ICLG

The International Comparative Legal Guide to:

# Data Protection 2017

## 4th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Bae, Kim & Lee LLC
Bagus Enrico & Partners
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Cuatrecasas
Dittmar & Indrenius
Drew & Napier LLC
Ecija Abogados
ErsoyBilgehan
Eversheds Sutherland
GANADO Advocates
Gilbert + Tobin
GRATA International
Hacohen & Co.
Herbst Kinsky Rechtsanwälte GmbH
Hunton & Williams
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys-at-Law
LPS L@w
Matheson
Mori Hamada & Matsumoto
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi Attorneys at Law Ltd.
Portolano Cavallo
Rato, Ling, Lei & Cortés Lawyers
Rossi Asociados
Subramaniam & Associates (SNA)
Wikborg Rein Advokatfirma AS

global legal group

global legal group

**Contributing Editors**
Anita Bapat and Aaron P. Simpson, Hunton & Williams

**Sales Director**
Florjan Osmani

**Account Director**
Oliver Smith

**Sales Support Manager**
Paul Mochalski

**Sub Editor**
Hollie Parker

**Senior Editors**
Suzie Levy, Rachel Williams

**Chief Operating Officer**
Dror Levy

**Group Consulting Editor**
Alan Falach

**Publisher**
Rory Smith

**Published by**
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

**GLG Cover Design**
F&F Studio Design

**GLG Cover Image Source**
iStockphoto

**Printed by**
Ashford Colour Press Ltd
May 2017



**ISBN** 978-1-911367-50-5
**ISSN** 2054-3786

**Strategic Partners**

MIX
Paper from responsible sources
FSC® C011748

## General Chapter:



## Country Question and Answer Chapters:

Chapter 26

# Russia

GRATA International

Yana Dianova

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

According to Art. 15 p. 4 of the Constitution of the Russian Federation (hereinafter – the "Constitution"), the universally recognised principles and rules of international law and international treaties of the Russian Federation are the integral part of its legal system, including the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (hereinafter – the "Strasbourg Convention"), which was ratified by Russia in 2005. Art. 23 of the Constitution establishes the right to privacy, including privacy of correspondence and telephone and other communications, for every individual, and Art. 24 prohibits the collection, storage, use and dissemination of the information on an individual's private life without his/her consent. The principles and requirements in the domain of data privacy and data protection are contained in the Federal Law No. 149-FZ dated 27 July 2006 on Information, Information Technologies and Data Protection (hereinafter – the "Information Protection Act"), and the Federal Law No. 152-FZ dated 27 July 2006 on Personal Data (hereinafter – the "Personal Data Act").

### 1.2 Is there any other general legislation that impacts data protection?

Chapter 14 of the Labour Code of the Russian Federation provides for the requirements to employers in connection with employees' personal data protection. The Code on Administrative Offences of the Russian Federation (hereinafter – the "Administrative Code") establishes liability for violation of the rules and requirements for data processing and protection. There are also the decrees of the President of the Russian Federation, the decisions of the Government of the Russian Federation and the orders of the Federal Service for the Supervision of Communications, Information Technology and Mass Media, Federal Service for Technical and Export Control ("FSTEC"), and the Federal Security Service ("FSS"), which establish administrative regulations and requirements regarding data protection in Russia.

### 1.3 Is there any sector-specific legislation that impacts data protection?

Provisions regarding data protection specific to certain sectors are contained, in particular, in the Federal Law No. 126-FZ "On Communication", the Air Code of the Russian Federation (Art. 85.1), the Federal Law No. 395-1-FZ on Banks and Banking Activity, the Federal Law No. 323-FZ on the Fundamentals of Protection of the Health of Citizens in the Russian Federation, the Federal Law No. 79-FZ "On State Civil Service in the Russian Federation", etc.

### 1.4 What is the relevant data protection regulatory authority(ies)?

The principal data protection regulatory authority is the Federal Service for Supervision of Communications, Information Technologies and Mass Media (the abbreviated appellation in Russian is "*Roskomnadzor*"). Its official website in English is found at http://eng.rkn.gov.ru/. *Roskomnadzor* reports to the Ministry of Telecom and Mass Communications of the Russian Federation (the abbreviated appellation in Russian is "*Minkomsvyazy*").

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"

  Any information relating directly or indirectly to an identified or identifiable individual (the data subject).
- "**Sensitive Personal Data**"

  Russian laws do not contain the concept of "sensitive personal data"; instead, the concept of "special categories of personal data" is envisaged by the Personal Data Act, and includes any information that relates to nationality, racial or ethnic origin, political opinions, religious or philosophical beliefs and the state of health or private life.
- "**Processing**"

  Any action (operation) or a set of actions (operations) towards personal data, whether or not performed by automated means, including collection, recording, systematisation, accumulation, storage, alteration (update, modification), retrieval, use, transfer (dissemination, provision, access), depersonalisation, blocking, deletion or destruction.
- "**Data Controller**"

  Russian laws do not contain the concept of "data controller". However, the Personal Data Act provides for the concept of "data operator", which may be a state or municipal body, legal or physical person, that organises and/or carries out (alone

or jointly with the other persons) the processing of personal data and which also determines the purposes of personal data processing, content of personal data and actions (operations) related to personal data.

- "**Data Processor**"

  Russian laws do not contain the concept of "data processor". However, the Personal Data Act refers to a party that may be acting (processing personal data), under the authorisation of the data operator on the basis of the corresponding agreement (including state contract) or by operation of the special state or municipal act and subject to data subject's consent.

- "**Data Subject**"

  An identified or identifiable individual (physical person).

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*

  - "**Cross-border Transfer of Personal Data**"

    Transfer of personal data to a foreign state, foreign state agency, foreign national or legal entity.

  - "**Database**"

    An accumulation of independent materials (articles, calculations, regulations, court decisions and other similar materials) systematised so that these materials may be found and processed by an electronic computer.

  - "**Personal Data Information System**"

    An accumulation of personal data contained in personal databases and information technologies and technical means providing for processing thereof.

  - "**Biometric Personal Data**"

    Data characterising physiological and biological particular features of a human, on the basis of which his/her identity may be ascertained.

