Data Protection & Privacy

Contributing editor
Rosemary P Jay

2016

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Data Protection & Privacy 2016

Contributing Editor

Rosemary P Jay

Hunton & Williams

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Business development managers
Alan Lee
alan.lee@lbresearch.com

Adam Sargent
adam.sargent@lbresearch.com

Dan White
dan.white@lbresearch.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3708 4199
Fax: +44 20 7229 6910

First published 2012
Fourth edition
ISSN 2051-1280

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

Russia

Ksenia Andreeva, Anastasia Dergacheva, Vasilisa Strizh and Brian Zimbler

Morgan, Lewis & Bockius LLP

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

Federal Law No. 152-FZ on Personal Data dated 27 July 2006 (the PD Law) is the main law governing personally identifiable information (personal data) in Russia. The PD Law was adopted in 2005 following the ratification of the Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data. In general, the PD Law takes an approach similar to the EC Data Protection Directive, but the Russian regulation places special emphasis on the technical (IT) measures for data protection. Data protection provisions can also be found in other laws, including Federal Law No. 149-FZ on Information, Information Technologies and Information Protection (2006) and Chapter 14 of the Labour Code of the Russian Federation (2001).

Further, numerous legal and technical requirements are set out in regulations issued by the Russian government and Russian governmental authorities in the data protection sphere, namely, the Federal Service for Communications, Information Technology and Mass Communications Supervision (known as Roskomnadzor), the Federal Service for Technical and Export Control (FSTEK) and the Federal Security Service (FSS). The regulations in this area are constantly being amended and developed (see 'Update and trends').

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The federal authority in charge of the protection of individuals' data rights (known under Russian law as 'personal data subjects') is Roskomnadzor. Roskomnadzor undertakes inspections of data processing activities conducted by companies that collect personal data (known under Russian law as 'data operators') and has the power to impose mandatory orders to address violations of data protection rules. Roskomnadzor's inspections can be either scheduled or extraordinary upon receipt of a complaint from an individual. During the inspections (both documentary inspections and field checks), Roskomnadzor may review and request a data operator's documents describing data processing activities and inspect information systems used for data processing.

According to the law currently in effect, administrative cases relating to violations of data privacy discovered by Roskomnadzor may be initiated by the prosecutor's office based on Roskomnadzor's administrative violations report. The administrative case is further considered by the court, which then makes an administrative ruling. According to the recently suggested amendments to the PD Law, Roskomnadzor could be entitled to initiate administrative cases without referring to the prosecutors' office, provided, however, that the imposition of administrative penalties is still the prerogative of a court.

Roskomnadzor is an influential body that interprets the provisions of the PD Law and addresses the problem areas in data protection practice. It publishes its views on various issues related to personal data and the procedures for their protection (including on violations revealed during inspections) at its 'Personal Data Portal' at www.pd.rsoc.ru. Roskomnadzor also maintains two main state registers in the data privacy sphere – a register of data operators and a register of 'data operators in breach'. Roskomnadzor also deals with requests and applications from individuals (see question 23).

Another important authority is the FSTEK. The FSTEK is responsible for the development of technical regulations on data processing, including requirements for IT systems used in processing and measures required for the legitimate transfer of data. The FSTEK is often involved in the inspections carried out by Roskomnadzor. The authority issues working papers, opinions and interpretations of the PD Law related to the technical protection of personal data on its website at www.fstec.ru.

3 Breaches of data protection

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Under article 24 of the Russian Constitution, it is forbidden to collect, store, use and disseminate information on the private life of any person without his or her consent. This constitutional right is also protected under the PD Law. Under article 24 of the PD Law, persons violating the PD Law are subject to civil, administrative or criminal liability.

Under the current Code for Administrative Offences of the Russian Federation, a data operator (and, as the case may be, its officers and other relevant employees) may be liable for a number of administrative offences in the data privacy sphere, including for violation of procedures for the gathering, storage, use or promulgation of personal data (article 13.11 of the Administrative Code), or failure to file or late filing to a government agency of necessary information on data processing activities (article 19.7 of the Administrative Code). Administrative liability for the offenses is monetary with a fine of up to 10,000 roubles. In addition, the court may order the confiscation of uncertified information systems, databases and software used for data processing. In December 2014, the Russian parliament suggested strengthening the penalties for non-compliance with the PD Law (up to 300,000 roubles per violation).

