Data Protection & Privacy 2021

Contributing editors
Aaron P Simpson and Lisa J Sotto

LEXOLOGY
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2012
Ninth edition
ISBN 978-1-83862-322-7

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

Data Protection & Privacy

2021

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Lexology Getting The Deal Through is delighted to publish the ninth edition of *Data Protection & Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Canada and Romania.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

LEXOLOGY®
Getting The Deal Through

London
August 2020

Reproduced with permission from Law Business Research Ltd
This article was first published in September 2020
For further information please contact editorial@gettingthedealthrough.com

Contents

Russia

Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva, Vasilisa Strizh and Brian L Zimbler
Morgan Lewis

LAW AND THE REGULATORY AUTHORITY

Legislative framework

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

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 EU Data Protection Directive and is based on the international instruments on privacy and data protection in certain aspects, but the Russian regulation places special emphasis on the technical (IT) measures for data protection. Notably, the PD Law has concepts similar to the one contained in the General Data Protection Regulation, which became effective in the EU on 25 May 2018. 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 (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.

Data protection authority

2 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 (eg, 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. The rules regulating the procedure for Roskomnadzor's inspections have been sufficiently updated in 2019. Administrative cases relating to violations of data privacy are initiated by Roskomnadzor and further considered by the court, which then makes an administrative ruling, for example, imposing administrative penalties. 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 procedures for data protection (including on violations revealed during inspections) at its 'Personal Data Portal' at www.pd.rkn.gov.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'.

Another important authority is FSTEK. 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. FSTEK is in some cases 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.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Under article 23 of the PD Law, Roskomnadzor is entitled to cooperate with foreign data protection authorities, including on the international exchange of information on the protection of data subjects' rights. As part of this cooperation, Roskomnadzor organises conferences and public meetings and invites representatives of data protection authorities and professionals from other jurisdictions to participate.

Breaches of data protection

4 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 article 13.11 of the Code for Administrative Offences of the Russian Federation (the Administrative Code), a data operator (and, as the case may be, its officers and other relevant employees) may be liable for several breaches of personal data processing, including for:

- data processing without the individual's written consent when obtaining such consent is required;
- failure to publish the policy on data processing on the website; and

- failure to provide the individual with the information related to the processing of his or her data, with fines for an offence up to 75,000 roubles.

In December 2019, article 13.11 of the Administrative Code was supplemented with severe penalties for non-compliance with the local storage requirement. Legal entities may be subject to fines of up to 6 million roubles for the first-time offence, and to 18 million roubles for the second-time offence.

In addition, the Administrative Code imposes separate liability for failure to file or late filing to a government agency of necessary information on data processing activities (article 19.7 of the Administrative Code), with a fine of up to 5,000 roubles.

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 with disqualification for up to three years.

Illegitimate access to computer information that has caused the destruction, blocking, modification or copying of personal data may also be subject to criminal liability, ranging from fines of up to 500,000 roubles and up 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. Civil liability in the data privacy sphere is provided by the Russian Civil Code.

SCOPE

Exempt sectors and institutions

5 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 Federal Law No. 152-FZ on Personal Data dated 27 July 2006 (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, 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, telecom operators, banks and healthcare organisations.

Communications, marketing and surveillance laws

6 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 under the Federal Law No. 144-FZ on Investigating Activities (1995). 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).

However, the rules on monitoring and surveillance of individuals are currently undergoing significant developments in the light of the Covid-19 pandemic. The recently adopted Federal Law No. 123-FZ dated 24 April 2020 establishes a framework for the development, creation and turnover of artificial intelligence (AI) technologies and services, including facial recognition products, as a five-year experiment to commence in Moscow on 1 July 2020. Such technologies will be tested and will process anonymised personal data (including health-related data) for governmental, municipal management and certain commercial business activities. Requirements and procedures for the use of such technologies will be detailed in Moscow government regulations.

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, email 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).

