ICLG

The International Comparative Legal Guide to:

Data Protection 2015

2nd Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

A.G. Erotocritou LLC
Adsuar Muñiz Goyco Seda & Pérez-Ochoa, P.S.C.
Affärsadvokaterna i Sverige AB
Brinkhof
Cuatrecasas, Gonçalves Pereira
Dittmar & Indrenius
ECIJA ABOGADOS
ELIG, Attorneys-at-Law
Eversheds
Gilbert + Tobin
Gorodissky & Partners
Herbst Kinsky Rechtsanwälte GmbH
Hogan Lovells BSTL, S.C.
Hunton & Williams LLP
Juridicon Law Firm
Jurisconsul
Lee and Li, Attorneys-at-Law
Matheson
Mori Hamada & Matsumoto
Opice Blum, Bruno, Abrusio
& Vainzof Advogados Associados
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi
Portolano Cavallo Studio Legale
Subramaniam & Associates (SNA)
Wigley & Company
Wikborg, Rein & Co. Advokatfirma DA

GLG
Global Legal Group

GLG
Global Legal Group

Contributing Editor
Bridget Treacy,
Hunton & Williams

Head of Business Development
Dror Levy

Sales Director
Florjan Osmani

Commercial Director
Antony Dine

Account Directors
Oliver Smith, Rory Smith

Senior Account Manager
Maria Lopez

Sales Support Manager
Toni Hayward

Sub Editor
Amy Hirst

Senior Editor
Suzie Levy

Group Consulting Editor
Alan Falach

Group Publisher
Richard Firth

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 2015

ISBN
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

Russia

Gorodissky & Partners

Sergey Medvedev Ph.D., LL.M.

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Generally, Articles 23 and 24 of the Russian Constitution recognise the fundamental right to privacy for each particular individual. Specifically, the principal national privacy and data protection legislation is contained in the Federal Law No. 149-FZ on Information, Information Technologies and Data Protection (2006) (hereinafter – "Data Protection Act") and the Federal Law No. 152-FZ on Personal Data (2006) (hereinafter – "Personal Data Protection Act"). Finally, the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (2005) (hereinafter – "Strasbourg Convention"), which has been ratified by Russia, protects and enforces data protection at the international level.

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

There are certain local administrative regulations and official requirements which have been issued by the Russian President, Russian Government, Federal Service for Supervision of Communications, Information Technology and Mass Media, Federal Service for Technical and Export Control (FSTEK) and Federal Security Service (FSS) which may also impact data protection in Russia.

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

Specific Data protection provisions can also be found in the aviation (Article 85.1 of the Russian Air Code), labour (Chapter 14 of the Russian Labor Code) and other sectors, such as banking (Federal Law No. 395-1 on Banks and Banking), healthcare (Federal Law No. 323 on the Fundamentals of Protection of the Health of Citizens in the Russian Federation), state/municipal, etc.

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

The principal local data protection regulatory authority is the Federal Service for Supervision of Communications, Information Technologies and Mass Media (also known as "*Roskomnadzor*"; hereinafter – "*Roskomnadzor*"). Its official website can be found in English at: http://eng.rkn.gov.ru/.

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"**

  Any information that relates to nationality, racial or ethnic origin, political opinions, religious or philosophical beliefs and the state of health or sex life.

- **"Processing"**

  Any action (operation) or a set of actions (operations) towards personal data, whether or not performed by the 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 data protection legislation does not contain the concept of "data controller". However, the Personal Data Protection Act refers to 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 data protection legislation does not contain the concept of "data processor". However, the Personal Data Protection Act refers to a party that may be acting (processing personal data), subject to data subject's consent, 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.

- **"Data Owner"**

  A person who has created information on his/her own, or has acquired by law or under an agreement the right to permit or limit the access to information which is defined by certain characteristics.

- **"Data Subject"**

  An identified or identifiable individual (physical person).