  - "**Search Engine**"

    An information system that carries out upon enquiry of a user search on the internet for information with particular content and provides to the user the information on the address of an internet site page for the purposes of access to the requested information on internet sites owned by other persons, except for information systems used for performance of state and municipal functions, provision of state and municipal services, as well as for exercise of other public authorities provided for by federal laws.

## 3 Key Principles

### 3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  The data subject has the right to be informed when his/her personal data are being processed by the data operator. The data operator must, *inter alia*, provide the data subject with information on (1) the purposes and methods of processing personal data, (2) its name and location (address), (3) the personal data being processed and the sources from which it has been received, (4) the persons who have access to personal data (except for the employees of the data operator), (5) the term of processing and retention of personal data, and (6) all other information (as applicable) required to ensure the transparent processing of personal data.

- **Lawful basis for processing**

  Processing of personal data must be done on a lawful and fair basis. The Personal Data Act establishes, in particular, the following lawful grounds for the processing of personal data: (1) a consent in writing is granted by the data subject, or processing is carried out; (2) to achieve the goals provided by an international treaty of the Russian Federation or a law to exercise and perform functions and powers assigned to and obligations imposed on an operator by the legislation – to administer justice, enforce a judgment or an act of another authority or official; (3) to exercise the powers of the federal executive authorities, state extra-budgetary funds, executive state authorities of the constituent entities of the Russian Federation, municipal authorities and functions of organisations involved in the provision of relevant state and municipal services; (4) to perform professional activities of a journalist and/or the lawful activities of mass media, or scientific, literary or other creative activities, or processing is required; and (5) for performance of the contract to which the data subject is a party or a beneficiary.

- **Purpose limitation**

  Processing of personal data must be limited to the achievement of objectives (purposes) which have to be specific, defined in advance and legitimate. Processing of personal data that is not consistent with the purposes of such processing is not allowed.

- **Data minimisation**

  Processing should be carried out only with respect to personal data that is consistent with the purposes of processing personal data. The content and volume of personal data to be processed must fully correspond to the claimed purposes of data processing. The processed personal data shall not exceed the claimed purposes of data processing.

- **Proportionality**

  The personal data must be accurate, sufficient and, where necessary, kept up to date in proportion to the purposes of data processing. The data operator must take all necessary measures (or procure taking the measures) requited to erase personal data, or adjust/rectify incomplete or inaccurate data.

- **Retention**

  Retention (storage) of personal data must be carried out in a form which allows defining the data subject and for a period no longer than is required for the purposes of processing personal data, unless the specific term of storage or retention of personal data is set forth by the law or by the agreement to which the data subject is a party, beneficiary or guarantor. Personal data which is processed must be destructed or depersonalised as soon as the objectives (purposes) of data processing are achieved, or in cases where the achievement of such purposes is no longer effective or necessary, unless it is otherwise provided by the federal law.

- *Other key principles – please specify*

  - **Division of databases of personal data**

    It is not permitted to consolidate databases of personal data which is being processed for incompatible purposes.

## 4 Individual Rights

### 4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  An individual has the right to access his/her data which is being processed by the data operator. The individual (or his/her representative) may file a request with the data operator containing the details of the passport (or another identification document) of the individual or his/her representative and the information on the respective relationship between him/her and the data operator. Such a request may be submitted as an electronic document and contain an e-signature.

Upon receipt of the request, the data operator must confirm the fact of data processing and provide to the data subject all the necessary information, including (1) its name and location (address), (2) the purposes and methods of processing personal data, (3) the personal data being processed and the sources from which it has been received, (4) the persons who have access to personal data, (5) the term of processing and retention of personal data, and (6) all other information required by the law and requested by the data subject. If the required information has not been provided in full by the data operator within 30 days from the original request (unless a shorter period is provided for by the law), the data subject is entitled to submit a repetitive request for provision of access to his/her personal data or the information regarding it. In certain cases, the data subject's right to access may be limited, as prescribed by the federal law.

- **Correction and deletion**

  The data subject may request the data operator to correct or adjust his/her personal data in cases where it is incomplete or inaccurate. The data subject may request as well the data operator to block the personal data, unless it is not prohibited by the law. Furthermore, the data subject is entitled to request the data operator to delete his/her personal data if such data are incomplete, inaccurate, is being processed in violation of the law or unnecessary for the purposes of data processing.

- **Objection to processing**

  The data subject may raise an objection to the processing of his/her personal data by the data operator or withdraw his/her consent to the data processing. Except where the personal data processing cannot be terminated or would result in violation of the law (e.g., labour law), the data operator must discontinue the data processing. Otherwise, the data subject will be able to enforce his/her rights by all available legal remedies.

- **Objection to marketing**

  Personal data may be processed for the purposes of marketing (e.g., by way of direct communications with a respective customer) only with the preliminary consent of the respective data subject. The burden of proof that the data subject's consent has been received rests with the data operator. The data operator must immediately discontinue the processing of the data subject's personal data upon the respective request of the latter.

- **Complaint to relevant data protection authority(ies)**

  In the event that the data subject believes that the data operator is processing his/her personal data in violation of the Personal Data Act or applicable laws, or otherwise infringing upon his/her rights and freedoms, the data subject is entitled to file a complaint with *Roskomnadzor*, or bring a civil action with a court. The data subject may avail herself of other legal remedies, including the reimbursement of losses and moral damages.

- *Other key rights – please specify*

  - **Objection to taking decisions on the basis of personal data automated processing**

    It is prohibited to make decisions that involve legal consequences for a data subject or otherwise concerning his/her rights and lawful interests exclusively on the basis of automated processing of the personal data, unless the data subject has granted a specific consent in writing for this and in other cases has been provided for by the federal laws.

## 5 Registration Formalities and Prior Approval

### 5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

The data operator must notify *Roskomnadzor* of its intention to process personal data before processing, in order to be recorded with the register of data operators. The notification may be submitted by the data operator in paper form or electronically. *Roskomnadzor* shall enter the information contained in the notification submitted by the data operator in the register of data operators within 30 days from the receipt of such notification. The data operator may start processing personal data in accordance with the relevant purposes and methods (as described in the notification) upon registration in the register of data operators maintained by *Roskomandzor*. The information in the register of data operators is publicly available (except for the information on technical means of data protection) (in Russian) at http://rkn.gov.ru/personal-data/register/. The data operator is also obliged to notify *Roskomnadzor* of any changes in the information provided in its original notification and upon termination of the personal data processing.

