

Data Protection & Privacy 2022

Contributing editors
Aaron P Simpson and Lisa J Sotto



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

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer-client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. The information provided was verified between May and July 2021. Be advised that this is a developing area.

© Law Business Research Ltd 2021
No photocopying without a CLA licence.
First published 2012
Tenth edition
ISBN 978-1-83862-644-0

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



Data Protection & Privacy

2022

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

Lexology Getting The Deal Through is delighted to publish the tenth 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 Jordan, Pakistan and Thailand.

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.



London
July 2021

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2021
For further information please contact editorial@gettingthedealthrough.com

Contents

Introduction	5	Hong Kong	104
Aaron P Simpson and Lisa J Sotto Hunton Andrews Kurth LLP		Gabriela Kennedy, Karen H F Lee and Cheng Hau Yeo Mayer Brown	
EU overview	11	Hungary	113
Aaron P Simpson, David Dumont, James Henderson and Anna Pateraki Hunton Andrews Kurth LLP		Endre Várady and Eszter Kata Tamás VJT & Partners Law Firm	
The Privacy Shield	14	India	121
Aaron P Simpson and Maeve Olney Hunton Andrews Kurth LLP		Arjun Sinha, Mriganki Nagpal and Siddhartha Tandon AP & Partners	
Australia	20	Indonesia	128
Alex Hutchens, Jeremy Perier and Meena Muthuraman McCullough Robertson		Rusmaini Lenggogeni and Charvia Tjhai SSEK Legal Consultants	
Austria	28	Israel	136
Rainer Knyrim Knyrim Trieb Rechtsanwälte		Adi El Rom and Hilla Shribman Amit Pollak Matalon & Co	
Belgium	37	Italy	145
David Dumont and Laura Léonard Hunton Andrews Kurth LLP		Paolo Balboni, Luca Bolognini, Davide Baldini and Antonio Landi ICT Legal Consulting	
Brazil	49	Japan	154
Fabio Ferreira Kujawski, Paulo Marcos Rodrigues Brancher and Thiago Luís Sombra Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados		Akemi Suzuki and Takeshi Hayakawa Nagashima Ohno & Tsunematsu	
Canada	57	Jordan	164
Doug Tait and Kendall N Dyck Thompson Dorfman Sweatman LLP		Ma'in Nsair, Haya Al-Erqsousi and Mariana Abu-Dayah Nsair & Partners - Lawyers	
Chile	65	Malaysia	170
Claudio Magliona, Nicolás Yuraszeck and Carlos Araya Magliona Abogados		Jillian Chia Yan Ping and Natalie Lim SKRINE	
China	72	Malta	178
Gabriela Kennedy, Karen H F Lee and Cheng Hau Yeo Mayer Brown		Paul Gonzi and Sarah Cannataci Fenech & Fenech Advocates	
France	82	Mexico	187
Benjamin May and Marianne Long Aramis Law Firm		Abraham Díaz and Gustavo A Alcocer OLIVARES	
Germany	96	New Zealand	195
Peter Huppertz Hoffmann Liebs Fritsch & Partner		Derek Roth-Biester, Megan Pearce and Victoria Wilson Anderson Lloyd	

Pakistan	202	Switzerland	265
Saifullah Khan and Saeed Hasan Khan S.U.Khan Associates Corporate & Legal Consultants		Lukas Morscher and Leo Rusterholz Lenz & Staehelin	
Portugal	209	Taiwan	276
Helena Tapp Barroso and Tiago Félix da Costa Morais Leitão, Galvão Teles, Soares da Silva & Associados		Yulan Kuo, Jane Wang, Brian Hsiang-Yang Hsieh and Ruby Ming-Chuang Wang Formosa Transnational Attorneys at Law	
Romania	218	Thailand	284
Daniel Alexie, Cristina Crețu, Flavia Ștefura and Alina Popescu MPR Partners		John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Patchamon Purikasem Formichella & Sritawat Attorneys at Law Co, Ltd	
Russia	226	Turkey	291
Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva and Alena Neskromyuk Morgan, Lewis & Bockius LLP		Esin Çamlıbel, Beste Yıldızili Ergül, Naz Esen and Nazlı Bahar Bilhan Turunç	
Serbia	235	United Kingdom	299
Bogdan Ivanišević and Milica Basta BDK Advokati		Aaron P Simpson, James Henderson and Jonathan Wright Hunton Andrews Kurth LLP	
Singapore	242	United States	309
Lim Chong Kin Drew & Napier LLC		Aaron P Simpson and Lisa J Sotto Hunton Andrews Kurth LLP	
Sweden	257		
Henrik Nilsson Wesslau Söderqvist Advokatbyrå			

Russia

Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva and Alena Neskromyuk

Morgan, Lewis & Bockius LLP

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 of 27 July 2006 (the PD Law) is the main law governing PII (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 concerning Automatic Processing of Personal Data. In general, the PD Law takes an approach similar to EU Directive 95/46/EC (the 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 (ie, IT) measures for data protection. Notably, the PD Law has concepts similar to the one contained in EU Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR), which became effective in the European Union 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. 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 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 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.