- **"Pseudonymous Data"**

  Russian data protection legislation does not contain the concept of "pseudonymous data". However, the Russian Civil Code stipulates that any citizen (individual) may use a pseudonym (assumed name) as provided by the law. Because an individual's name may be one the types of personal data, the pseudonym (assumed name) shall be regarded as personal data in combination with any other information relating directly or indirectly to an identified or identifiable individual (the data subject).

- **"Direct Personal Data"**

  Russian data protection legislation does not contain the concept of "direct personal data". Usually, the question of whether the personal data is direct or indirect will be dependent on the particular situation.

- **"Indirect Personal Data"**

  Russian data protection legislation does not contain the concept of "indirect personal data". Usually, the question of whether the personal data is indirect or direct will be dependent on the particular situation.

- *Other key definitions*

  "Cross-border Transfer of Personal Data"

  Transfer of personal data to a foreign state, foreign state agency, foreign physical or legal person.

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 her or his personal data is being processed by the data operator. The data operator must *inter alia* provide to the data subject (1) the purposes and methods of processing of personal data, (2) its name and location (address), (3) the recipients of personal data, (4) the persons who have access to personal data, (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. For example, the processing of personal data shall be made with the consent of a data subject, unless the data processing is subject to certain legal exemptions. The data subject may freely grant consent to processing of the relevant personal data using her or his will and interest. Data operators or other persons who have obtained an access to personal data shall not disclose or distribute such personal data to third parties without the consent of the data subject, unless otherwise provided by the law.

- **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 shall be made only with regard to personal data that is consistent with the purposes of processing of 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 be excessive as to the claimed purposes of data processing.

- **Proportionality**

  Personal data may be processed only insofar as it is adequate and relevant. 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 secure the effectuation of measures) related to erasure of personal data, or adjusting/rectifying of incomplete or inaccurate data.

- **Retention**

  Retention of personal data must be done in a form which allows defining the data subject for as long as the purposes of processing of personal data are effective or necessary, 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 valid 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 case the achievement of such purposes is no longer effective or necessary, unless otherwise provided by the law.

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 her or his data being processed by the data operator. The individual (or her/his representative) may send a request to the data operator by submitting a passport (or similar document) and describing the respective relationship between her/him and the data operator. Such a request may be sent out as an electronic document and contain an e-signature. Upon receipt of such 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 of personal data, (3) the recipients of personal data, (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, the data subject reserves the additional right to have further access to data. In certain cases, the data subject's right to access may be limited, as prescribed by the law.

- **Correction and deletion**

  The data subject may request the data operator to correct or adjust her/his personal data in case it is incomplete or inaccurate. Also, the data subject may request the data operator to block the personal data, unless it is not prohibited by the law. Further, the data subject may request the data operator to delete her/his personal data if such data is incomplete, inaccurate, illegitimate or unnecessary for the purposes of data processing.

- **Objection to processing**

  The data subject may raise an objection to processing of her/his personal data by the data operator. 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 her/his rights by all possible legal means.

- **Objection to marketing**

  Processing of personal data for the purposes of marketing (e.g. by way of direct communications with a respective customer)

shall be allowed only with the preliminary consent of the data subject. The burden of proof that the data subject's consent has been received rests with the data operator. If so requested by the data subject, the data operator must immediately discontinue the processing of her/his personal data.

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

  If the data subject believes that the data operator is processing her/his personal data in violation of the data protection legislation, or otherwise infringing upon her or his rights and freedoms, the data subject has the right to file a complaint with Roskomnadzor, or bring a civil action with the competent court. In any event, the data subject may seek various legal remedies, including the reimbursement of losses and moral damages, as available under the law.

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.)

Before processing of any personal data the data operator must notify Roskomnadzor of its intention related to data processing in order to be recorded with the relevant register. The notification may be submitted by the data operator on paper or electronically. The data operator does not need to notify Roskomnadzor of every case of data processing, although it has to notify Roskomnadzor of the corresponding amendments (as applicable). Practically, the data operator may start processing personal data in accordance with the relevant purposes and methods (as described in the notification) only upon registration with Roskomandzor. Roskomnadzor maintains a register of data operators based upon the information contained in the notifications received. The register of data operators is public and may be found in Russian at: http://rkn.gov.ru/personal-data/register/.

