BACK TO DATAGUIDANCE

DataGuidance
GLOBAL GUIDANCE IN ONE

GUIDANCE NOTES

Russia - Data Protection Overview

Irina Anyukhina

10 March 2015

1. Data Protection Compliance is on the Agenda for Russian Regulatory Authorities

Until recently compliance with Russian personal data legislation was a secondary issue for many Russian companies. The reason for this was rather ineffective enforcement and, in particular, small administrative fines for violation of the relevant legislation.

However, the situation has changed dramatically for many companies. It seems that in the context of recent political events, data security and privacy issues have become a hot topic for Russian lawmakers and Government, which have recently adopted a set of bills in the sphere of personal data, unofficially named the 'antiterrorist package of bills'. This package, among other innovations, includes such widely debated amendments as data localisation requirements and new powers of the Russian data protection authority (Roskomnadzor) aimed at restricting access to information resources where personal data is processed contrary to Russian data protection laws. These amendments will come into force from 1 September 2015 and companies operating in Russia must take steps to become compliant with the new requirements, as well as with existing data protection requirements, by this date, especially in light of potential blocking of incompliant information resources by Roskomnadzor.

The situation is also getting more serious due to a recent draft bill suggesting an increase in the size of administrative fines for violation of personal data legislation. The new bill proposes a maximum level of administrative fine which can be imposed on a data operator for certain data protection breaches of RUB 300,000 (approximately £3,100). Just to make a comparison, the current maximum level of fines for these data protection breaches is RUB 50,000 (approximately £520) .

2. Basic Measures for Better Personal Data Protection Compliance

The primary peculiarity of the Russian personal data landscape is that it is quite formal and bureaucratic. Russian regulatory authorities, in the course of checks, pay a great deal of attention to the existence of documentation evidencing compliance with data protection requirements and their proper formalisation and registration with the Roskomnadzor.

Therefore, particular attention must be paid to the drafting of the required documentation and fulfilling certain formal requirements. It often appears that the legislation specifies a mandatory form and wording for data protection documentation.

Russian data protection laws provide for a number of requirements applicable to data operators and we consider in this article the most important requirements for companies operating in Russia.

First of all, companies operating in Russia are required to ensure that they have legitimate grounds for the processing of personal data. For this purpose companies should consider if any of the grounds provided by the Russian Federal Law on Personal Data ('the Data Protection Act') are applicable to the intended processing of data. If not, then properly formalised consent of data subjects will serve as the legitimate ground for processing of data or, if relevant, data can be processed on the ground of an agreement concluded with a data subject or to which data subject is a beneficiary or guarantor.

In this respect, companies should be aware that the specific wording and form of data subject consent can be prescribed by the Data Protection Act or other specific laws, such as the Labour Code in respect of employee personal data, and shall be strictly followed. Agreements, as grounds for processing of individuals' data, shall contain wording evidencing data subjects' awareness of the processing of their data conducted under such agreement and their consent with such processing.

In practice, the majority of companies operating in Russia transfer personal data to their parent entities abroad and engage data processors. Unless authorised by Russian laws or international treaties to which Russia is a party, such transfer is only possible if performed on the basis of an agreement concluded between a company transferring data (data operator) and the company receiving it for further processing (other data operator or data processor). This agreement must contain some mandatory terms specified by the Data Protection Act. Thus, data operators should carefully review their intragroup agreements and agreements concluded with contractors and ensure that they contain the provisions required by the Data Protection Act. Data operators must ensure that the consent of individuals for the transfer of their data to any third party is executed in the form and in accordance with the provisions prescribed by the Russian Data Protection Act and covers cross-border transfer if data is transferred outside Russia.

Russian data operators must appoint a person responsible for managing the processing of personal data. This person has a role very similar to the role of a data protection officer in

About The Authors

Irina Anyukhina is Head of Labour and Employment practice at ALRUD. She is an expert in data protection, real estate, intellectual property, media, brands and technology practices. Irina coordinates the work of ALRUD labour law practice in cooperation with the Ius Laboris Alliance. Irina is also an active member of the Global Advertising Lawyers Alliance (GALA), a network of independent law firms, which provides a worldwide resource to individuals and corporations interested in answers to questions and solutions to problems involving the complex legal issues affecting advertisers and marketers. She has handled matters related to international secondments, implementation of incentive systems, gross misconduct issues, and labour-related disputes. Irina also has an extensive experience in employment aspects of restructuring and white collar crimes. Irina is a frequent speaker at foreign and domestic conferences and contributes to legal periodicals on various areas of Labour law. Some of the latest publications include those for Getting the Deal Through, PLC, and Employment Law Review.

Irina is a member of International Bar Association (IBA), American Bar Association (ABA).

