GRATA INTERNATIONAL

PERSONAL DATA PROTECTION IN RUSSIA

1 Legislative Framework and Regulatory Authorities

1.1 What are the principal laws on data protection?

The Constitution of the Russian Federation (hereinafter – the "Constitution") establishes the right to privacy, including privacy of correspondence and telephone and other communications, for every individual (Art. 23) and prohibits collection, storage, use and dissemination of the information on an individual's private life without his/her consent (Art. 24). Art. 15 p. 4 of the Constitution also provides the universally recognised principles and rules of international law and international treaties of the Russian Federation are the integral part of its legal system, which applies to the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (hereinafter – the "Strasbourg Convention") that was ratified by Russia in 2005.

The principles and requirements in the domain of data privacy and data protection are contained in the Federal Law No. 149-FZ dated 27.07.2006 on Information, Information Technologies and Data Protection (hereinafter – the "Information Protection Act"), and the Federal Law No. 152-FZ dated 27.07.2006 on Personal Data (hereinafter – the "Personal Data Act").

1.2 Are there any other law and regulatory acts that impact data protection?

Chapter 14 of the Labour Code of the Russian Federation provides the requirements to employers in connection with employees' personal data protection. 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 Supervision of Communications, Information Technology and Mass Media, Federal Service for Technical and Export Control ("FSTEC"), and the Federal Security Service ("FSS") adopted on the basis of

the Personal Data Act, an Information Protection Act and other federal laws establish detailed administrative regulations and requirements regarding data protection in Russia. 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.

1.3 Is there legislation that impacts data protection in specific sectors?

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 Which regulatory authority(ies) is (are) supervising data protection?

The principal authorised body for the protection of the rights of subjects of personal data, which is responsible for ensuring control and supervision over the compliance of processing of personal data with the requirements of Personal Data Act 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 can be 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 Terms and Definitions

2.1 What are the key definitions used in the data protection legislation?

- **"Personal Data"**

  Any information relating directly or indirectly to an identified or identifiable individual (the data subject).

- **"Biometric Personal Data"**

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

- **"Special Categories of 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.

- **"Data Operator"**

  A state or municipal body, legal entity or individual, 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 Subject"**

An identified or identifiable individual (physical person)

- **"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.

- **"Search Engine"**

  An information system that carries out upon enquiry of a user search in 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 providedfor by federal laws.

3 Key Principles of Data Processing

3.1 What are the key principles that apply to the 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 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 for 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 judgement or an act of another authority or official; (3) to exercise 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.

- **Transparency**

  A data subject has the right to be informed when his/her personal data is being processed by the data operator. The data operator must, *inter alia*, provide to the data subject the information on (1) the purposes and methods of

processing of 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.

- **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 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**

  The personal data must be accurate, sufficient and, where necessary, kept up to date in accordance to the purposes of data processing. The data operator must take all necessary measures (or procure for taking the measures) required 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 of personal data, unless the specific term of storage or retention of personal data is set forth by 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.

- **Division of databases of personal data**

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

4 Rights of Data Subjects

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

- **Access to data**

  An individual (data subject) 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 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 of 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 also request the data operator to block the personal data, unless it is not prohibited by law. Furthermore, the data subject is entitled to request the data operator to delete his/her personal data if such data is 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 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.

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

  It is prohibited to take decisions that involve legal consequences for the 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 written consent for this and in other cases it has been providedfor by the federal laws.

- **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.

5 Formalities for Personal Data Processing

5.1 Is registration or notification to the relevant data protection regulatory authority(ies) required for processing of personal data?

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

Under the Personal Data Act, every data operator that is involved in the processing of any categories of personal data in the territory of Russia, and who uses a personal data information system or personal data database is obliged 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 other rules of Russian laws regarding data protection if they process personal data of citizens of the Russian Federation. 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.

5.3 Are there any exemptions to the registration/notification requirement?

The data operator is exempt from the obligation to notify *Roskomnadzor* in the cases provided for by the Personal Data Act, in particular, on processingof 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 is 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) related 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;
(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 the 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.

5.4 What information must be included in the notification?

The following information must be included in the notification:

- the name and address of the data operator;
- the purpose of personal data processing;
- the categories of personal data;
- the categories of data subjects whose data is being processed;
- the legal grounds for processing of personal data;
- the list of actions towards personal data;
- the description of methods of personal data processing;
- the description of the information systems and the security measures (including encryption) being taken for personal data protection;
- 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 the cross-border data transfer of 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 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.