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 processing of different categories of personal data in the territory of Russia and is using its internal IT system or database subject to the data protection legislation. At the same time, the data operator will be released from this statutory requirement and will be able to process personal data without notification/registration in the following instances:

- personal data is processed only under the labour law;
- personal data has been received by the data operator in connection with a contract with a respective data subject (individual), provided that such personal data is not transferred to third parties without the individual's consent, and only used to perform the contract or to enter into further contracts with the individual;
- personal data relates to a certain type of processing by a public association or religious organisation acting under the applicable laws, provided that such personal data is not distributed or disclosed to third parties without the data subject's consent;
- personal data has been made publicly available by the data subject;
- personal data consists only of the surname, first name and patronymic of the data subject;
- personal data is necessary for granting the data subject one-time access into the premises where the data operator is located, or in certain other cases;
- personal data is included in IT systems that have acquired the status of state computer IT systems under the applicable laws, or in state IT systems created for the purposes of state security and public order;
- personal data processed without the use of automatic systems under the applicable laws subject to the compliance with the rights of the data subject; and
- personal data 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.)

According to the official position of Roskomnadzor, the notification/registration requirement must be secured by the local legal entities and representatives/brand offices of foreign legal entities that are involved in data processing in the territory of Russia. At the same time, foreign legal entities and companies will be subject to compliance with the other rules of Russian data protection legislation, provided they process personal data of Russian individuals (please see question 16.2 below).

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 of personal data;
- the categories of personal data;
- the categories of data subjects whose data is being processed;
- the list of actions towards personal data, the description of methods of processing of personal data;
- the description of IT systems and security measures (including encryption);
- the 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;
- the cross-border data transfer; and
- the location of the database containing the personal data of the Russian individuals (starting from September 1, 2015 (please see question 16.2 below)).

In the absence of any further questions or enquiries, Roskomnadzor carries out the registration of the data operator within 30 days from the date of receipt of the corresponding notification. All of the above information, except for the description of the data operator's IT systems and corresponding security measures, becomes publicly available (once included in the register).

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

Failure to provide notification to Roskomnadzor and secure registration in the register of data operators may result in an administrative fine up to 10,000 RUB (for legal entities). Also, failure to notify Roskomnadzor on the data processing will result in an administrative fine up to 5,000 RUB.

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

Notification (or any further amendment – as applicable) and registration does not require the payment of any state or official fee.

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

Relevant registration shall not be renewed, although the data operator must notify Roskomnadzor of any amendments of information in the register of data operators as well as any information on the termination of data processing within 10 working days from the corresponding amendment or termination date.

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

Aside from notification/registration requirement, the data operator must obtain the data subject's consent (unless it is released from such obligation by the law) and implement the other necessary organisational/technical measures required under the law before processing any personal data. Prior approval from Roskomnadzor is not required in order to perform data processing activities.

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?

Yes, the data operator that is acting as 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?

Failure to appoint a mandatory data protection officer may result in the administrative fine of up to 10,000 RUB (as a result of inspection and binding order of 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 will be the selection of a responsible person who will be monitoring the organisation of the data processing within the premises of the data operator and compliance by the data operator with the data protection legislation. The other advantage would be the involvement of the data protection officer in the processing of data subjects' requests or letters.

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

Data protection legislation does not set any specific qualifications for the data protection officer to be engaged by the data operator. In practice, the data protection officer will be the employee within the administrative, legal or accounting department of the data operator who has a good general knowledge of the data protection legislation.