The Criminal Code of the Russian Federation provides criminal liability for unlawful collection or dissemination of personal data amounting to a personal or family secret without that person's consent, as well as the public dissemination of such data. Such criminal offences are punishable by monetary fines of up to 200,000 roubles, 'correctional labour' or even imprisonment for a period for up to two years. Illegitimate access to computer information that has caused the destruction, blocking, modification or copying of such information may also be subject to criminal liability, ranging from fines of up to 500,000 roubles and to seven years' imprisonment. Under article 173.2 of the Criminal Code, the use of false documents accompanied with the illegal use of personal data is subject to criminal liability ranging from fines up to 500,000 roubles and up to three years' imprisonment.

In Russia, criminal penalties are imposed only on individuals and not on legal entities. The claim is usually filed by the prosecutor's office either after the office's own investigation or upon the request of Roskomnadzor or the injured individual.

Scope

4 Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Article 1 of the PD Law expressly excludes from the scope of the PD Law any data processing in connection with record keeping and the use of personal data contained in the Archive Fund of the Russian Federation, classified information (ie, state secrets), as well as any processing related to the activities of the Russian courts. Further, the PD Law does not regulate data processing that is performed by individuals exclusively for personal and family needs, unless such actions violate the rights of other individuals.

In all other cases, the regulations of the PD Law are equally applicable to all organisations that collect personal data in Russia, irrespective of their sector or area of business. In certain industries it is common practice to develop standards for the processing and protection of personal data. Such 'industry standards' already exist for non-governmental pension funds (see the recommendations published on the website of the National Association of Non-Governmental Pension Funds at www.napf.ru/14154), for telecom operators (published on the website of the Communication Services Market Participants' Union at http://icu.org.ru/docs/int/triton/) and banks (published on the website of the Central Bank of the Russian Federation at www.cbr.ru/credit/Gubzi_docs/st-10-14.pdf). Draft standards are currently being developed in the spheres of health-care and tourism.

5 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Article 23 of the Russian Constitution guarantees the right to privacy of personal life, personal and family secrets and correspondence for every individual. Therefore, as a general rule, the interception of communications or the monitoring and surveillance of an individual is allowed only with his or her explicit consent, unless such actions are performed in the course of investigative activities by state authorities. Certain limited activities related to the collection of personal data may be performed by private detectives with a state licence, as required by the Law of the Russian Federation No. 2487-1 on Private Detective and Safeguarding Activity (1992).

The PD Law sets out general principles for the use of personal data in the promotion of goods, work and services directly to potential consumers (via telephone, e-mail or fax), including an obligatory opt-in confirmation. Electronic marketing procedures are also regulated by Federal Law No. 38-FZ on Advertising (2006) and the Law of the Russian Federation No. 2300-1 on Consumers' Rights Protection (1992) (see question 4).

6 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Specific provisions for the protection of certain types of personal data are covered by a variety of laws, which are nonetheless based on the general principles set out in the PD Law. For example, the protection of patients' data is regulated by Federal Law No. 323 on the Fundamentals of Protection of the Health of Citizens in the Russian Federation (2011). Personal data processing by banks and bank secrets are regulated by Federal Law No. 395-1 on Banks and Banking (1990). The principles of data handling by notaries and advocates are set out in the Fundamentals of Legislation of the Russian Federation on the Notariat (1993) and Federal Law No. 63-FZ on Advocacy and Advocate Activity in the Russian Federation (2002), respectively. In addition, the Family Code of the Russian Federation, the Tax Code of the Russian Federation, Federal Law No. 98-FZ on Commercial Secrets and other laws regulate the processing of different types of personal data.

7 PII formats

What forms of PII are covered by the law?

The PD Law does not distinguish between personal data in paper or electronic format and is equally applicable to both.

8 Extraterritoriality

Is the reach of the law limited to data owners and data processors established or operating in the jurisdiction?

The PD Law does not specify its jurisdictional scope. Under Roskomnadzor's interpretation, published on its website, the PD Law applies to any legal entity, including any foreign entity with a legal presence in Russia, which collects personal data in Russia (see publication at http://pd.rkn.gov.ru/faq/faq17.htm).

9 Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide services to owners?