5.6 What are the sanctions for failure to register/notify the regulatory authority?

A failure to submit to *Roskomnadzor* a notification on processing of personal data for the registration in the register of data operators may result in an administrative fine of up to RUB 5,000 on a legal entity. Also, the processing of personal data without

the notification of *Roskomnadzor* where such notification is required under the Personal Data Act will result in an administrative fine of up to RUB 10,000 for a legal entity.

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

Registration in the register of data operators is carried out on the 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.

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. The main advantage of voluntarily appointing the 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. Another advantage is that the Data Protection Officer will be directly in charge with dealing with data subjects' applications or requests.

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 Are there 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 should be an 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.

6.4 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.

6.5 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 CCTV and Employee Monitoring

7.1 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 regulated under the internal regulations (policies); (2) unless it is provided in the employment agreement with each employee, it should be communicated to the respective employees by way of advance notice (and against the employees' signatures, if CCTV is being installed in the premises of the employer for the first time, since it is deemed changing of the terms of employment); and (3) employees have given their consent to the use of their images and video surveillance recordings in writing (according to Art. 9 p. 4 of the Personal Data Act). According to the clarifications of *Roskomnadzor*, the CCTV surveillance should be conducted only for specific purposes defined in the respective internal regulations (policies).

7.2 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, social media monitoring and audio-listening. 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).

7.3 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 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 CCTV cameras are not hidden (i.e. there are placards notifying on such surveillance) and the materials of the surveillance will not be further made public.

7.4 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).

7.5 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 from *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).

8 Restrictions on International Data Transfers

8.1 Are there any restrictions on the transfer of personal data abroad?

Before transferring personal data of Russian nationals to other countries, every data operator must ensure that the rights and interests of the respective data subject are fully protected in the "adequate manner" in the respective jurisdiction. The jurisdictions which provide "adequate protection" of the rights and interests of data subjects include: (a) all the countries that are signatories to the Strasbourg Convention; (b) the countries included in an official list adopted by *Roskomnadzor*, in particular, Australia, Argentina, Canada, Israel, United Mexican States, and New Zealand.

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 defense 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.

Furthermore, under the Personal Data Act, cross-border data transfer may be prohibited or restricted for the purposes of protection of the foundations of

constitutional system of the Russian Federation, morality, health, rights, and lawful interests of citizens, national defence and security.

8.2 Which 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 to is a party to the Strasbourg Convention or included in the list of countries adopted by *Roskomnadzor* that provides an "adequate protection". In the event the country (countries) to the territory of which the transfer of the personal data of Russian nationals is intended does (do) not provide an "adequate protection" of the rights and interests of data subjects and/or the goals of such transfer are not in line with the goals of the initial collection of the respective personal data, the data operators would obtain written consents from the respective data subjects for cross-border transfer and execute agreements on personal data processing with the third parties to whom the personal data is transferred. 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)?

It is not required to register with *Roskomnadzor* or to have approvals by the letter of cross-border transfer of personal data or entering into the agreements on personal data processing. 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 Marketing and Cookies

9.1 Are there any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message?

Distribution of marketing communications by telephone, email, or SMS text message without authorisation of recipients is 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 13.03.2006 ″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 mobile telephone communications operator, depending on whose initiative the messaging was effected. 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.

9.2 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: "*Rospotrebnadzo*r"), 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.

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

The use of personal data for marketing communications without prior authorisation may result in the administrative fine of up to RUB 10,000 on legal entities; violation of the requirements of the Federal Law ″On Advertising″ and the Federal Law "On Communication″ (e.g. unsolicited SMS text message) may involve an administrative fine in the amount of up to RUB 500,000 on legal entities. 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.

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

Russian laws on data protection, advertising and other laws do not contain the definition 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. Furthermore, *Roskomnadzor* in practice has started considering the data on visitors of Internet sites gathered by means of cookies as personal data of the respective data subjects processing of which requires their express consent and notification of *Roskomnadzor*.

9.5 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 fine and, if the respective communications involve violation of privacy and unlawful access to computer information, criminal sanctions.

10 Processing Data in the Cloud

10.1 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 the cloud computing agreement. In the event that the server is located outside the territory of Russia, before transferring personal data to the processor, the data operator is under an obligation to make sure that the server is located in a country which provides an adequate protection of personal data (please see question 8.1. above) and, in the event that it is located in a foreign country that does not provide that, the

data operator has to obtain a specific written consent of the customer to the 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.

10.2 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)?

A cloud computing agreement between a customer and a data operator providing cloud-based services should include, in particular, the list of personal data, the purposes of personal data usage and the means of their processing, provisions on the storage location related to personal data, 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, a cloud computing agreement should provide for the post-termination obligations of the data operator in connection with cease of processing of the personal data and erasure thereof. Cloud computing agreements are currently not subject for approval by or registration with *Roskomnadzor*.