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.

Article 13.11 of the Administrative Code was significantly amended during the past two years. In 2019, article 13.11 was supplemented with liability for non-compliance with the local storage requirement. Fines for the violation of the local storage requirement may be up to 6 million roubles, and up to 18 million roubles for repeated violation. In December 2020, fines for violations of the PD Law (save for violations of the local storage requirement) were increased and new types of liability for the repeated violations were introduced. For example, fines for processing personal data without the written consent of a data subject (if such consent is required) may be up to 150,000 roubles, and up to 500,000 roubles for a repeat violation. Fines for failure to meet the data subject's request to amend, block, or destroy his or her personal data may be up to 90,000 roubles, and 500,000 roubles for a repeat violation.

Also, in contrast to the previous version of article 13.11, which allowed Roskomnadzor to issue in certain cases a 'warning for violations' to give a company time to rectify the wrongdoing, the current version of article 13.11 allows the authority to impose fines only rather than to issue warnings.

Also, 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 of 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 Federal Law No. 152-FZ on Personal Data of 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 health-care 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 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 currently undergo significant developments in light of the covid-19 pandemic. Federal Law No. 123-FZ of 24 April 2020 established a framework for the development, creation, and turnover of artificial intelligence technologies and services, including face recognition products, as a five-year experiment to commence in Moscow on 1 July 2020. Such technologies will be tested and applied for the processing of anonymised personal data (including health-related data) and further used for governmental, municipal management and certain commercial business activities. Requirements and procedures for the use of such technologies are 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 are regulated by Federal Law No. 395-1 on Banks and Banking (1990), 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. Also, 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). Government Decree No. 955 of 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. Order of the Federal Tax Service No. ED-7-11/304@ dated 7 April 2021 sets out requirements for personal data registers of gambling participants compiled by organisers of gambling games.

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 format.

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.

Also, 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 (eg, a company engaged in online business activity) is required to ensure that the recording, systemisation, accumulation, storage, clarification (updating and 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 to achieve the objectives of international treaties, for 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?

Federal Law No. 152-FZ on Personal Data of 27 July 2006 (the PD Law) provides that any operation performed on PII (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 concerning 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 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 general exemptions from the consent requirement, including instances where data is processed:

- under an international treaty or pursuant to Russian law;
- for judicial purposes;
- to render 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 the protection of the life, health or other legitimate interests of the individual, in cases where obtaining his or her consent is impossible;
- for statistical or other scientific purposes, on the condition that the data is anonymised;
- for processing of depersonalised personal data for purposes of state or municipal management as well as for purposes specified in Federal law No. 123-FZ of 24 April 2020 on Experimental Regime for Development and Implementation of Artificial Intelligence Technologies in Moscow;
- for the protection of the data operator's or third parties' rights or the attainment of public purposes, provided there is no breach of an individual's rights and freedoms;
- for mandatory disclosure or publication of personal data in cases directly prescribed by law; or
- in the context of professional journalistic, scientific, literary or other creative activities, provided there is no breach of an individual's rights and freedoms.

Other exemptions from the consent requirement set out in articles 10 to 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:

- 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;
- 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
- biometric personal data, which includes data such as fingerprints, iris images and, arguably, certain types of photographic images.

The processing of data in the last two points 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 before 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 Federal Law No. 152-FZ on Personal Data of 27 July 2006 (the PD Law); and
- the data source.

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 federal law or a contract to which the individual is either a beneficiary or guarantor;
- the personal data permitted for disclosure is processed under prohibitions and restrictions set out in article 10.1 of the PD Law;
- the personal data is processed by the operator for statistical or other research purposes, or to pursue 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, object to 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 and diagnosis) is sensitive. However, if it is administrative or financial information about health such as medical certificates for sick leave management or other human resources-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, some rules 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 may vary from one year up 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 concerning 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?

Several complex security requirements apply to data operators and third-party service providers that process PII (personal data) under the operators' instructions. Federal Law No. 152-FZ on Personal Data of 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 of 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 Federal Service for Technical and Export Control (FSTEK) has issued several 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.