### 5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

The notification/registration requirement will be applicable to every data operator that is involved in the processing of any categories of personal data in the territory of Russia, and which uses a personal data information system or personal data database.

The data operator is exempt from the obligation to notify *Roskomnadzor* in the cases provided for by the Personal Data Act, in particular, on processing of the personal data:

(1) obtained in accordance with the labour law;

(2) received under a contract to which the respective data subject is a party, provided that such personal data are not transferred to third parties without the data subject's consent, and only used to perform the contract or to enter into further contracts with the data subject;

(3) relating to a certain type of processing by a public association or religious organisation acting under the applicable laws, provided that such personal data are not distributed or disclosed to third parties without the data subject's consent;

(4) made by the data subject publicly available;

(5) consisting only of the surname, first name and patronymic of the data subject;

(6) which is necessary for granting the data subject onetime access into the premises where the data operator is located, or in certain other cases;

(7) contained in the state automated information systems or in the state information systems created for the purposes of state security and public order;

(8) processed without the use of automatic systems under the applicable laws subject to the compliance with the rights of the data subject; and

(9) processed in accordance with the laws and regulations related to the transport security.

**5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)**

Under the Personal Data Act, an entity deemed a data operator is under an obligation to file a notification with *Roskomnadzor* in order to be registered in the register of data operators. According to the official position of *Roskomnadzor*, the notification/registration requirement applies to Russian legal entities and representatives/branch offices of foreign legal entities that are involved in data processing in the territory of Russia. At the same time, foreign legal entities are subject to compliance with the other rules of Russian laws regarding data protection if they process personal data of citizens of the Russian Federation (please see question 16.2 below). Furthermore, in the event that a data operator commissions processing of personal data to a third party (subject to consent in writing of the respective data subject), the data operator is still under the obligation to notify *Roskomnadzor* on personal data processing.

**5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)**

The following information must be included in the notification:

- the name and address of the data operator;
- the purpose of processing personal data;
- the categories of personal data;
- the categories of data subjects whose data are being processed;
- the legal grounds for processing personal data;
- the list of actions towards personal data;
- the description of methods of processing personal data;
- the description of the information systems and the security measures (including encryption) being taken for the protection of personal data;
- the full name and contact details of the Data Protection Officer;
- the start date of processing personal data;
- the term of processing or the condition for termination of processing personal data;
- whether or not the cross-border data transfer of the personal data is carried out in the course of the personal data processing; and
- the location of the databases containing the personal data of the citizens of the Russian Federation.

In the event that incomplete or inaccurate information is provided in the notification, *Roskomnadzor* may require the operator to make the information precise before it is entered into the register of data operators.

**5.5 What are the sanctions for failure to register/notify where required?**

A failure to provide notification to *Roskomnadzor* on the processing of personal data for the registration in the register of data operators may result in an administrative fine up to RUB 5,000 on a legal entity. Also, processing of personal data without notification of *Roskomnadzor*, where such notification is required under the Personal Data Act, will result in an administrative fine up to RUB 10,000 for a legal entity (regarding the administrative fines effective from 1 July 2017, please see question 16.1 below).

**5.6 What is the fee per registration (if applicable)?**

Registration in the register of data operators does not require the payment of any state or official fee.

**5.7 How frequently must registrations/notifications be renewed (if applicable)?**

Registration in the register of data operators is carried out on a permanent basis and does not require renewal. However, the data operator must notify *Roskomnadzor* of any amendments of information in the register of data operators, as well as the termination of the data processing within 10 working days from the respective amendment or termination date.

**5.8 For what types of processing activities is prior approval required from the data protection regulator?**

The data operator must obtain the data subject's consent (unless it is released from such obligation under the law) and implement the necessary organisational/technical measures provided for by the Personal Data Act, the requirements to the protection of personal data in the course of processing thereof in the personal data information systems approved by the Decision of the Government of the Russian Federation dated 1 November 2012 No. 1119 and other applicable regulatory acts. Prior approval by *Roskomnadzor* is not required in order to perform the processing of personal data.

**5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.**

Please see question 5.8 above.

## 6 Appointment of a Data Protection Officer

**6.1 Is the appointment of a Data Protection Officer mandatory or optional?**

The data operator that is a legal entity (company) must appoint a Data Protection Officer. In all other cases, the appointment of the Data Protection Officer will be optional.

**6.2 What are the sanctions for failing to appoint a mandatory Data Protection Officer where required?**

A failure to appoint a Data Protection Officer where such appointment is mandatory may result in the administrative fine of up to RUB 10,000 on the data operator (the respective breach may be revealed upon results of an inspection by *Roskomnadzor*).

**6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?**

The main advantage of voluntarily appointing a Data Protection Officer is that the respective person will be monitoring the organisation of the data processing within the premises of the data operator and compliance by the data operator and its

employees with the data protection laws and regulatory acts. The other advantage is that the Data Protection Officer will be directly in charge with dealing with data subjects' applications or requests.

**6.4 Please describe any specific qualifications for the Data Protection Officer required by law.**

Data protection laws do not establish any specific qualifications for the Data Protection Officer to be appointed by the data operator. As a matter of practice, the Data Protection Officer will be the employee within the IT, administrative, legal or accounting department of the data operator who has sufficient knowledge of the requirements regarding data processing and protection set forth by the applicable legislation and the clarifications (official positions) of the Ministry of Telecom and Mass Communications of the Russian Federation and *Roskomnadzor* regarding application thereof.

**6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?**

Under the Personal Data Act, the Data Protection Officer shall be obliged, in particular: (1) to perform internal control over the compliance by the data operator (its employees) of the data protection legislation, including over the requirements to data protection established by the Government of the Russian Federation and other authorised bodies; (2) to notify the employees of the data operator about the relevant provisions of the data protection legislation, internal regulations (policies) on the issues of personal data processing, requirements to data protection; and (3) to organise the processing of applications and requests of the data subjects (or their representatives) and perform necessary control over such processing. Other responsibilities may be provided by the internal corporate regulations (local acts) of data operators. The Data Protection Officer shall receive specific instructions from the data operator's CEO and shall report directly to the CEO according to the Personal Data Act.