The PD Law does not distinguish between 'data controllers' and 'data processors'. Instead, a company engaged in data processing is a 'data operator' that organises or carries out (alone or with other operators) the processing of personal data and a company or individual who determines the purpose, content and method of personal data processing is a 'data operator'.

Under article 6 of the PD Law, a data operator may assign or delegate data processing to a third party. Such a third party will be acting on a so-called 'instruction of the operator' (see question 29). A third party does not need to obtain the separate consent of an individual to process his or her data within the same scope as permitted by the operator's instruction. It is the data operator who must ensure that all necessary consents are obtained. Arguably, all other requirements on data processing under the PD Law are equally applicable to both data operators and third parties acting on their instructions.

Legitimate processing of PII

10 Legitimate processing – grounds

Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The PD Law provides that any operation performed on personal data, whether or not by automatic means, such as collection, recording, organisation, storage, alteration, retrieval, consultation, use, transfer (dissemination or providing access), blocking, erasure or destruction amounts to 'processing' of personal data and is subject to regulation. Thus, almost any activity relating to personal data constitutes 'processing' under the PD Law.

Any processing of personal data must be lawful, fair and transparent in relation to the individuals concerned. In particular, the specific purpose for which the data are processed must be explicit, legitimate and determined at the point of data collection (article 5 of the PD Law). The data should be adequate, relevant and limited to a minimum necessary for the purpose of data collection and processing. This requires the data operator to assess regularly whether the processed data are excessive and the period necessary for processing such data.

As a general rule, the processing of personal data requires the consent of the individual. However, article 6 of the PD Law provides 10 general exemptions from the consent requirement, including instances where data are processed:

- under an international treaty or pursuant to Russian law;
- for judicial purposes;
- for the purpose of rendering state and municipal services;
- for performance of an agreement to which the individual is a party or under which the individual is a beneficiary or guarantor, including where the operator exercises its right to assign a claim or right under such an agreement;
- for statistical or other scientific purposes, on the condition that the data are anonymised;
- for the protection of the life, health or other legitimate interests of the individual, in cases where obtaining his or her consent is impossible;
- for the protection of the data operator's or third parties' rights or for the attainment of public purposes, provided there is no breach of an individual's rights and freedoms;
- for the purpose of mandatory disclosure or publication of personal data in cases directly prescribed by law;

- in the context of professional journalistic, scientific, literary or other creative activities, provided there is no breach of an individual's rights and freedoms; or
- if such data have been made publicly available by the individual or under his or her instruction.

Other exemptions from the consent requirement set out in articles 10, 11 and 12 of the PD Law may also apply depending on the type of data being processed.

11 Legitimate processing – types of data

Does the law impose more stringent rules for specific types of data?

Under the PD Law, all personal data is divided into the following categories:

(i) general data, which include an individual's full name, passport details, profession and education, and in essence amount to any personal data other than sensitive or biometric data;
(ii) sensitive data, which include data relating to an individual's health, religious and philosophical beliefs, political opinions, intimate life, race, nationality and criminal records; and
(iii) biometric personal data, which includes data such as fingerprints, iris images and, arguably, certain types of photographic images.

The processing of data in categories (ii) and (iii) above must be justified by reference to a specific purpose and, in most cases, requires explicit written consent by an individual. Further, the processing of data relating to criminal records may only be carried out in instances specifically permitted by the PD Law and other laws.

Data handling responsibilities of owners of PII

12 Notification

Does the law require owners of PII to notify individuals whose data they hold? What must the notice contain and when must it be provided?

A data operator must notify an individual prior to processing his or her data, if such data was received from a third party. In particular, the data operator must give the individual notice of the following:

- the data operator's name and address;
- the purpose of processing and the operator's legal authority;
- the prospective users of the personal data;
- the scope of the individual's rights, as provided by the PD Law; and
- the source of data.

13 Exemption from notification

When is notice not required?

Notification of the data subject is not required if the data operator received the personal data directly from the concerned individual.

Further, the requirement on the data operator to give the notice before processing data received from a third party does not apply if:

- the individual has already been notified of the processing by the relevant operator;
- the personal data were received by the operator in connection with a federal law or a contract to which the individual is either a beneficiary or guarantor;
- the personal data were made publicly available by the individual or were received from a publicly available source;
- the personal data are processed by the operator for statistical or other research purposes, or for the purpose of pursuing professional journalistic, scientific, literary or other creative activities, provided there is no breach of the individual's rights and freedoms; and
- providing such notification would violate the rights or legitimate interests of other individuals.