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

The data protection officer must receive specific instructions from the data operator's CEO (and has to report directly to the CEO) according to the provisions of the Personal Data Protection Act. Generally, the data protection officer shall be obliged by operation of law: (1) to perform internal control over the compliance by the data operator (its employees) of the data protection legislation, including over the requirements on data protection; (2) to notify the employees of the data operator about the relevant provisions of the data protection legislation, local rules or acts on the issues of personal data processing, requirements on data protection; and (3) to organise the processing of letters 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 rules or acts of data operators.

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

The data protection officer must be notified to 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, e-mail, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

Unauthorised marketing communications, whether sent by telephone, e-mail, or SMS, are not allowed. Any marketing communication must be authorised by the data subject (as required by the Personal Data Protection Act) or addressee (as required by the national advertising/telecom legislation) beforehand. 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?

Yes, Roskomnadzor, the Russian Federal Antimonopoly Service as well as the Russian Consumer Protection Agency (also known as "*Rospotrebnadzor*") are being quite active in the enforcement of the breaches of marketing restrictions set forth by the national data protection, advertising, telecom and consumer protection legislation. The relevant infringers are severely prosecuted depending on the nature of such breaches.

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

In practice, different administrative penalties (fines) are usually imposed for sending unauthorised marketing communications. For example, while breach of data protection legislation, including the use of personal data, will usually result in the administrative fine of 10,000 RUB, violation of relevant advertising/telecom legislation (e.g. unsolicited SMS text message) may lead to an administrative fine for the amount of up to 500,000 RUB. Sometimes, the solicitation marketing communications will be in breach of the relevant consumer protection legislation in which case the administrative fine may be up to 20,000 RUB.

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

Neither the national data protection, nor the advertising legislation, nor any other laws contain the definition of "cookies". Also, there are no official guidelines from Roskomnadzor (or other state agency) on the use or distribution of cookies. According to Article 10 (3) of the Data Protection Act, a person who is distributing information must provide to the addressee the explicit option of rejecting such information when using the means allowing identification of such addressee, including when sending regular post messages and electronic messages. Hence, it is now presumed that all types of cookies require opt-in consent in the absence of specific legislation with regard to cookies.

7.5 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 7.4 above.

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

To date, Roskomnadzor has not taken any enforcement action in relation to cookies. If the special legislation that will govern the use and distribution of cookies is adopted in the future, Roskomnadzor will be able to take relevant enforcement actions, provided it is empowered with such legal competence.

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

Theoretically, if cookies were regarded simply as marketing communications, the breaches of relevant data protection and advertising/telecom legislation would entail various administrative and criminal sanctions. To date, there is no case yet in this regard.

8 Restrictions on International Data Transfers

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

In the event of an international transfer of personal data every data operator must ensure (before such transfer) that the rights and interests of the respective data subject are fully protected in the "adequate manner" in the corresponding foreign country. All countries that are signatories to the Strasbourg Convention are regarded as the jurisdictions which provide "adequate protection" of rights and interests of data subjects. In addition, Roskomnadzor has adopted an official list of countries (including Australia, Argentina, Canada, Israel, Mexico and New Zealand) which may secure "adequate protection" for the purposes of cross-border transfers of personal data. International data transfer to any jurisdiction with the "adequate protection" level is not subject to any restriction, provided that the consent of the respective data subject has been received.

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

- the written consent of the respective data subject has been received;
- the cross-border data transfer is allowed under the international treaties (which Russia is a party to);
- 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 made 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 her/his 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 check the level of data protection before transferring any personal data abroad. Further, such companies would obtain written consents from the respective data subjects 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 rules 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.

Roskomnadzor does not need to register or approve the international data transfer agreement. Such agreement must be simply signed by the relevant data operator and data subject. However, the data operator must notify Roskomnadzor of its right to cross-border data transfer at the time of sending the notification for the purposes of registration (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.)

Corporate whistle-blower hotlines are not regulated under the applicable laws, nor is there any binding guidance issued by Roskomnadzor in this regard. Employees may be obliged to "blow the whistle" under the internal corporate rules or policies of the employer (data operator).