11 Big Data and Analytics

11.1 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)?

Although Russian data protection laws do not prohibit the utilisation of big data and analytics in general, according to Art. 16 of the Personal Data Act, any decisions or solutions should not be taken 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 or other video monitoring, the requirements described in question 7.1 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, dissemination. In practice, however, the above-mentioned general rules are rarely applied in the course of utilisation of big data and analytics.

In 2017 a working group for Internet development matters under the administration of the President of the Russian Federation started developing a draft federal law regulating usage of Big Data that will provide, in particular,for the common standards for storage and collection of Big Data and unified user agreement for data usage for all the companies operating in Russian segment of Internet.
The Fund for Development of Internet Initiatives is also preparing its alternative draft federal law on Big Data.

12 Data Security and Data Breach

12.1 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 obligation of a data operator to take or provide for taking necessary legal, organisational and technical measures in the course of processing of personal data in order to protect thereof from unlawful or accidental access, destruction, modification, blocking, copying, provision, or distribution as well as from any other unauthorised actions with regard to the personal data.
Such measures include, in particular:
(1) the appointment of a Data Protection Officer;
(2) the 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) the implementation of the legal, organisational and technical security measures provided for the applicable legislation;
(4) carrying out an internal control and/or audit for the data processing compliance with the data protection laws and data operator's policy/regulations/local acts;
(5) the 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) the 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.
The requirements to 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 01.11.2012 No. 1119 and other applicable regulatory acts.
Security measures to be taken by the data operator include, in particular:
(1) the determination of security threats in the course of processing of personal data in relevant information systems;
(2) the provision of the appropriate level of protection of processing of personal data in relevant information systems in accordance with the requirements set forth by the Government of the Russian Federation;
(3) the application of different duly certified means of protection of personal data (including, encryption);
(4) the evaluation of efficiency of security measures (prior to putting into operation of the information systems);
(5) the recording of computer media containing personal data;

(6) the revealing of unauthorised access to personal data;
(7) the retrieval of personal data that has been modified or destructed due to the unauthorised access;
(8) the 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;
(9) the control over the security measures with regard to personal data and level of protection of relevant information systems.
The List and content of organisational and technical measures for providing security of personal data in the course of processing thereof in information systems is approved by the order of the Federal Service for Technical and Export Control ("FSTEC") No. 21 dated 18.02.2013.
The data operator should evaluate the efficiency of the security measures for protection of personal data independently or by engaging companies or individual entrepreneurs possessing license for technical protection of information. FSTEC clarified that the respective evaluation may be conducted as well 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 of certain personal data (e.g., biometric data) would require the approval from FSTEC and/or Federal Security Service ("FSS"). Furthermore, in the event personal data is 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 No. 378 dated 10.07.2014.

12.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If no legal requirement exists, under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting?

Russian data protection laws do not provide for the obligation of data operators 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 (or provide for their destruction) it within six months.

13 Enforcement and Sanctions

13.1 Which enforcement powers the data protection authority(ies) possess?

Power	Administrative 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 in the amount of up to RUB 300 (for individuals); or (2) an administrative fine of up to RUB 500 (for officials); and (3) an administrative fine of up to RUB 5,000 (for legal entities). Failure to submit, or untimely submission of information (data) allowing to identify blogger or an owner of a news aggregator, by a provider of hosting shall involve: (1) an administrative fine in the amount of up to RUB 30,000 (for individuals); or (2) an administrative fine of up to RUB 300,000 (for legal entities).
Conducting planned and extra-planned 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.	
Requiring the data operator to amend, block or destroy false or illegally-obtained personal data.	Effective from 1 July 2017 a failure by the operator to comply within the time frame established by the legislation with the demand from *Roskomnadzor* to clarify the 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 an access to the information processed in a breach of the data protection laws effective from 25 March 2017 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.	Not applicable
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) a termination of the data breaches; (2) an award of damages and compensation of moral harm; and (3) a publication of court order.
Sending to FSTEC and FSS the information on the technical and organisational measures for personal data protection implemented by a data operator.	Not applicable
Filing a petition with the authorised body for the purposes of suspension or cancellation of the licence issued to the data operator.	Not applicable
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.	Not applicable
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 (other than in the cases specified above) shall involve the following administrative sanctions: (1) an administrative fine in the amount of up to RUB 500 (for individuals); or (2) an administrative fine of up to 2,000 or disqualification for a term of up to three years (for officials); or (3) an administrative fine of up to RUB 20,000 (for legal entities).

13.2 What is the data protection authority's approach to exercising its powers?

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 the state control and surveillance over personal data processing are established by the Government of the Russian Federation.