Other laws

7 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 (including e-health records) is regulated by Federal Law No. 323 on the Fundamentals of Protection of the Health of Citizens in the Russian Federation (2011).
- Personal data (including credit information) processing by banks and bank secrets is regulated by Federal Law No. 395-1 on Banks and Banking (1990) and Federal Law No. 218 on Credit Histories (2004).
- 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 Labour Code of the Russian Federation, 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 (including rules on employee monitoring).

New Government Decree No. 955 dated 24 July 2019 (effective from 31 October 2021) governs data processing by air carriers and operators of automated information systems for processing air traffic information.

PII formats

8 | 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. There are, however, separate rules applicable to processing data in paper and electronic formats.

Extraterritoriality

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

The PD Law does not specify its jurisdictional scope and generally applies to any legal entity, including any foreign entity with a legal presence in Russia, that collects personal data in Russia.

In addition, the PD Law provides for the local storage requirement, which applies to any data operator that processes the personal data of Russian citizens, regardless of its jurisdiction. Pursuant to the local storage requirement, an operator (for example, a company engaged in online business activity) is required to ensure that the recording, systemisation, accumulation, storage, clarification (updating, modification) and retrieval of Russian citizens' personal data is conducted only through the databases that are physically located in Russia. There are certain exceptions to this requirement. For example, data 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 directly in the foreign databases.

Covered uses of PII

10 | Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

The PD Law does not use the terms 'data owners', 'data controllers' and 'data processors'. Instead, the PD Law distinguishes between 'data operators' and 'third parties acting on an instruction of a data operator'. A company engaged in data processing is a data operator, if it organises or carries out (alone or with other operators) the processing of personal data and, more importantly, determines the purpose, content and method of personal data processing.

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 an 'instruction of the operator'. 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

Legitimate processing – grounds

11 | 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 Federal Law No. 152-FZ on Personal Data dated 27 July 2006 (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 is 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 is 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 is processed:

- under an international treaty or pursuant to Russian law;
- for judicial purposes;
- for the purpose of rendering state and municipal services;
- for the 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 is 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 has 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.

Legitimate processing – types of PII

12 | Does the law impose more stringent rules for specific types of PII?

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

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

The processing of data in categories (2) and (3) 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

Notification

13 Does the law require owners of PII to notify individuals whose PII 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.

Exemption from notification

14 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 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 was 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 was made publicly available by the individual or was received from a publicly available source;
- the personal data is 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.

Control of use

15 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.

The individual has the right to control the use of his or her information upon obtaining access to the data by a request to the data operator. In cases where the data processed by the operator is illegitimately processed or is inaccurate or irrelevant for the purpose of processing, the individual may request that the data operator rectify, block or entirely delete his or her personal data or, alternatively, raise an objection against the purpose or method of processing with the Federal Service for Communications, Information Technology and Mass Communications Supervision (Roskomnadzor) or in court.

Notably, health-related data is not always considered sensitive data under the PD Law. The medical data (such as doctor prescriptions, or medical examination reports, laboratory tests results, diagnosis) is sensitive data. However, if it is administrative or financial information about health such as medical certificates for sick leave management or other HR-related purposes, such information is not sensitive data, according to the Roskomnadzor's interpretation.

Data accuracy

16 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).

Amount and duration of data holding

17 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 (2010) 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 vary from one to 75 years.

Finality principle

18 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 is 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.

Use for new purposes

19 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

Security obligations

20 What security obligations are imposed on PII owners and service providers that process PII on their behalf?

A number of complex security requirements apply to data operators and third-party service providers that process personal data under the operators' instructions. The Federal Law No. 152-FZ on Personal Data dated 27 July 2006 (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, Federal Service for Technical and Export Control (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 FSTEK. 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 FSTEK or the Federal Security Service (FSS).

Notification of data breach

21 | Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The PD Law does not expressly require the data operator to notify the authorities of data security breaches. If the request for rectification was made by the affected individual or Roskomnadzor, then the operator has an obligation to notify the affected individual or Roskomnadzor within three days of rectification.