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 not prohibited, neither is it strongly discouraged, under the applicable laws. Typically, companies (data operators) would address this issue in their internal corporate rules or 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.

Corporate whistle-blower hotlines do not require separate notification/registration or approval with Roskomnadzor.

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)?

CCTV does not require separate notification/registration or prior approval from Roskomnadzor as this issue will usually be dependent on the employer-employee relationship. Video surveillance will be allowed, provided that: (1) it is provided in the employment agreement and regulated under the internal corporate rules or policies; (2) it is communicated to the employees by way of advance notice (e.g. data placards in the premises); and (3) employees have given their consent to such surveillance. It is also assumed that the employers must use the CCTV on a reasonable basis and avoid disclosures of video-content to third parties.

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 corporate rules and policies of employers (data operators). For example, in addition to video surveillance, companies would sometimes use e-mail/Internet browsing, social media monitoring and audio-listening. In rare cases, GPS tracking may be applied.

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

Yes, it is necessary to make the relevant employees (individuals) aware and obtain their prior consent to perform employee monitoring. Typically, employers would place data placards inside/outside the premises of the business and obtain written consent from all employees at the time of execution of employment agreements. Prior to the execution of employment agreements, all employees will be duly acquainted with the internal corporate rules or policies effective at the employers' offices.

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

Works councils, trade unions and employee representatives must be notified/consulted in advance and in writing to the extent the 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 corporate rules or policies as well as their data protection 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)?

Data protection legislation does not prohibit the processing of personal data in the cloud. Depending on the nature of cloud computing agreement and data in question, the processor may need to obtain the customer's prior consent to be able to store/use it at the appropriate server as defined by the agreement. The processor's privacy policy and specific contractual obligations have to be given due diligence. If the processor represents the Russian legal entity, or 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 made by a customer and processor providing cloud-based services must clearly address all possible data protection issues. Provisions, such as on the storage location related to personal data (please see the question 16.2 below), usage of the personal data, access to such data and monitoring the customer's data during the contractual term, must appear in the agreement of this type. In addition, any cloud computing agreement should describe the post-termination obligations of the processor. Finally, the processor shall be obliged to take the most effective security measures in relation to personal data subject to processing. Cloud computing agreements shall not be recorded or approved by 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)?

Data protection legislation does not prohibit the utilisation of big data and analytics in general. However, it has to be noted that it is prohibited by law to adopt any decisions or solutions on the basis of automated processing of personal data which may produce certain legal effects concerning data subjects or otherwise significantly affect their rights and interests (Article 16 (1) of the Personal Data Protection Act). At the same time, any data subject may be theoretically subjected to such a decision or solution, provided the written consent has been obtained in due course, or in all other cases as authorised by the applicable law which also lays down specific measures to safeguard the data subject's legitimate rights and 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 her/his personal data and identify potential legal effects of the same (along with the option of opt-out). In addition, the data operator must discuss the enforcement proceedings with the data subject. In practice, these basic rules or steps are rarely tested in the course of utilisation of big data and analytics.

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 Protection Act provides for the data operator's obligation to take necessary and sufficient protective measures (by defining the content and list of such measures) to comply with the data protection legislation. Specifically, the data operator must: (1) appoint a data protection officer; (2) adopt the data protection policy and other documents, including local/corporate rules, intended for prevention and detection of breaches of the data protection legislation; (3) apply for the relevant legal, organisational and technical security measures; (4) perform internal control and/or audit for the data processing compliance with the data protection legislation and data operator's policy/documents/local; (5) evaluate the damages that may be caused to data subjects in the event of breach of data protection legislation; and (6) disclose the relevant provisions of the data protection legislation and data protection requirements defining the policy/documents/local rules of the data operator to the employees and secure appropriate studies of the employees. The data operator must publish its internal data protection policy (e.g. on the Internet) and be ready to open all the documents/local rules to *Roskomnadzor*, if so requested in the course of inspection.