Generally, *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 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 2018 is available (in Russian) at https://rkn.gov.ru/plan-and-reports/.

In the event that breaches constituting crimes are committed (i.e., illegal gathering or dissemination of the information constituting 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.

Roskomnadzor, as part of the transition to a risk-based model of control and supervision, has reduced the number of inspections. In the communications sector, in 2017, compared to 2016, the number of scheduled inspections decreased by 7.3% (respectively, 368 and 397 scheduled inspections), in 2018 it will be reduced by an additional 18.3% - to 301.

A risk-based model of control and supervision activities, the transition to which is carried out in 2016 under the decision of the President and the Government of the Russian Federation, implies that planning of inspections is carried out depending on the category of risk or class of danger the activity of the audited persons and is aimed at reducing administrative pressure on business.

13.3 What are the administrative penalties for breaches of the personal data legislation?

Federal Law No.13-FZ dated 07.02.2017 amended Article 13.1. of the Administrative Code by establishing new administrative offense elements and a liability for violations of the legislation on personal data, in particular:

1) the 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 offense, 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 roubles; on legal entities - up to RUB 50,000;

2) the personal data processing without the written consent by the personal data subject, if these actions do not contain elements of a criminal offense, 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; on legal entities - up to RUB 75,000;
3) the 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 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 10,000 roubles; on legal entities - up to RUB 30,000.

The abovementioned amendments became effective from 1 July 2017

13.4 In which cases criminal sanctions apply for data security violations?

Under the Criminal Code of the Russian Federation unauthorised or illegal collection or distribution of data constituting private secret or family secret shall involve the following criminal sanctions: (1) a criminal fine of up to RUB 200,000 or a salary amount for the period of 18 months; or (2) a forced labour for the period of 360 hours; or (3) correctional works for the period of 12 months; or (4) compulsory works for the period of two years with or without disablement for the period of three years; or (5) an arrest for the period of four months; or (6) an imprisonment for the period of up to two years with disablement for a period of three years.

Using the 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 3 years; or (2) compulsory works for the period of three years; or (3) an imprisonment for the period of up to three years.

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 3 years; or (2) correctional works for the period of 12 months; or (3) a compulsory works for the period of two years; or (4) a restriction of freedom for the period of two years; or (5) an imprisonment for the period of up to two years.

13.5 What enforcement trends have emerged during the previous 12 months?

According to *Roskomnadzor* typical violations in the area of personal data revealed during inspections of personal data operators in 2017 included:

1) the submission to *Roskomnadzor* of a notice on the personal data processing containing incomplete and/or inaccurate information;

2) the failure by the operator to take the required and sufficient measures to perform the duties provided by the Personal Data Act and the regulatory legal acts adopted in accordance therewith;

3) the non-compliance of standard forms of documents, the information in which intends or allows the inclusion of personal data therein, with the statutory requirements;

4) the non-compliance by the operator with the requirements for informing persons engaged in the personal data processing without the use of automation equipment;

5) the non-compliance of the written consent of the personal data subject to the personal data processing to the statutory requirements;

6) the processing of personal data in cases not provided for in the Personal Data Act;

7) the lack of a place (places) with the operator for storing personal data (material media), a list of persons, who process personal data or have access thereto.

Starting from 1 September 2015 *Roskomnadzor* maintains the Register of violators of the rights of subjects of personal data which is available (in Russian) at http://pd.rkn.gov.ru/registerOffenders/viewregistry/ (the Register of infringers). The Internet addresses and domain names of Internet resources where personal data of Russian nationals is processed in violation of the requirements of the Personal Data Act and other applicable legislation are included in the Register of infringers upon a court decision and an access to such resources is restricted in the territory of Russia.

The first precedent for inclusion into the Register of infringers of a foreign social media and a limitation 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. 18-FZ dated 22.02.2017 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 it 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; 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 came into force on 25 March 2017.

****

The information above is provided with a view of laws and regulatory act effective as of March 2018 and does not constitute legal advice. It is prepared for the general information of our clients and other interested persons and it may include links to websites other than the GRATA International website. This information should not be acted upon in any specific situation without appropriate legal advice.

Contacts:

Yana Dianova

Director of Corporate and Commercial Law Department

GRATA International Law Firm

Tel: +7 495 660 11 84

Email: ydianova@gratanet.com

URL: www.gratanet.com

Yana Dianova was admitted to practise in Russia in 2002, and prior to joining GRATA International Law Firm she worked as in-house counsel for Nissan Motor Rus, as an Associate in the Tax and in Legal Department of Mazars and in the Moscow office of an 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), an MBA 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.