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 the Federal Service for Communications, Information Technology and Mass Communications Supervision (Roskomnadzor), then the operator must 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 Federal Law No. 152-FZ on Personal Data of 27 July 2006 (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 under the PD Law. However, the Federal Service for Communications, Information Technology and Mass Communications Supervision generally expects the data protection officer to be employed by the data operator. The officer 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 officer must:

- implement appropriate internal controls over the data operator and its employees;
- make the data operator's employees aware of PII (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 a 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 Federal Law No. 152-FZ on Personal Data of 27 July 2006 (the PD Law), data operators are required to be registered with the Federal Service for Communications, Information Technology and Mass Communications Supervision (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 of 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 human resources-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 PII (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, 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 the processing;
- the time frame of the 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 paid 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, under the purposes and methods described in the notification, upon submitting notification to Roskomnadzor.

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 of 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 the standard form or precedent of the data transfer agreement approved by the Federal Service for Communications, Information Technology and Mass Communications Supervision (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 PII (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, the 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).

Effective from 1 March 2021, the PD Law has been amended with new rules on the disclosure of personal data. Before 1 March 2021, a data operator had the right to process personal data (inter alia, to disclose personal data) based on a single consent of an individual. Currently, disclosure of personal data requires a separate detailed consent of an individual according to article 10.1 of the PD Law.

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 a party to the above European Convention but are, nonetheless, considered to be 'safe' countries for cross-border transfers (including Canada, Costa Rica, Gabon, Israel, Japan, Kazakhstan, Mali, Mongolia, New Zealand, Peru, Qatar, Singapore, South Africa, New Zealand 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 to protect 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 Federal Law No. 152-FZ on Personal Data of 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 PII (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 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, the Federal Service for Communications, Information Technology and Mass Communications Supervision (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 the Federal Service for Communications, Information Technology and Mass Communications Supervision 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 the Federal Service for Communications, Information Technology and Mass Communications Supervision (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 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

Morgan Lewis

Ksenia Andreeva

ksenia.andreeva@morganlewis.com

Anastasia Dergacheva

anastasia.dergacheva@morganlewis.com

Anastasia Kiseleva

anastasia.kiseleva@morganlewis.com

Alena Neskromyuk

alena.neskromyuk@morganlewis.com

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

electronic communications marketing are set out in article 15 of Federal Law No. 152-FZ on Personal Data of 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 the storage of personal data will be generally subject to all requirements of the PD Law.

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 past couple of years, the localisation requirement remains a key topic affecting all types of processing activities, both on the Internet and offline, in particular, in the context of severe penalties and the emerging court practice.

Harmonisation with the EU data protection concepts has also been largely discussed. Additional Protocol to Council of Europe Convention No. 108 has not been ratified yet. However, its potential implementation would require significant amendments to Federal Law No. 152-FZ on Personal Data of 27 July 2006 (the PD Law), including, the introduction of new concepts ('data controllers' and 'data processors'), categories of personal data (genetic data), data subjects' rights (data portability right) as well as new data operators' obligations (data leakage notifications).

Further, amendments to the PD Law proposed by state authorities are controversial. On one hand, draft law No. 992331-7 presented by the government proposes to make certain data processing requirements more relaxed, for example, to grant one consent for several processing purposes. This draft law was adopted by the State Duma in the first

reading. On the other hand, the government is reportedly working on another draft law aimed to impose additional requirements and restrictions to the processing of depersonalised personal data. According to this draft law, it will be prohibited to use any additional information that helps to determine the identity of a data subject. Also, identification of a data subject will be prohibited save for the cases where it is necessary to protect the health and life of a data subject. This draft law has not been introduced to the State Duma yet.

Coronavirus

47 | What emergency legislation, relief programmes and other initiatives specific to your practice area has your state implemented to address the pandemic? Have any existing government programmes, laws or regulations been amended to address these concerns? What best practices are advisable for clients?

The covid-19 pandemic has forced authorities to take restrictive measures. Most of the anti-covid-19 regulations were adopted by regional authorities. Such measures require employers to collect and process certain health-related data of employees and persons in the employee's household. For example, one of the measures adopted in Moscow is the mandatory medical screening of personnel, which includes temperature screens in the workplace at least once every four hours, covid-19 testing for at least 10 per cent of personnel every 15 days, blood sampling for enzyme immunoassay analysis. The data that employers may collect from such screening is considered sensitive personal data and is subject to certain restrictions of the PD Law on its collection and use. As with any other sensitive personal data, an employer must keep such health-related data received from its employees secure and confidential.

Generally, employers should review and update their personal data protection policies to account for the processing of health-related data, including communicating this data to the authorities or third parties, where required. An employer should consider adopting tailored consent forms that its employees would sign to authorise the employer to process such sensitive data during the pandemic period. Once this period is over, this data must be destroyed in compliance with the PD Law.

Other titles available in this series

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

Also available digitally

[lexology.com/gtdt](https://www.lexology.com/gtdt)