In any event, the data operator must take necessary legal, organisational and technical measures for the protection of personal data from any unauthorised/illegal or accidental access, destruction, modification, blocking, copying, provision, or distribution as well as from any other unauthorised actions with regard to personal data. Security measures may be established by way of: (1) location of security threats in the course of processing of personal data in relevant IT systems; (2) provision of the appropriate level of protection of processing of personal data in relevant IT systems; (3) application of different certified methods of protection of personal data (including, encryption); (4) evaluation of efficiency of security measures (prior to implementation of the same); (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 the unauthorised access; (8) adoption of rules governing the access to personal data being processed in relevant IT systems, registration and recording of all actions related to personal data in relevant IT systems; or (9) control over the security measures with regard to personal data and level of protection of relevant IT systems.

In most cases, any IT system that is processing personal data of an individual must be duly certified by Federal Service for Technical and Export Control. Otherwise, the use of hardware and software for the purposes of processing of certain personal data (e.g. biometric data) would require the approval of the Federal Service for Technical and Export Control and/or Federal Security Service. Further, the encryption is not prohibited, although it must be secured in accordance with the applicable rules and regulations.

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 of location or detection of unauthorised processing of personal data the data operator (or the relevant authorised person) must terminate such processing within three business days. In case it is not possible to turn the unauthorised processing of personal data into a legitimate manner of processing, the data operator must destruct such personal data within 10 business days. Following the termination of processing of personal data or destruction of personal data, the data operator must notify the data subject (or its representative), and in the event the request for termination or destruction has been made by Roskomnadzor – the notification must be sent to *Roskomnadzor*.

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.

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 and obtain necessary information on processing of personal data.		
Doing inspections and checking the information containing the **notifications on processing of personal data** (submitted by the data operators) or engagement of other state agencies for this specific purpose.	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 may entail the following. **administrative sanctions**: (1) warning or administrative fine in the amount from 100 to 300 RUB (for individuals); (2) warning or administrative fine from 300 to 500 RUB (for officials); or (3) warning or administrative fine from 3,000 to 5,000 RUB (for legal entities).	
Claiming rectification, blocking or destruction of false or illegally-obtained personal data.		
Limiting access to data that is processed under the breach of the data protection legislation (starting from September 1, 2015 (please see question 16.2 below).		
Suspending or terminating the processing of personal data that has been initiated under the breach of the data protection legislation.		
Bringing **civil actions** with competent courts for the protection of rights of data subjects and representing the interests of data subjects before the trial.	Civil action will lead to the following **legal remedies**: (1) cessation of the data breaches; (2) damages, including moral damages; (3) publication of court order; and (4) other remedies (as applicable).	
Filing petitions to the Federal Service for Technical and Export Control, Federal Security Service and other state agencies for the purposes of suspension or cancellation of relevant licences.		
Sending materials to the Prosecutor's Office and other law enforcement agencies for the purposes of commencement of **criminal cases** for the data breaches.		Unauthorised or illegal collection or distribution of personal data or privacy data may lead to the following **criminal sanctions**: (1) criminal fine of up to 200,000 RUB; (2) salary amount for the period of 18 months; (3) forced labour for the period of 360 hours; (4) correctional works for the period of 12 months; (5) compulsory works for the period of two years with or without disablement for the period of three years; (6) arrest for the period of four months; or (7) imprisonment for the period of up to two years with disablement for a period of three years.
Issuing binding orders and bringing the guilty persons to **administrative liability**.	Breach of the established legal order for the collection, storage, use or distribution of personal data may entail the following **administrative sanctions**: (1) warning or administrative fine from 300 to 500 RUB (for individuals); (2) warning or administrative fine from 500 to 1,000 RUB (for officials); or (3) warning or administrative fine from 5,000 to 10,000 RUB (for legal entities).	