14 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

As a general rule, the individual will confirm the purposes and methods for the use of his or her personal data in the consent on processing granted to the data operator.

If such consent was not required or was implied, the individual would be able to control the use of his or her information only upon obtaining access to the data by a request to the data operator (see question 34). In cases where the data processed by the operator are inaccurate or irrelevant for the purpose of processing, the individual may request that the data operator rectify, block or delete his or her personal data and may raise an objection against the purpose or method of processing with Roskomnadzor or in court.

15 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

One of the basic principles of data processing is that the personal data kept by the data operator must be relevant, accurate and up to date. Therefore, the data operator must regularly review the data and update, correct, block or delete it as appropriate (articles 21 and 22 of the PD Law).

16 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

As a general rule, the personal data must be stored by the data operator for the period required to accomplish the purpose of processing. Such a period must be limited to a strict minimum. The period during which the personal data can be retained will usually depend on the retention rules for the documents containing the personal data.

For example, there are rules that cover the length of time certain personnel-related and other relevant records should be kept. Federal Law No. 125-FZ on Archiving in the Russian Federation (2004) and Order No. 558 of the Ministry of Culture of the Russian Federation on Approval of a List of Model Management Archival Documents Created in the Course of Activities of the Government Authorities, Local Self-Government Authorities and Organisations with Retention Period Specified (2012) set out minimum and maximum periods during which a company's documents, including documents containing personal data, should be retained. Depending on the nature of the document, such periods may vary from one year up to 75 years.

17 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Under article 5 of the PD Law, any data processing must be carried out for specific, explicit and legitimate purposes, and the data collected or processed must be adequate, relevant and proportionate to the purposes of collection or further processing. The data operator must take all reasonable steps to ensure that inaccurate personal data are rectified or deleted. Article 5 of the PD Law obliges the data operator to destroy or depersonalise the concerned personal data, when the purposes of processing are met.

18 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The PD Law does not provide for any exceptions from the finality principle.

Security

19 Security obligations

What security obligations are imposed on data owners and entities that process PII on their behalf?

A number of complex security requirements apply to data operators and third parties that process personal data under the operators' instructions. The PD Law only refers to general principles of data security and does not contain any specific requirements. The Regulation of the Russian Government No. 1119 dated 1 November 2012 describes the organisational and technical measures and requirements that must be taken to prevent any unauthorised access to the personal data. Following the adoption of the above regulation, the FSTEK has issued a number of further regulations relating to technical measures aimed at the protection of processed data.

The data operator must take appropriate technical measures against the unauthorised and unlawful processing of data, as well as against accidental loss, blocking or destruction of processed data. For example, in most cases, any personal data information system (even a simple database) must be certified by the FSTEC. In certain cases, such as the processing of large volumes of data or biometric data, the data operator can only use hardware and software for the processing that has been approved by the FSTEC or the FSS.

20 Notification of security breach

Does the law include obligations to notify the regulator or individuals of breaches of security?

Article 21 of the PD Law provides for obligations related to data security breaches. These include an obligation on the data operator to rectify any breach (including a security breach) within three days and to notify the affected individual within three days of rectification. In the event of a rectification made at Roskomnadzor's request, the data operator must inform Roskomnadzor within three days of rectification. In practice, however, the notification requirement for security breaches rarely appears to be implemented or enforced.

Internal controls

21 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

Under article 22.1 of the PD Law, the data operator must appoint a data protection officer. There is no specification whether the officer must be an employee of the data operator, but arguably, this should be the case. The officer must report directly to the general manager (director) and is responsible for the 'internal application of the provisions of the PD Law' and other data-related laws, as well as for maintaining a register of data processing operations. In particular, the officer must:

- implement appropriate internal controls over the data operator and its employees;
- make the data operator's employees aware of personal data-related regulations, any internal rules on data protection and other data protection requirements; and
- deal with applications and requests from individuals.

22 Record keeping

Are owners of PII required to maintain any internal records or establish internal processes or documentation?

The PD Law requires the data operator to establish a system of internal (local) documents with a detailed description of protective measures taken by the operator (so-called 'organisational measures' of protection). One of the protective measures required from the data operator to secure the data involves establishing an internal system of control over access to the personal data processed, which includes keeping records of access to the data. As a general rule, such access to data is only granted for a temporary period and for business needs.