**6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

The information on the Data Protection Officer must be included in the notification to be submitted by the data operator with *Roskomnadzor* and recorded in the register of data operators. Please see question 5.4 above.

## 7 Marketing and Cookies

**7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)**

Marketing communications, whether sent by telephone, email, or SMS text message, without authorisation of recipients, are not allowed. Any marketing communication must be authorised by the data subject beforehand (as required by the Personal Data Act) or addressee (as required by the Federal Law No. 38-FZ dated 13 March 2006 "On Advertising" and the Federal Law No. 126-FZ "On Communication"), the burden of proof of the receipt of such consent lies with the person who ordered messaging or the operator of mobile telephone communications, depending on whose initiative the messaging is affected. The data subject's or addressee's consent may also be revoked; in which case, the data operator or advertising/telecom distributor will have to immediately discontinue any marketing communications to avoid the breach.

**7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

*Roskomnadzor*, the Federal Antimonopoly Service of the Russian Federation, as well as the Federal Service for Surveillance on Consumer Rights Protection and Wellbeing (the abbreviated appellation in Russian: "*Rospotrebnadzor*"), are being quite active in the enforcement of the restrictions on marketing set forth by the national data protection, advertising, telecom and consumer protection legislation. The entities and their officials infringing the restrictions are brought to liability (administrative fines, etc.) depending on the nature of the respective breaches.

**7.3 Are companies required to screen against any "do not contact" list or registry?**

Currently, there is no official "do not contact" list or registry in Russia.

**7.4 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

While breach of data protection legislation, including the use of personal data for marketing communications without prior authorisation, will usually result in the administrative fine of RUB 10,000 (regarding the administrative fines effective from 1 July 2017, please see question 16.1 below), violation of the requirements of the Federal Law "On Advertising" and the Federal Law "On Communication" (e.g. unsolicited SMS text messages) may involve an administrative fine in the amount of up to RUB 500,000. The solicitation marketing communications may be also in breach of the relevant consumer protection legislation if an addressee of the respective communications is not provided with the required and reliable information on the goods (services, works), the manufacturer, seller or provider; in which case, the administrative fine may be up to RUB 10,000.

**7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?**

Russian laws on data protection, advertising and other laws do not contain the definition of "cookies". There are also no official guidelines from *Roskomnadzor* (or another authorised body) on the use or distribution of cookies. However, according to Art. 10 p. 3 of the Information Protection Act, in the event that a person is distributing information using the means allowing identification of an addressee, including by means of sending regular postal messages and electronic messages, such a person must provide to the addressee the explicit option of rejecting such information. It is presumed therefore that all types of cookies require opt-in consent in the absence of specific legislation with regard to cookies.

**7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?**

Please see question 7.5 above.

**7.7 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

*Roskomnadzor* has not taken any enforcement action in relation to cookies so far. In the event that the special legislation regulating the use and distribution of cookies is adopted in the future, *Roskomnadzor* may be granted with the authority to enforce compliance with the respective regulation.

**7.8 What are the maximum penalties for breaches of applicable cookie restrictions?**

In theory, if cookies were regarded simply as marketing communications, the breaches of relevant data protection and advertising/telecom legislation would result in administrative and, if the respective communications involve violation of privacy and unlawful access to computer information, criminal sanctions.

## 8 Restrictions on International Data Transfers

**8.1 Please describe any restrictions on the transfer of personal data abroad.**

In the event of a cross-border transfer of personal data, every data operator must ensure (before such a transfer) that the rights and interests of the respective data subject are fully protected in the "adequate manner" in the respective jurisdiction. All the countries that are signatories to the Strasbourg Convention are regarded as the jurisdictions which provide "adequate protection" of the rights and interests of data subjects. In addition, an official list of countries was adopted by *Roskomnadzor* which provide for "adequate protection" for the purposes of cross-border transfers of personal data. The list includes, in particular, Australia, Argentina, Canada, Israel, United Mexican States and New Zealand. Furthermore, under the Personal Data Act, cross-border data transfer may be prohibited or restricted for thepurposes of protection of the foundations of the constitutional system of the Russian Federation, morality, health, rights and lawful interests of citizens, national defence and security. Cross-border data transfer to any jurisdiction with the "adequate protection" level is not subject to any restriction, provided that the goals of such transfer are in line with the goals of the initial collection of the respective personal data.

At the same time, cross-border transfer of personal data to countries which do not provide the "adequate protection" is permitted only in the following cases:

- the written consent of the respective data subject has been received;
- the cross-border data transfer is allowed under the international treaties to which Russia is a party;
- the cross-border data transfer is allowed under the applicable laws if it is necessary for the purposes of protection of the Russian constitutional system, the national state defence and state security, as well as secure maintenance of the transportation system, protection of interests of individuals, society and state in the transportation sphere from illegal intrusion;
- the cross-border data transfer is carried out for the performance of the contract to which the data subject is a party; or
- the cross-border data transfer is required to protect the data subject's life, health or other vital interests and it is impossible to obtain his/her prior consent in writing.

**8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.**

Typically, companies that are acting as data operators would verify whether or not the country to which personal data is transferred is a party to the Strasbourg Convention or included in the list of countries adopted by *Roskomnadzor* which provide for "adequate protection". Further, such companies would obtain written consent from the respective data subjects for cross-border transfer or execute international data transfer agreements with these subjects. After that, they would proceed with cross-border data transfers in accordance with their internal corporate regulations or policies.

**8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.**

It is not required to register with *Roskomnadzor* or to have approved by the latter consents for cross-border transfer of personal data or the international data transfer agreement. The respective consent or agreement must simply be signed by the relevant data subject, and the agreement by the data operator as well. However, the data operator must notify *Roskomnadzor* on cross-border transfer of the personal data in the notification for the purposes of registration in the register of data operators (please see question 5.4 above).

## 9 Whistle-blower Hotlines

**9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)**

Currently, usage of corporate whistle-blower hotlines is not regulated specifically by Russian laws, and no binding guidance has been issued by *Roskomnadzor* in this regard. Employees may be obliged to "blow the whistle" under the internal regulations (policies) of the employer (data operator), provided that such regulations are approved as local regulatory acts in compliance with the Labour Code.

**9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?**

Anonymous reporting is neither prohibited nor strongly discouraged under the applicable laws. Companies (data operators) need to address this issue in their internal regulations (policies).

