Identification of a data representative (if any);

- The identity and address of the data operator or the entity that processes personal data on behalf of the data operator (if any);
- The purpose of the processing;
- The list of personal data which may be collected and processed;
- The authorized types of processing;
- The term for which the consent remains valid;
- Means for revocation of consent; and
- The data subject’s signature.

For personal data allowed by the personal data subject for dissemination there must be a separate form of consent containing following information:

- Full name of the data subject;
- Contact information for the data subject (telephone number, e-mail address or postal address);
- Information on the data operator, including name, registered address, taxpayer identification number, and state registration number (if known to the data subject);
- Information about the information resources of the data operator, through which the processing of the personal data and access to the data will be provided, including identification of the protocol (http or https), server (www), domain, the directory on the server and file name of the web page;
- Purpose(s) of personal data processing;
- Descriptions of the personal data for which the consent is given, including “standard” personal data, any special categories of personal data, and any biometric data;
- Categories and list of personal data, for which the data subject establishes conditions and prohibitions;
- Conditions under which the personal data may be transmitted by the operator only through its internal network, providing access to information only for strictly defined employees, or using information and telecommunication networks, or without transmitting the personal data (to be filled in at the request of the personal data subject);
- The period of validity of the consent.

Consent in any case may be revoked at any time.

A key feature of Russian personal data law involves what is often referred to as the “Data Localization Rule” instituted in 2015. The Data Localization Rule requires all 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 and fines up to ₽6 000 000 and up to ₽18 000 000 for repeated violations.

According to DPA, storing and processing of personal data of Russian individuals outside of Russia can still be compliant with the law as long as the primary (often interpreted as initial) storage and other processing activities prescribed by DPA is done in Russia. As one can imagine, compliance with the Data Localization Rule can be complicated for international data operators.

TRANSFER

According to recently adopted amendments to the law, prior to a transfer of personal data out of Russia, the data controller must notify Roskomnadzor on cross-border data transferring.

The law distinguishes between the countries that provide adequate protection of personal data and countries that do not provide adequate protection of personal data. This differentiation impacts the procedure of data transferring as commented below.

The fact that the recipient state ratified the Convention is sufficient ground to deem that the state provides adequate protection of personal data for the purposes of the DPA.

In addition to the above, the *Roskomnadzor* 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.

In connection to both types of countries Roskomnadzor has the right to restrict cross-border transfers. For the countries which provide the adequate protection of personal data the controller must notify Roskomnadzor beforehand but may commence the cross-border data transfer without waiting for Roskomnadzor’s express or tacit approval of the transfer (and has to discontinue such transferring if Roskomnadzor objects). For the countries which do not provide the adequate protection of personal data for the purposes of the DPA, the transfer to those countries is not permissible until Roskomnadzor issues the express or tacit approval within the statutory set timeframes.

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

Under the recently adopted amendments, in case of establishing the fact of unlawful or occasional transfer or dissemination of personal data, that caused a violation of data subject rights, the data controller must:

- within 24 hours notify *Roskomnadzor* about:
  - the incident;
  - believed reasons that caused violation of data subject rights;
  - estimated harm inflicted to data subject rights;
  - measures taken to cure consequences of the incident; and
  - details of the contact person to communicate with *Roskomnadzor*.
- within 72 hours notify *Roskomnadzor* about the results of internal investigation of the incident as well as to provide the information on the parties, if any, whose actions caused the incident.

The above timeframes are very short that may cause significant practical difficulties in complying with them.

ENFORCEMENT

In Russia, the Agency is responsible for the enforcement of data protection rules. The Agency is entitled to:

- carry out checks;
- consider complaints from data subjects;
- demand necessary information about personal data processing by the data operator;
- order the data operator to undertake certain actions according to the law, including discontinuance of the processing of personal data;
- file court actions;
- initiate criminal cases; and
- impose administrative liability for violations of data privacy rules.

If the Agency becomes aware that a data operator is in violation of the law, an enforcement notice may be issued, requiring the data operator to correct the violation.

A data operator can face civil or administrative penalties for violation of personal data law. Executives of the data operator responsible for violation of data rules may also face personal liability, including, in some cases, criminal liability. Criminal liability is not often applied, but may be imposed for violations, such as:

- Unlawful collection or dissemination of information about a data subject's private life, personal or family secreta, or public dissemination or leak to mass media of such information;

- Violation of data subjects’ right so secrecy of correspondence, telephone conversations, postal, telegraphic and other communications; or
- Unlawfully accessing legally protected computer information, if this act resulted in the destruction, blocking, modification or copying of computer information, including personal data.

Usually, in the case of violation of data protection law, the Agency will serve an enforcement notice requiring the correction of the violation. In many cases, the Agency and may also impose an administrative penalty and in some cases, may also recommend further actions against the individuals responsible for the violation.