Registration and notification

23 Registration

Are owners and processors of PII required to register with the supervisory authority? Are there any exemptions?

Yes, data operators are registered with Roskomnadzor in the following way.

The data operator must notify Roskomnadzor before starting to process personal data. This is a one-off notification and the data operator does not need to notify the authority in each instance of data processing. The data operator should amend the notification if the information contained in the initial notification changes. Roskomnadzor maintains a public register of data operators, based on the information contained in the notifications received. In the absence of any queries, Roskomnadzor acknowledges receipt of the notification and adds the information on the data operator to the register within 30 days of receipt of notification.

Most collection and processing of data requires formal notification to Roskomnadzor. There are exceptions for simple, one-off collections of data and HR-related data. For example, exemptions apply if:

- the data are processed under employment law only;
- the data are received by the data operator in connection with a contract with the individual, provided that such personal data are not transferred to or circulated among third parties without the individual's consent, and only used either to perform the contract or to enter into further contracts with the individual;
- the data relate to a certain type of processing by a public association or religious organisation;
- the data were made publicly available by the individual;
- the data consist only of the surname, first name and patronymic of the individual; or
- the data are necessary for granting one-time access to the individual into the premises where the data operator is located and in certain other cases.

24 Formalities

What are the formalities for registration?

The notification form can be found on Roskomnadzor's website at www.pd.rsoc.ru, together with guidance on its completion. The notification must contain:

- the name and address of the data operator;
- the type of data being processed;
- a description of the categories of the data subjects whose data is being processed;
- the purpose of processing;
- the timeframe of processing; and
- a description of IT systems and security systems used by the data operator.

All of the above information, except for the description of the operator's IT systems and security measures, is made publicly available.

The notification may be submitted electronically on Roskomnadzor's website. However, the data operator must also send a paper version of the notification signed by its general manager (director) to the territorial division of Roskomnadzor. If the information contained in the notification changes (including, for example, the scope of IT systems used by the data operator to process the personal data), the operator must notify Roskomnadzor of such changes within ten working days of the change. Notification or any further amendment of the entry in Roskomnadzor's register does not require any fee payment by the data operator.

25 Penalties

What are the penalties for a data owner or processor for failure to make or maintain an entry on the register?

Failure by the data operator to notify Roskomnadzor of data processing is subject to an administrative fine of up to 5,000 roubles under article 19.7 of the Code for Administrative Offences of the Russian Federation. The same administrative penalties are imposed for late submission of the notification or amendments thereto.

26 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Provided that the notification is complete and contains the correct data, Roskomnadzor has no authority to refuse the data operator an entry in the register. Article 22 of the PD Law allows Roskomnadzor to obtain rectification of the information contained in the notification from the data operator before the information is recorded.

27 Public access

Is the register publicly available? How can it be accessed?

The register of data operators is available to a certain extent on Roskomnadzor's website at http://pd.rkn.gov.ru/operators-registry/operators-list; however, it has limited search capacities. The register contains information on the particulars of data processing by the data operator, except for the description of IT systems and security measures. The information in the register is in Russian only.

28 Effect of registration

Does an entry on the register have any specific legal effect?

The data operator may start processing the data, in accordance with the purposes and methods described in the notification, upon submitting notification to Roskomandzor.

Transfer and disclosure of PII

29 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Under article 6 of the PD Law, the data operator may assign or delegate the processing to a third party, which will act under the instruction of the operator.

There is no statutory form for such instruction by the operator, or for the standard form or precedent of the data transfer agreement approved by Roskomnadzor. The PD Law requires that the instruction of the operator must list the aims of processing, the actions the third party is permitted to perform on the data and the rules of data processing that the third party must comply with (including certain purely technical requirements on data processing).

A third party processing personal data under the operator's instruction must undertake to the operator to maintain the security and confidentiality of the data transferred. As a general rule, assignment of data processing to a third party providing outsourced processing services requires the individual's consent absent an exemption under the PD Law (see question 10).