**9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.**

It is not required under Russian laws currently in force to have corporate whistle-blower hotlines registered or approved by *Roskomnadzor* or to notify the latter thereof.

**9.4 Do corporate whistle-blower hotlines require a separate privacy notice?**

Under Russian laws currently in force, corporate whistle-blower hotlines do not require a separate privacy notice. However, employees should be notified by data operators on the existence of corporate whistle-blower hotlines and the procedures for their functioning in the internal regulations (policies).

**9.5 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?**

Russian laws currently in force do not require consultation with works councils/trade unions/employee representatives on implementation of corporate whistle-blower hotlines, unless such implementation involves deterioration of the working conditions in the company – in which case, the trade union to which the company's employees are members should be notified three months in advance and consulted with regarding observance of the rights of its members (Art. 12 p.2 of the Federal Law dated 12 January 1996 No. 10-FZ "On Professional Unions, Their Rights and Guarantees of Their Activity").

## 10 CCTV and Employee Monitoring

**10.1 Does the use of CCTV require separate registration/ notification or prior approval from the relevant data protection authority(ies)?**

The use of CCTV in the premises of an employer does not require separate notification/registration or prior approval from *Roskomnadzor* as this issue is in the domain of the employer-employee relationship. Video surveillance will be allowed, on condition that: (1) it is provided for in the employment agreement and regulated under the internal regulations (policies); (2) it is communicated to the employees by way of advance notice, in particular, by placing placards in the areas where CCTV is operating (and against employees' signatures, if CCTV is being installed in the premises of the employer for the first time, since it is deemed as changing the terms of employment); and (3) employees have given their consent to such surveillance in writing. According to the clarifications of *Roskomnadzor*, the CCTV surveillance should be conducted only for specific purposes defined in the respective internal regulations (policies).

**10.2 What types of employee monitoring are permitted (if any), and in what circumstances?**

In practice, different types of employee monitoring may be permitted under the internal regulations and policies of employers (data operators). For example, in addition to video surveillance, companies would sometimes use email/internet browsing and social media monitoring and audio recording. In certain cases, GPS tracking may be applied (i.e., with respect to sales representatives who work in subdivisions of a company outside its principal place of business).

**10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

It is necessary to make the relevant employees (individuals) aware and obtain their prior consent to perform employee monitoring and CCTV surveillance and using his/her biometric personal data, as a separate document signed by each employee. The respective terms and conditions regarding employees' monitoring should be also included in the employment agreements. All the employees should be duly acquainted with the internal regulations or policies effective at the employer's office regarding CCTV surveillance at the work place: current employees – prior to, or upon introduction of the respective surveillance, newly hired employees – prior to, or at the time of, the entering into employment agreements. The employer would also place placards with the notification on surveillance inside/ outside the respective premises. CCTV surveillance with respect to third parties in the premises of a company may be carried out without the consent of the respective persons for security and similar purposes, provided that they are not the main subject of video surveillance and the materials of the surveillance will not be further made public.

**10.4 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?**

Trade unions should be notified three months in advance and consulted with regarding observance of the rights of its members and in writing to the extent that CCTV or other monitoring is introduced against their respective employees (individuals).

**10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?**

Employee monitoring does not require separate notification/ registration or prior approval with *Roskomnadzor*, although some data operators tend to notify *Roskomnadzor* on their right to perform employee monitoring to the extent such monitoring is regarded as a valid security measure according to their internal regulations (policies).

## 11 Processing Data in the Cloud

**11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?**

Russian laws do not prohibit the processing of personal data in the cloud. The data operator needs to obtain the customer's prior consent for a transfer of the customer's personal data to the processor and store/use it at the appropriate server as defined by a cloud computing agreement. In the event that the server is located outside the territory of Russia, the data operator is under an obligation to make sure, before transfer of personal data to the processor, that the server is located in a country which provides for adequate protection of personal data (as defined by the Personal Data Act)

and, in the event that it is located in a foreign country that does not provide for such, to obtain a specific written consent of the customer to cross-border transfer. Furthermore, according to the requirements effective from 1 September 2015, in such cases, the data operator is obliged to provide for initial collection, actualisation and storage of personal data of Russian citizens in the databases located in Russia. If the processor is a Russian legal entity, or a representative/branch office of a foreign legal entity that will be processing the customer's personal data in the territory of Russia under the cloud computing agreement, *Roskomnadzor* must be notified for the purposes of registration of the processor with the register of data operators.

**11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?**

Any cloud computing agreement between a customer and a data operator providing cloud-based services must clearly address all possible data protection issues. Such an agreement should include, in particular, the provisions on the storage location related to personal data (please see question 16.2 below), the purposes of usage of the personal data and the means of their processing, provision of access to such data to the customer and monitoring the customer's data during the term of the agreement. The data operator should be obliged to take the security measures in relation to personal data subject to processing for the purposes of adequate protection thereof and comply with the principles of data processing established by the Personal Data Act. Furthermore, any cloud computing agreement should describe the post-termination obligations of the data operator. Cloud computing agreements are currently not subject for approval by or registration with *Roskomnadzor*.

## 12 Big Data and Analytics

**12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?**

Russian data protection laws do not prohibit the utilisation of big data and analytics in general. However, according to Art. 16 of the Personal Data Act, it is prohibited to adopt any decisions or solutions on the basis of automated processing of personal data only, which may involve certain legal effects concerning data subjects or otherwise significantly affect their rights and interests unless the respective data subject has granted a specific written consent to be subject to such a decision or solution, or in the other cases provided for by federal laws that establish measures to safeguard the data subject's rights and legitimate interests. In this case, the data operator must describe to the data subject the general principles of adoption of the decision on the basis of automated processing of his/her personal data and identify potential legal effects of the same to provide to the data subject the opportunity to object, as well as to describe the procedures for protection by the data subject of his/her rights in this connection. Furthermore, in the event that big data includes biometric personal data obtained in the course of CCTV monitoring, the requirements described in question 10.1 apply, as well as the requirement to use and store such personal data, if outside the information systems, on the tangible media that provide for protection thereof from illegal or accidental access, destruction, alteration, copying, transfer or dissemination. In practice, however, the above-mentioned general rules are rarely applied in the course of utilisation of big data and analytics.