INTERNAL CONTROLS

Data protection officer

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

Under article 22.1 of the Federal Law No. 152-FZ on Personal Data dated 27 July 2006 (the PD Law), the data operator must appoint a data protection officer (DPO). There is no specification whether the officer must be an employee of the data operator under the PD Law. However, Federal Service for Communications, Information Technology and Mass Communications Supervision (known as Roskomnadzor) generally expects a DPO to be employed by the data operator. The DPO must report directly to the general manager (director) and is responsible for the application of the provisions of the PD Law within the company and other data-related laws, as well as for maintaining a register of data processing operations. In particular, the DPO 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.

Record keeping

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

The PD Law requires data operators as well as third-party service providers that process personal data under the operators' instructions to establish a system of internal (local) documents with a detailed description of protective measures taken by such person ('organisational measures' of protection). One of the protective measures 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 granted only for a temporary period and for business needs.

New processing regulations

24 | Are there any obligations in relation to new processing operations?

The PD Law does not provide for obligations in relation to new processing operations, such as privacy-by-design approach or privacy impact assessments. Article 18.1 of the PD Law generally obliges operators to regularly conduct internal audits of personal data-processing activities for their compliance with the PD Law.

REGISTRATION AND NOTIFICATION

Registration

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

As a general rule under article 22 of the Federal Law No. 152-FZ on Personal Data dated 27 July 2006 (the PD Law), data operators are required to be registered with Federal Service for Communications, Information Technology and Mass Communications Supervision (known as Roskomnadzor). The PD Law does not specifically regulate whether data processors must be registered with Roskomnadzor. Nevertheless, Roskomnadzor believes that both data operators and data processors must be registered unless an exemption from the general rule applies.

The registration procedure includes a one-off notification from the data operator to Roskomnadzor. If the data processing characteristics (purposes, terms, third parties having access to the data or other) change, the data operator should notify Roskomnadzor on these changes. Roskomnadzor maintains a public register of data operators. In the absence of any queries, Roskomnadzor acknowledges receipt of the information from the data operator and adds the information on the data operator to the register within 30 days.

There are exceptions from the general rule on the obligatory registration for simple, one-off collections of data and HR-related data. For example, exemptions apply if the data:

- is processed under employment law only;
- is received by the data operator in connection with a contract with the individual, provided that such personal data is 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;
- relates to a certain type of processing by a public association or religious organisation;
- was made publicly available by the individual;
- consists only of the surname, first name and patronymic of the individual; or
- is necessary for granting one-time access to the individual into the premises where the data operator is located and in certain other cases.

Formalities

26 | What are the formalities for registration?

The notification form to be filled by the data operator can be found on Roskomnadzor's website at www.pd.rkn.gov.ru, together with guidance on its completion. The information to be provided to Roskomnadzor includes, inter alia, the following:

- 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 time frame of processing;
- the information on the location of the database with the personal data of Russian citizens; 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 IT systems and security measures used for the protection of processed data, 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. The registration does not require renewal, unless the information contained in the notification changes (including, eg, the scope of IT systems used by the data operator to process the personal data). In this case the operator must notify Roskomnadzor of such changes within 10 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.

Penalties

27 | What are the penalties for a PII owner or processor of PII 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 Administrative Code. The same administrative penalties are imposed for late submission of the notification or amendments thereto.

Refusal of registration

28 | 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.

Public access

29 | 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. 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.

Effect of registration

30 | 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.

Other transparency duties

31 | Are there any other public transparency duties?

Under article 18.1 of the PD Law, an operator is required to publish on its website or otherwise provide unlimited access to its policy describing data processing activities and data protection measures.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

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

Under article 6 of Federal Law No. 152-FZ on Personal Data dated 27 July 2006 (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 the Federal Service for Communications, Information Technology and Mass Communications Supervision (known as 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 with which the third party must comply (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.

Restrictions on disclosure

33 | 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 (unless explicitly allowed by the PD Law or other laws). If such consent is obtained by the data operator, there are no restrictions on the disclosure to which consent was given.