30 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Any transfer (including disclosure) of personal data requires the consent of the individual. If such consent is obtained by the data operator, there are no restrictions on the disclosure to which consent was given. The recipient of the personal data must maintain the security and confidentiality of such data under the agreement with the data operator.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Under article 12 of the PD Law, in the event of a cross-border transfer of data, the data operator must check that the data subjects' rights are adequately protected in the foreign country before the transfer. All countries that are party to the European Convention on Personal Data of 28 January 1981 are considered to be countries 'having adequate protection of data subjects' interests' (ie, 'safe' countries). Further, Roskomnadzor has approved a list of countries that are not party to the above European Convention but are, nonetheless, considered to be 'safe' countries for the purpose of cross-border transfers (including Canada, Israel, New Zealand, Mongolia and Peru).

Cross-border transfers of personal data to 'safe' countries are not subject to any specific requirements, provided that the data operator has received consent from the data subject on the transfer of his or her data. Data transfers to 'non-safe' countries (eg, Japan and the United States) are allowed only if one of the following requirements is met:

- the subject consented in writing to the cross-border transfer of his or her data;
- the transfer is made under an international treaty of the Russian Federation;
- the transfer is required by applicable laws for the purpose of protecting the constitutional system of the Russian Federation, its national defence or the secure maintenance of its transportation system;
- the transfer is necessary to perform the contract to which the individual is a party or under which he or she is a beneficiary or guarantor; or
- the transfer is needed to protect the individual's life, health or other vital interests and it is impossible to obtain his or her prior consent.

32 Notification of transfer

Does transfer of PII require notification to or authorisation from a supervisory authority?

There is no obligation to notify Roskomnadzor or any other supervisory authority of any data transfer.

33 Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The restrictions on data transfers (including cross-border transfers to 'safe' or 'non-safe' countries) are equally applicable to any transfer of data.

Rights of individuals

34 Access

Do individuals have the right to see a copy of their personal information held by PII owners? Describe any limitations to this right.

Under article 14 of the PD Law, the individual is entitled to request the details of the processing of his or her data from the data operator and access his or her personal data. The data operator may not charge a fee for providing the information or access to the data.

The individual has the right to obtain confirmation on whether his or her personal data are being processed at any time on request to the data operator. The request may also be submitted by a representative of the data subject. There is no statutory form for the request; however, the PD Law requires that it must contain information on the requester's identity (ie, passport details of the data subject or his or her representative) and the information necessary to find the appropriate records (ie, a detailed explanation of the relationship between the data subject and the data operator, including, for example, references to the relevant agreement or other arrangements).

If the personal data are being processed by the data operator, the operator has 30 days to respond to the request of the data subject or his or her representative and to provide all of the following information:

- confirmation of the processing of data;
- the legal grounds for and purposes of the processing;
- the purposes and methods of processing;
- the name and address of the data operator and any recipients (other than the data operator's employees) who have access to the personal data or to whom the personal data are to be disclosed under an agreement with the data operator or otherwise as required by law;
- the scope of the personal data processed and the source of the personal data (unless another procedure for receiving personal data is established by a federal law);
- the terms of processing, including the period for which the personal data will be stored;
- the scope of rights of the individual as provided by the PD Law;
- information on any (implemented or planned) cross-border transfers of the personal data;
- if applicable, the name and address of any third-party processor of the personal data acting under 'instruction of the operator'; and
- any other information as required by applicable law.

Update and trends

In July 2014, the Russian State Duma approved amendments to the PD Law to include so-called 'local storage requirements' (Local Storage Law). The Local Storage Law comes into force on 1 September 2015. In accordance with the new requirements, an operator is required to ensure that the recording, systemisation, accumulation, storage, clarification (updating, modification) and retrieval of Russian citizens' personal data is to be conducted only in 'databases located within Russia.' There are a number of exceptions to this requirement. For example, processing for the purposes of achieving the objectives of international treaties, for the purposes of implementation of an operator's statutory powers and duties, for professional activities of journalists or the lawful activities of mass media, or scientific, literary or other creative activities may be performed within the foreign databases.

The Local Storage Law contains rather vague language, and there is still no official interpretation or other reliable guidance from Russian authorities on how to implement the new requirement. One of the most sensitive issues is whether the Local Storage Law applies to companies that have no legal presence in Russia but work with Russian individuals. The general consensus among experts is that companies with no corporate presence in Russia (either in the form of a subsidiary, a branch or a representative office) should not be covered by the Local Storage Law. At the same time, online businesses with no local presence could still be affected, particularly if they customise their websites for Russian users or promote their services in Russia.