Furthermore, a draft federal law regulating usage of Big Data is currently being developed by a working group for internet development matters under the administration of the President of the Russian Federation. In particular, the common standards for storage and collection of Big Data and unified user agreement for usage of data for all the companies operating in the Russian segment of the internet are being proposed.

## 13 Data Security and Data Breach

**13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?**

The Personal Data Act provides for the data operator's obligation to take or provide for taking necessary legal, organisational and technical measures in the course of processing personal data for protection thereof from unlawful or accidental access, destruction, modification, blocking, copying, provision, or distribution, as well as from any other unauthorised actions with regard to personal data. Such measures include, in particular: (1) appointment of a Data Protection Officer; (2) adoption of the policy on data protection and other documents, including internal regulations (local acts) for the purposes of prevention and detection of breaches of the data protection laws and removal of their consequences; (3) implementation of the legal, organisational and technical security measures provided for the applicable legislation; (4) carrying out internal control and/or audit for the data processing compliance with the data protection laws and data operator's policy/regulations/local acts; (5) evaluation of the damage that may be caused to data subjects in the event of a breach of data protection laws and correlation of such damage and the measures implemented by the data operator; and (6) disclosure of the relevant provisions of the data protection laws and data protection requirements defining the policy/documents/local acts of the data operator to the employees and providing for the respective training of the employees. The data operator must publish its internal data protection policy (e.g., on its internet site) and be ready to disclose all the documents/local acts to *Roskomnadzor*, if so requested in the course of an inspection. Security measures to be taken by a data operator include, in particular: (1) determination of security threats in the course of processing personal data in relevant information systems; (2) provision of the appropriate level of protection of processing personal data in relevant information systems in accordance with the requirements set forth by the Government of the Russian Federation; (3) application of different duly certified means of protection of personal data (including, encryption); (4) evaluation of efficiency of security measures (prior to putting into operation of the information systems); (5) recording of computer media containing personal data; (6) revealing of unauthorised access to personal data; (7) retrieval of personal data that has been modified or destructed due to unauthorised access; (8) adoption of rules governing the access to personal data being processed in relevant information systems, registration and recording of all actions related to personal data in relevant information systems; and (9) control over the security measures with regard to personal data and level of protection of relevant information systems. In accordance with p. 6 of the List of organisational and technical measures for providing security of personal data in the course of processing thereof in information systems approved by the order of the Federal Service for Technical and Export Control ("FSTEC") dated 18 February 2013 No. 21, the data operator evaluates the efficiency of the security measures for protection of personal data independently

or by engaging companies or individual entrepreneurs possessing a licence for technical protection of information. FSTEC clarified as well that the respective evaluation may also be conducted by attestation of a personal data information system in accordance with the National Standard GOST RO 0043-003-2012 "Protection of information. Attestation of the objects of informatisation. General provisions". The use of hardware and software for the purposes of processing certain personal data (e.g., biometric data) would require the approval of FSTEC and/or Federal Security Service ("FSS"). Furthermore, in the event personal data are processed with the use of encryption means of protection of information, the data operator should implement the organisational and technical measures for providing security of personal data in the course of processing thereof in information systems approved by the order of FSS dated 10 July 2014 No. 378.

**13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.**

Generally, there is no legal requirement to report data breaches to *Roskomnadzor* or to individuals (data subjects). In the event that unauthorised processing of personal data is detected, the data operator (or the relevant authorised person) must terminate such processing upon application of the respective data subject within three business days. In cases where it is not possible to provide for processing of personal data in compliance with the applicable law, the data operator must destruct (or provide for destruction by the third party to whom the processing of the personal data was entrusted) such personal data within 10 business days. Following the termination of processing of personal data or destruction thereof, the data operator must notify the data subject (or his/her representative) thereof, and in the event that the request for termination or destruction has been made by *Roskomnadzor*, to notify the latter. If the personal data may not be destroyed within the above-mentioned term, the data operator should block (or provide for blocking by the third party processor) the personal data and destroy it (or provide for their destruction) within six months.

**13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.**

Please see question 13.2 above.

**13.4 What are the maximum penalties for security breaches?**

A breach of the security requirements set forth by the personal data protection legislation may result in an administrative fine of up to RUB 10,000 on the data operator, and in the event that such a breach consists in using uncertified information systems and databases, as well as uncertified information protection, it can entail an administrative fine of up to RUB 25,000 on the data operator with confiscation of the respective uncertified information protection means or without such.

Effective from 1 July 2017, in case of processing personal data without the use of automation means, failure by the operator to comply with the conditions ensuring the safety of personal data during storage of material media of personal data and preventing unauthorised access to them, when it entailed unlawful or accidental access to the personal data, their destruction, change, blocking, copying, provision, distribution or other illegal actions in relation to the personal data (provided that it does not contain the elements of a criminal offence) shall entail a warning or an administrative fine on legal entities in the amount of up to RUB 50,000.