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

Typically, Roskomnadzor will serve a binding order to the data operator requiring the rectification of the personal data due to the breach of data protection legislation. Further, Roskomnadzor will usually impose certain administrative sanctions for the relevant data breaches. Also, Roskomnadzor may seek criminal prosecution (using the necessary assistance of law enforcement agencies) against the data infringers. Although different administrative fines and blockage of infringing Internet-resources will be the examples of liability/consequences for offended persons in recent privacy cases, there have been a lot of talks and arguments in favour of strengthening the overall sanctions against violation of data protection legislation in Russia.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

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

Russian law, including the Data Protection Act and Personal Data Protection Act, does not contain any provisions related to foreign e-discovery or foreign disclosure proceedings. Therefore, Russian companies 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, to which Russia is a party. According to Article 4 (4) of the Personal Data Protection Act, if the international treaty sets out the rules different from those stipulated by the national data protection legislation, the rules of the international treaty shall be applied. In the absence of such treaties or agreements, Russian companies shall be guided by 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.

Privacy and data protection is an emerging, trendy area of law nowadays. Data protection legislation has been enforced quite actively over the last few years in Russia. Specifically, data subjects would send various complaints to Roskomnadzor, and appeal the orders of Roskomnadzor with the competent courts, while seeking appropriate legal remedies, including moral damages, available under the law. On a separate note, there have been a growing number of appeals by data operators against orders/decisions of Roskomnadzor/courts imposing different administrative sanctions and blockage of Internet-resources for the breaches of data protection legislation. Therefore, the national case law in the sphere of data protection continues to develop all the time.

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

One of the "hot topics" that is currently under the focus of Roskomnadzor and the "audience" is the so-called "new data localisation law" that has been adopted and will become effective very soon in Russia. On July 21, 2014 the President of the Russian Federation has signed Federal Law No. 242-FZ "On Amendments to Certain Legislative Acts of the Russian Federation for Clarification of Personal Data Processing in Information and Telecommunication Networks" (hereinafter – "New Data Protection Law"), which will become effective on September 1, 2015 according to the amendments to the New Data Protection Law that have already been adopted by the Federal Law No. 526-FZ dated December 31, 2014.

The New Data Protection Law addresses basically two issues: (1) the New Data Protection Law amends the Personal Data Protection Act by way of introducing certain new obligations for data operators with regard to collection, storage and processing of personal data of Russian citizens (individuals); and (2) the New Data Protection Law amends the Data Protection Act by introducing the new mechanism for Roskomnadzor to block websites and online resources which process personal data of Russian citizens (individuals) in an illegal manner. Specifically, the New Data Protection Law introduces an obligation on all data operators to "ensure recording, systematisation, accumulation, storage, modification and extraction of personal data of Russian citizens with the use of data centres located in the territory of the Russian Federation in the course of collection of relevant personal data of individuals, including via the Internet". In other words, any personal data of Russian citizens (individuals) collected by data operators will have to be stored in servers, IT systems or data centres located in Russia. Although the New Data Protection Law does not stipulate this expressly, the mentioned requirement is likely to be interpreted as prohibiting the storage of personal data on Russian citizens (individuals) outside Russia. At the same time, the New Data Protection Law does not prohibit accessing the servers, IT systems or data centres to be located within the Russian territory from abroad, nor does the New Data Protection Law impose any special restrictions on the transfers, including cross-border data transfers, or duplication of data. Therefore, by literal interpretation of the New Data Protection Law foreign companies would be required to process or organise processing of personal data of the Russian citizens in Russia, subject to compliance with all other general requirements of the data protection legislation.

New Data Protection Law may raise a number of issues that would require further clarification. However, it is anticipated that certain official comments/arguments or practical guidance/tips will be issued or provided in the future by the time the New Data Protection Law will be tested in practice.