In addition to the duty to procure the requirement that databases that process Russian citizens' personal data are located within Russia, an operator will be required to provide data on the location of such databases to Roskomnadzor, unless one of the exemptions apply (eg, where the collected personal data from the personal data subjects includes their full names only).

Finally, according to the Local Storage Law, Roskomnadzor will be entitled to block access to information resources (websites) that are processing personal data in breach of the PD Law. Arguably, Roskomnadzor may block access to the website irrespective of the location of the data operator or the website administrator. Moreover, Roskomnadzor will create a special register of violators of personal data subjects' rights, which, on the basis of a court decision, will include information about data operators that violate the PD Law. This register will contain information about the domain names or other links to website pages on the internet containing personal data processed in violation, network addresses that enable the identification of such web-sites and other information.

Article 14 of the PD Law sets out a narrow set of circumstances in which the access rights of the individual may be limited. For example, access may not be provided if the data processing relates to investigative or anti-money laundering activity carried out by state authorities, or if granting access to the information would curtail the rights of other data subjects.

35 Other rights

Do individuals have other substantive rights?

In addition to the right to require access to his or her personal data and request the details of data processing, the data subject may also request the correction of inaccurate data processed by the operator and require the operator to inform any third party with access to the inaccurate data of the corrections made. Further, data subjects are entitled to demand that the data operator discontinue the processing of the personal data (except where the processing cannot be terminated or would result in violations of Russian law, for example, labour law requirements). The data subjects can request the deletion of particular data, if such data are inaccurate, unlawfully obtained or unnecessary for the purpose of processing by the data operator.

36 Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Under article 24 of the PD Law, compensation for any moral damage to an individual resulting from an infringement of his or her rights related to personal data processing and protection must be provided irrespective of any compensation for property damage or other losses. There is no legal interpretation as to what kind of violation of PD Law would lead to an imposition of monetary damages. As a general rule, articles 151 and 1101 of the Civil Code of the Russian Federation require the court to consider the so-called 'degree of guilt' (ie, whether the infringement was gross or merely negligent, and whether there was an element of any intention or malice) and the 'degree of suffering' of the individual. However, compensation for moral damage caused by a violation of the personal data protection rules is rarely applied in practice.

37 Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Article 17 of the PD Law provides that if the data subject discovers a violation of his or her rights by the operator, the data subject is entitled to protect these rights through the authorised body for the protection of data subjects' rights (ie, Roskomnadzor), or in court. Roskomnadzor is entitled to impose administrative penalties on data operators for non-compliance with personal data protection laws, which the data operators may appeal in court.

Morgan Lewis

Ksenia Andreeva **kandreeva@morganlewis.com**
Anastasia Dergacheva **adergacheva@morganlewis.com**
Vasilisa Strizh **vstrizh@morganlewis.com**
Brian Zimbler **bzimbler@morganlewis.com**

Tsvetnoy Bulvar, 2
Moscow 127051
Russia

Tel: +7 495 212 2500
Fax: +7 495 212 2400
www.morganlewis.com

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

There appear to be no further exemptions apart from those described above.

Supervision

39 Judicial review

Can data owners appeal against orders of the supervisory authority to the courts?

The orders of Roskomnadzor may be appealed in court. There have been a growing number of appeals by data operators against decisions imposing administrative liability for non-compliance with personal data protection laws.

40 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

Russian law does not regulate the use of 'cookies'. There is also no official guidance on this subject by Roskomnadzor.

41 Electronic communications marketing

Describe any rules on marketing by e-mail, fax or telephone.

Unsolicited electronic communications (including via e-mail, fax or telephone) are prohibited. Any data processing for the purpose of direct marketing is allowed only with the prior consent of the data subject. Such consent can be revoked by the data subject at any time, meaning that the data operator is unable to further process personal data. The rules on electronic communications marketing are set out in article 15 of the PD Law and in article 18 of Federal Law No. 38-FZ on Communication (2006).

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Climate Regulation
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Enforcement of Foreign Judgments
Environment
Executive Compensation & Employee Benefits
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Private Antitrust Litigation
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Securities Litigation
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

iPad app

Available on iTunes

Law Business Research

Data Protection & Privacy
ISSN 2051-1280

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the ABA Section of International Law