## 14 Enforcement and Sanctions

### 14.1 Describe the enforcement powers of the data protection authority(ies):

| Investigatory Power | Civil/Administrative Sanction | Criminal Sanction |
|---|---|---|
| Sending requests to individuals/ legal entities for providing the necessary information on processing of personal data. | Failure to submit, or untimely submission of, information (data) which is required by the law and is necessary for the performance of lawful activities, or submission of such data in an incomplete or distorted manner shall involve the following administrative sanctions: (1) an administrative fine from RUB 100 to 300 (for individuals); or (2) administrative fine from RUB 300 to 500 (for officials); and (3) administrative fine from RUB 3,000 to 5,000 (for legal entities). | |
| Conducting planned and unplanned inspections and checking the information containing the notifications on the processing of personal data (submitted by the data operators) or engagement of other state agencies for this specific purpose. | | |
| Requiring the data operator to amend, block or destroy false or illegally-obtained personal data. | A failure to perform in due term a lawful prescription (order, decision) of *Roskomnadzor* (its authorised official) regarding amending a breach of the legislation shall involve the following administrative sanctions: (1) an administrative fine from RUB 300 to 500 (for individuals); or (2) an administrative fine from RUB 1,000 to 2,000 or disqualification for a term of up to three years (for officials); or (3) an administrative fine from RUB 10,000 to 20,000 (for legal entities).<br>Effective from 1 July 2017, a failure by the operator to comply within the time limits established by the legislation with the demand of *Roskomnadzor* to clarify personal data, block or destruct them shall involve a warning or an administrative fine on individuals in the amount of up to RUB 2,000; on officials – up to RUB 10,000; on individual businessmen – up to RUB 20,000; on legal entities – up to RUB 45,000. | |
| Restricting access to the information processed in a breach of the data protection laws (provided for blocking of an internet site according to the procedure established by the Information Protection Act). | A failure to perform in due term a lawful prescription of *Roskomnadzor* (its authorised official) on restricting access to the information processed in a breach of the data protection laws shall involve: (1) administrative fine in the amount from RUB 300 to 500 (for individuals); or (2) administrative fine from RUB 1,000 to 2,000 or disqualification for a term of up to three years (for officials); or (3) administrative fine from RUB 10,000 to 20,000 (for legal entities).<br>Effective from 25 March 2017, the same breach shall involve a fine of up to RUB 5,000; for individual entrepreneurs – up to RUB 30,000; for legal entities – up to RUB 100,000. | |
| Suspending or terminating the processing of personal data that has been conducted in breach of the data protection laws. | | |
| Bringing civil actions with competent courts for the protection of rights of data subjects and representing the interests of data subjects before the trial. | The following legal remedies that may be granted upon a court's decision include: (1) termination of the data breaches; (2) award of damages and compensation of moral harm; and (3) publication of a court order. | |
| Sending to FSTEC and FSS the information on the technical and organisational measures for personal data protection implemented by a data operator. | | |
| Filing a petition with the authorised body for the purposes of suspension or cancellation of the licence issued to the data operator. | | |

| Investigatory Power | Civil/Administrative Sanction | Criminal Sanction |
|---|---|---|
| Sending materials to the Prosecutor's Office and other law enforcement agencies for the purposes of commencement of criminal cases in connection with the breaches of data subjects' rights. | | Unauthorised or illegal collection or distribution of data constituting a private secret or a family secret shall involve the following criminal sanctions: (1) a criminal fine of up to RUB 200,000 or salary amount for the period of 18 months; (2) forced labour for the period of 360 hours; (3) correctional works for the period of 12 months; (4) compulsory works for the period of two years with or without disablement for the period of three years; (5) arrest for the period of four months; or (6) imprisonment for the period of up to two years with disablement for a period of three years.<br>Use of personal data obtained by illegal means, if such actions are committed for the purposes of entering data on a straw person in the unified state register of legal entities shall involve the following criminal sanctions: (1) a criminal fine of up to RUB 500,000 or a salary of a convicted person for the period of up to three years; or (2) compulsory works for the period of three years; or (3) imprisonment for the period of up to three years.<br>Illegal access to computer information protected by law, if such action involved distraction, blocking or modification of such information shall involve the following criminal sanctions: (1) a criminal fine of up to RUB 200,000 or a salary of a convicted person for the period of up to three years; or (2) correctional works for the period of 12 months; or (3) compulsory works for the period of two years; or (4) restriction of freedom for the period of two years; or (5) imprisonment for the period of up to two years. |
| Issuing binding prescriptions and bringing the persons at fault to administrative liability. | A failure to perform in due term a lawful prescription (order, decision) of *Roskomnadzor* (its authorised official) regarding amending a breach of the legislation shall involve the following administrative sanctions: (1) an administrative fine from RUB 300 to 500 (for individuals); or (2) an administrative fine from RUB 1,000 to 2,000 or disqualification for a term of up to three years (for officials); or (3) administrative fine from RUB 10,000 to 20,000 (for legal entities). | |

**14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

Typically, *Roskomnadzor* exercises its powers in connection with incompliance by data operators with the requirements of the data protection laws if the respective breaches are reported by data subjects directly to *Roskomnadzor* or its officials reveal them in the course of scheduled or non-scheduled inspections of data operators. In the first case, *Roskomnadzor* usually sends a request to the data operator to provide the information in connection with the data subject's complaint. If the information provided by the data operator confirms that a breach of data protection laws was sustained by the latter or a breach is revealed in the course of an inspection, *Roskomnadzor* will serve a binding prescription to the data operator requiring the rectification of the breach. *Roskomnadzor* may, in addition, impose administrative sanctions (fines) for the relevant breaches of the data protection laws and restrict access to the information being processed in a breach of the personal data protection laws (provide for the blocking of an internet site according to the procedure established by the Information Protection Act). Currently, *Roskomnadzor* conducts inspections of data operators in accordance with the Administrative regulation approved by *Minkomsvyaz*; the schedule of inspections for 2017 is available (in Russian) at http://77.rkn.gov.ru/p5275/p10222/p20168/.

In the event that breaches constituting crimes are committed (i.e., illegal gathering or dissemination of the information constituting a private or family secret of an individual), *Roskomnadzor* may, with the necessary assistance of law enforcement agencies, institute criminal proceedings with respect to officers of the data operator.

## 15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

Russian law, including the Information Protection Act and Personal Data Act, does not contain any specific provisions regarding foreign e-discovery or foreign disclosure proceedings. Art. 15 p. 2 of the Federal Law No. 242-FZ dated 3 December 2008 "On State Genome Registration in the Russian Federation" provides that genome

information (which may be deemed biometric personal data) may be used in the interests of foreign states in accordance with international treaties of the Russian Federation. According to Art. 4 p. 4 of the Personal Data Act, if the international treaty establishes rules which are different from those stipulated by the national data protection legislation, the rules of the international treaty shall be applied. For example, according to Art. 16 of the Convention on legal assistance on civil, family and criminal cases of 1994 to which Russia is a party, Member States shall provide for each other assistance in accordance with their national laws for determination of addresses of persons residing in the territories of the respective Member States, and the justice institutions of the Member States shall provide to each other assistance for determination of the place of work of persons residing in the territories of the respective Member States. Consequently, Russian entities are not obliged to respond to the foreign e-discovery or disclosure requests, unless there are effective imperative provisions set forth by the corresponding international treaties on mutual legal support (assistance), or similar international agreements ratified by Russia. In the absence of such treaties or agreements, Russian entities shall follow the national data protection legislation when assisting foreign law enforcement agencies in terms of privacy or data protection issues.

### 15.2 What guidance has the data protection authority(ies) issued?

*Roskomnadzor* has not issued any official guidance in this regard.