Cross-border transfer

34 | 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 dating from 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 Qatar, Costa Rica, Japan, Singapore, Mali, Gabon, Kazakhstan, Republic of South Africa, Canada, Israel, New Zealand, Mongolia, Peru and some others).

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 and issued 'an instruction of a data operator', if needed. Data transfers to 'non-safe' countries (eg, 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.

Notification of cross-border transfer

35 | Does cross-border 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.

Further transfer

36 | 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

Access

37 | Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Under article 14 of the Federal Law No. 152-FZ on Personal Data dated 27 July 2006 (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 is 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 references to the relevant agreement or other arrangements).

If the personal data is 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 the 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 is 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 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.

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.

Other rights

38 | 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, eg, labour law requirements). The data subjects can request the deletion of particular data, if such data is inaccurate, unlawfully obtained or unnecessary for the purpose of processing by the data operator.

Compensation

39 | 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 '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.

Enforcement

40 | 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, Federal Service for Communications, Information Technology and Mass Communications Supervision (known as 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.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

41 | 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.

SUPERVISION

Judicial review

42 | Can PII owners appeal against orders of the supervisory authority to the courts?

The orders of Federal Service for Communications, Information Technology and Mass Communications Supervision (known as 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.

SPECIFIC DATA PROCESSING

Internet use

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

The use of 'cookies' and equivalent technology on tracking behavioural data is not clearly regulated by Russian law. According to Federal Service for Communications, Information Technology and Mass Communications Supervision (known as Roskomnadzor), the use of cookies and equivalent technologies may in certain cases be considered as personal data processing subject to the user's explicit consent.

Electronic communications marketing

44 | Describe any rules on marketing by email, fax or telephone.

Unsolicited electronic communications (including via email, 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. This 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 Federal Law No. 152-FZ on Personal Data dated 27 July 2006 (the PD Law) and in article 18 of Federal Law No. 38-FZ on Advertising (2006).

Cloud services

45 | Describe any rules or regulator guidance on the use of cloud computing services.

Russian law does not specifically regulate the use of cloud computing services. There is also no official guidance on this subject by Roskomnadzor. The use of cloud computing services for storage of personal data will be generally subject to all requirements of the PD Law.

Morgan Lewis

Ksenia Andreeva
ksenia.andreeva@morganlewis.com

Anastasia Dergacheva
anastasia.dergacheva@morganlewis.com

Anastasia Kiseleva
anastasia.kiseleva@morganlewis.com

Vasilisa Strizh
vasilisa.strizh@morganlewis.com

Brian L Zimbler
brian.zimbler@morganlewis.com

Legend Business Centre
Tsvetnoy Bulvar, 2
Moscow 127051
Russia
Tel: +7 495 212 2500
Fax: +7 495 212 2400
www.morganlewis.com

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

During the last couple of years, the localisation requirement remains key topic affecting all types of processing activities, both on the internet and offline; in particular, in the context of new severe penalties implemented by amended Article 13.11 of the Administrative Code.

Harmonisation with the European Union data protection concepts has also been largely discussed. Additional Protocol to Council of Europe Convention No. 108 has not been ratified yet. However, its implementation would require significant amendments to the PD Law, including the introduction of new concepts (eg, data controllers and data processors), categories of personal data (eg, genetic data), data subjects' rights (eg, data portability right), as well as new data operators' obligations (eg, data leakage notifications).

Further, in response to the government programme Digital Economy (2017), in September 2019, the Ministry of Digital Development, Communications and Mass Media presented a new draft law amending the PD Law (the Draft Law). The Draft Law proposes to make certain data processing requirements more relaxed (eg, extending the grounds for data processing without data subject's consent). The Draft Law also introduces the notions of anonymised data and anonymized personal data, and makes the processing of the latter subject to the requirements of the Federal Law No. 152-FZ on Personal Data dated 27 July 2006 (the PD Law). In addition, the draft law details the consent requirements, explicitly providing for the possibility to grant consent electronically (by SMS, email and otherwise), as well as a single consent for several processing purposes. As of April 2020, the draft law has not been introduced to the State Duma yet.

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-322-7