Sergey Medvedev Ph.D., LL.M.
Gorodissky & Partners
B. Spasskaya, 25, bldg.3
129090 Moscow
Russia

Tel: +7 495 937 6116
Fax: +7 495 937 6104
Email: medvedevs@gorodissky.ru
URL: www.gorodissky.com

Sergey is a senior lawyer working in the Moscow office of the law firm "Gorodissky & Partners" (Russia). He is officially registered as the trademark, design, software and database attorney. He specialises in various legal issues related to legal protection, ownership, acquisition, exploitation, licensing, franchising, securitisation, litigation and enforcement of IP and IT rights in Russia and the Commonwealth of Independent States (CIS). Sergey deals with various types of IP/IT, including copyrights and related rights, software and databases, patents and designs, trademarks, brands, and domain names. He also deals with know-how and confidential information as well as privacy and data protection.

Sergey provides legal support to clients in connection with different transactions related to the disposal and conveyance of IP/IT assets. He is regularly in charge of developing, reviewing, negotiating and perfecting (registering) licensing agreements, franchising contracts, security interests and other arrangements. Sergey is also involved in heavyweight M&A, joint venture and investment projects, IP/IT legal due diligence and IP/IT transfer process.

Sergey litigates IP/IT rights and combats unlawful/unauthorised use of IP/IT and illegal content on the Internet, unfair competition and false advertising, parallel imports and grey market goods, counterfeits and piracy. He represents the interests of clients in commercial courts and courts of general jurisdiction and with law enforcement agencies on different infringement matters. Sergey participates in extra-judicial as well as judicial dispute resolution actions, civil procedures, and administrative and criminal proceedings.

Sergey also advises the clients on data notifications, registrations and cross-border data transfers, employee monitoring, marketing communications, outsourcing and cloud computing. He is regularly involved in data audits and implementation of security measures, including encryption. He has been engaged in several data breach matters representing the data operators on the defendant-side.

Sergey delivers speeches at seminars and conferences. He is the author of a number of articles and works published by the leading Russian and international publishing houses, such as Global Legal Group (GLG), Kluwer, Getting The Deal Through (GTDT), Les Nouvelles, IPProTheInternet and others.

GORODISSKY

Gorodissky & Partners (G&P) is a universal intellectual property (IP) law firm providing a full range of services connected with the IP life cycle. The firm researches, prosecutes, acquires, exploits, evaluates, commercialises, transfers, franchises, protects, defends, litigates and enforces IP and related intangible assets. G&P practices IP law in Russia, Ukraine and the Commonwealth of Independent States (CIS).

G&P is the biggest IP law firm in the Russian jurisdiction, residing in the list of the 10 largest IP firms in Europe. Over 400 employees, including 140 registered patent/trademark attorneys and IP lawyers, work for the firm.

The firm's patent/trademark attorneys and IP lawyers are members of AIPPI, FICPI, LESI, INTA, MARQUES, ECTA, PTMG, AIPLA, ABA, the Russian Chamber of Patent Attorneys and the Council of Eurasian Patent Attorneys. Many of them have advanced technical backgrounds in combination with legal and economic degrees.

G&P deals with all types of IP in various business sectors, including aviation and automotive, banking and financial, biotechnology and life sciences, consumer products and retail, energy and utilities, hotels and leisure, mechanical and industrial, oil and gas, sports, media and entertainment, nanotechnology and telecoms. The firm handles different matters and projects, whether contentious (litigious) or non-contentious (commercial), related to copyrights, related rights and designs, software and databases, patents and know-how, trademarks, brands and domain names, mask works and semiconductor chips, as well as plant breeders' rights.

G&P is also famous for its new data protection and privacy practice. The law firm has much legal experience and professional day-to-day expertise in data notifications, registrations and cross-border data transfers, data audits and security, advertising and marketing communications, outsourcing, cloud computing and big data, data breach prosecution and enforcement.

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 Recovery & Insolvency
- Corporate Tax
- Data Protection
- Employment & Labour Law
- Environment & Climate Change Law
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Litigation & Dispute Resolution
- Lending & Secured Finance
- Merger Control
- Mining Law
- Oil & Gas Regulation
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks

GLG
Global Legal Group

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

www.iclg.co.uk