The default administrative fines for most initial violations of data privacy rules are between ₽60, 000 – 150, 000 and ₽300,000 for repeated violations.

There are some specific rules for a breach of rules for written consent. In these cases, the fine for initial offences is between ₽ 300, 000 and ₽700, 000, and for repeated violations ₽1, 000, 000 – ₽1, 500, 000.

For violation of data localization rules, the maximum administrative penalty is currently ₽18, 000, 000 for repeated violations, actual penalties are imposed at lower levels.

The State Duma is considering significantly increasing existing fines and implementing new fines:

- Failure to fulfill or untimely fulfillment of the obligation to notify the Agency of the intention to process personal data - from ₽ 100,000 to ₽300,000;
- Failure to notify or late notification of the Agency of a leak of personal data. Companies are proposed to be fined up to ₽3, 000, 000 for this violation;
- Actions (or inaction) of the data operator causing a leak of personal data would involve a fine for companies between ₽5, 000, 000 and ₽20, 000 000, depending upon the number of affected data subjects, as well as the number of identifiers relating to affected data subjects. For repeated leaks, a fine ranging from 0.1% to 3% of the data operator’s aggregate revenue (in any case it must be not less than ₽15, 000, 000 or more than ₽ 500, 000, 000); and
- It is also proposed to criminalize the unlawful processing of computer information containing personal data, as well as the creation or operation of information resources intended for the unlawful storage or dissemination of such information. Penalties would include fines, compulsory labor and imprisonment.

While there has been a strong negative reaction in industry to the new fines and it would be expected that the proposed bill will be changed, it does appear that higher penalties for data law violations will come into force in the foreseeable future.

ELECTRONIC MARKETING

Processing of personal data for directly contacting data subjects for purposes of sales and marketing is allowed only with the consent of the data subject. In addition to the consent requirement under personal data rules, electronic marketing activities are regulated by the Law “on Advertising” No. 38-FZ dated 13 March 2006. The Advertising Law features an Anti-Spam rule under which the distribution of advertising through telecommunications networks, in particular, through the use of telephone, facsimile and mobile telephone communications, is allowed only with the consent of party receiving the advertising. The advertiser bears the burden of proof to show that consent was received. Consent to receive advertising may be revoked at any time, and the advertiser is obligated to immediately cease distribution of the advertising upon such revocation.

ONLINE PRIVACY

Russian data law does not generally specifically regulate online privacy. That said, however, Russian personal data rules are broadly written so that they would apply to online privacy, and it would appear that online privacy was a concern of the legislators when the rules are drafted. One specific area of application of the rules to online privacy involves the specific rules for personal data subject for dissemination.

Personal data allowed by the personal data subject for dissemination

A certain subset of personal data involves that data for which a data subject has given consent for dissemination. While not specifically limited to online dissemination, these rules were made with online activity in mind – particularly social media and other platforms from which information is shared. Consent in this regard must be executed separately from other consents of the subject of personal data to the processing of his / her personal data and requires specificity about the types of personal data which may be disseminated. The data operator must provide the data subject with the opportunity to determine the list of personal data for each category of personal data specified in the consent. The consent must be explicit; silence or inaction of the personal data subject can under no circumstances be considered as implied consent.

The data subject may establish prohibitions on the transfer or disclosure (except for granting access) of the personal data by the data operator, as well as prohibitions or conditions on public processing (except for obtaining access) of thee. The data operator must publish information on these prohibitions and conditions on processing within three working days from the date of obtaining the relevant consent of the data subject.

The data subject may revoke consent at any time. The transfer, dissemination, provision, or granting access to personal data authorized by the personal data subject for dissemination shall be stopped within three working days from the request of the data subject.

In case of public disclosure of personal data directly by the data subject, the personal data, although disclosed, is still protected under law. So, where a data subject makes the personal data public (for example on social media), further dissemination or processing of this personal data still must be performed under a valid legal basis (usually consent).

In cases of public disclosure of personal data was done unlawfully or under force majeure circumstances, that personal data is also still protected under law and the further dissemination or other processing of such personal data lies on each person who carried out the dissemination or other processing.

Cookies

There is a well-established approach that cookies may constitute personal data if the information contained fits the definition of personal data (pertaining to or able to be used to identify a data subject) and in such cases, there must be a consent for its processing. As most cookies do carry personal data, necessity for consent is, in practice, presumed.\

Other

In addition to cookies, other types of information associated with online activity may also constitute protected personal data. If information on number, length of visits of particular web-sites, IP address and other information relates directly or indirectly to a specific or defined physical person then that would constitute protected personal data. Information regarding online activity may also be governed by legal protections in additional personal data laws, for example, those involving secrecy of communications.

KEY CONTACTS

Michael Malloy
Partner
Nextons
T +7 812 325 84 44
michael.malloy@nextons.ru

DATA PRIVACY TOOL

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