## 16 Trends and Developments

### 16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Within one year from the date of entry into force of the requirements under the Federal Law No.242-FZ dated 21 July 2014 (hereinafter – the "Law No. 242") to data operators to provide for the recording, classification, collection, storage, clarification (updating, changing), and retrieval of the personal data of citizens of the Russian Federation in the course of collection of relevant personal data, including via the internet, by using databases located in the territory of Russia, except for certain cases provided by the Personal Data Act, that became effective on 1 September 2015. By 1 September 2016, *Roskomnadzor* conducted 954 planned scheduled inspections and 82 non-scheduled inspections in the domain of personal data. In the course of these inspections, 1,822 violations of the requirements of the personal data laws were detected, including 23 violations in connection with the localisation of personal data and trans-boarder transfer thereof. In addition, 479 inspections were completed by the end of 2016. In the course of systematic surveillance by *Roskomnadzor*, 492 violations of the requirements of the personal data laws were detected, including eight violations of the requirements of the Law No. 242. In each of the abovementioned cases, prescriptions were issued for eliminating the respective violations with the term for compliance of up to six months. Over 160 internet resources were included in the Register of infringers of the rights of personal data subjects which is available (in Russian) at http://pd.rkn.gov.ru/registerOffenders/viewregistry/ (the Register of infringers).

The first precedent for inclusion into the Register of infringers of a foreign social network and imitation of access thereto was the decision of the Tagansky Court of Moscow dated 4 August 2016 on the claim of *Roskomnadzor* against LinkedIn Corporation (USA), which is an administrator of the internet resources http://www.linkedin.com and http://linkedin.com. The decision was upheld by the appellate ruling made by the civil board of the Moscow City Court dated 10 November 2016.

Federal Law No.13-FZ dated 7 February 2017 amended Art. 13.1 of the Code of the Russian Federation on Administrative Offences (hereinafter – the "Administrative Code") by establishing new sets of offence elements and liability for violations of the legislation on personal data, in particular:

1) personal data processing in cases not provided for by the legislation on personal data, or personal data processing that does not match the purposes of personal data collection, if these actions do not contain elements of a criminal offence, shall involve a warning or an administrative fine on citizens in the amount of up to: RUB 3,000; on officials – up to RUB 10,000; and on legal entities – up to RUB 50,000;
2) personal data processing without the consent in writing by the personal data subject, if these actions do not contain elements of a criminal offence, or personal data processing in violation of the requirements for the information to be included in the consent to the personal data processing established by the legislation on personal data, shall involve an administrative fine on citizens in the amount of up to: RUB 5,000; on officials – up to RUB 20,000; and on legal entities – up to RUB 75,000; and
3) failure by the operator to perform the obligation to publish or otherwise provide unrestricted access to the document that defines the operator's policy in relation to personal data processing, or information about on the current requirements for the personal data protection, shall involve a warning or an administrative fine on citizens in the amount of up to: RUB 1,500; on officials – up to RUB 6,000; on individual businessmen – up to RUB 10,000; and on legal entities – up to RUB 30,000.

The abovementioned amendments become effective from 1 July 2017.

Federal Law No. 18-FZ dated 22 February 2017 introduced amendments to the Administrative Code establishing the administrative liability for a failure by an internet provider to perform the obligation to limit or resume access to the information, access to which should be limited or resumed on the basis of the data received from *Roskomnadzor*: a fine of up to: RUB 5,000 for individuals; for individual entrepreneurs – up to RUB 30,000; and for legal entities – up to RUB 100,000. Protocols on administrative offences under the said article shall be issued by *Roskomnadzor* officials. The authority to consider cases on the respective administrative offences is conferred to judges. The abovementioned amendments become effective on 25 March 2017. (Before this date, the abovementioned failure of an internet provider entails liability under the general provision of the Administrative Code on the liability for engaging in business activity in violation of the licence, in the form of a fine of up to RUB 40,000 for legal entities.)

### 16.2 What "hot topics" are currently a focus for the data protection regulator?

The inspections of data operators' compliance with the requirements of the Law No. 242 to provide for recording, classification, collection, storage, clarification (updating, changing), and retrieval of the personal data of Russian citizens by using databases located in the territory of Russia and the consequences of a failure to comply with this requirement has been one of the "hot topics" for both regulatory authorities and business community.

In November 2016, *Roskomnadzor* presented a new platform, "Digital House", for interaction of government authorities, business and society and invited to participate in development of this platform all the companies, civic and government organisations that implement their proper projects aimed at users security in digital domain. The principal activity areas of "Digital House" shall be improvement and harmonisation of legislation, unification of approaches to data processing in digital domain with a view of international best practices, implementation of self-regulation principle, formation of a safe *modus operandi* model of participants of information processes.

According to the amendments introduced by the Federal Law No.16-FZ dated 22 February 2017 to the Personal Data Act (effective from 1 March 2017), *Roskomnadzor* is authorised to effect control and surveillance over compliance of personal data processing with the requirements of the Personal Data Act (the state control and surveillance over personal data processing). The procedures for organisation and conducting of inspections of legal entities and individual entrepreneurs – personal data operators by *Roskomnadzor*, as well as the procedures for organisation and conducting of the state control and surveillance over personal data processing shall be established by the Government of the Russian Federation.

**Yana Dianova**
GRATA International
21/5, Kuznetsky Most Street
Moscow, 107996
Russia

*Tel:* +7 495 660 11 84
*Email:* ydianova@gratanet.com
*URL:* www.gratanet.com

Yana Dianova was admitted to practise in Russia in 2002. Prior to joining GRATA International (Moscow office) as the Director of the Corporate and Commercial Law Department, she worked as in-house counsel for Nissan Motor Rus, as an Associate in the Tax and Legal Department of Mazars and in the Moscow office of the international law firm, Squire Sanders. Ms. Dianova graduated with a law degree from the International Law faculty of the Moscow State Institute of International Relations (University), received an M.B.A. degree in Management and Business Law from the Moscow International Higher School of Business (MIRBIS), and an LL.M. in Corporate Finance Law from the University of Westminster.

Practice focus areas include:

- Antitrust Law;
- Commercial Law;
- Corporate Law/Mergers & Acquisitions;
- Life Science; and
- Personal Data.

Ms. Dianova speaks Russian, English and French.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com