E-mail: IAnyukhina@alrud.com

Maria Ostashenko's advice on personal data protection includes general issues of privacy under the Russian law, confidentiality obligations and disclosures of information under applicable restrictions, as well as requirements applicable to data operators and persons involved in processing, structuring data flows within groups of companies among affiliates located in different jurisdictions, registration with the regulatory authorities (filing

notifications with the Russian Data Protection Authority (Roscomnadzor), reviewing privacy policies for e-commerce projects, conducting data protection compliance audit of company's activities in Russia, investigations of incidents with disclosure of information with limited access, representing the clients before Roscomnadzor, etc. Maria also possesses vast experience in structuring and implementation of complex projects, including complicated commercial transactions, regulatory advice, as well as provides ongoing advice on the client's business activities in Russia.

Maria is a member of the International Bar Association (the IBA).

E-mail: MOstashenko@alrud.com

Anastasia Petrova provides consultations to foreign and Russian clients on a wide range of Labour and Employment questions, participates in HR audits and due diligences of varying companies, successfully supports processes of staff transfer, hiring and dismissals, provides consultations on migration issues and supports process of legalisation of foreign nationals' residence and working activity in Russia. Anastasia advices on different corporate issues and successfully supports processes of emission of securities, transactions related to alienation of participatory interest in companies, incorporation of new companies and separate subdivisions in Russia, she advises clients on maintenance of confidentiality and data protection. Anastasia assists clients in their liaising with the state authorities, including in course of inspections of the State Labour Inspectorate. Before joining ALRUD team Anastasia worked for one of the leading Russian law firms for more than 2 years, and was a member of a work group specialised in projects on corporate and labour law, M&A, and real estate transactions.

E-mail: apetrova@alrud.com

the EU. Such a person shall be appointed by the written order of the authorised officer of the respective Russian legal entity.

Data operators in Russia are also obliged to notify Roskomnadzor that they process personal data. Such notification is required in general with respect to all types of processing. It must be prepared in strict accordance with the requirements set by the Data Protection Act and must be filed prior to the commencement of processing of personal data. If it is not filed prior to commencement of data processing, it must be filed as soon as possible.

As regards the data security issues, de facto implementation of efficient security measures by the company may be not sufficient to comply with Russian data security requirements. In case of inspection by state authorities, the availability of certain documents evidencing the application of security measures in the company, as required by Russian laws, might be crucial to avoid potential penalties.

The Data Protection Act provides for a minimum list of measures for ensuring personal data security. Among these measures companies must implement additional security measures in accordance with the Decree of the Russian Government Number 1119 (‘the Decree Number 1119’), outlining procedures for implementing security measures. To figure out what particular measures are deemed relevant for the company it is required to apply a threat modelling method. This method allows the identification and rating of threats which are likely to affect the information system of the company, and requires an IT audit of the company’s information system, as well as the elaboration of the so-called ’security threats model’. This model is required to be applied, internally documented within the company and approved by its authorised officer.

Based on the security threat model the company’s information system shall be classified in accordance with three types of security threats as prescribed by the Decree Number 1119. Depending on what particular type of security threat is applicable to the company’s information system, the required level of personal data security may be determined.

The Decree Number 1119 stipulates four levels of security of personal data processed in information systems. Each level determines the particular security measures which must be undertaken. In order to implement these measures the support of the company’s IT department and/or external IT organisations or experts competent in Russian information security regulations are required. Specialists implementing these measures must also be aware of the numerous state regulations, which provide for more detailed guidance on the implementation of data security measures, in particular the Acts issued by the Federal Security Service and the Federal Service for Technical and Export Control.

Under Russian law, each company must have an internal policy on the processing of personal data. This policy must outline all the data management procedures existing in the company. The policy is required to be in hardcopy and must be approved by a local authorised official.

Data operators are required to conduct an audit for compliance with Russian data protection requirements at least once every 3 years.

A data operator may fulfil all information security requirements itself or it may outsource this function to a specialised organisation having the required licences.

3. The Data Localisation Requirement and New Challenges

The data localisation requirement imposes an obligation on companies to ensure that the following types of processing of Russian nationals’ personal data are carried out in databases located in the territory of Russia at the moment of the data’s collection (including collection via the internet): collection, recording, systematization, accumulation, storage, adaptation or alteration, retrieval and extraction (‘the target types of processing’).

Thus, primary characteristics of the localisation requirement might be outlined as follows:

- The company carries out the target types of processing;
- Personal data being processed belongs to Russian nationals;
- The company must perform the obligation at a particular moment in time, namely in the course of collection of the personal data.

The amendment has raised debates among experts and representatives of the business community with respect to its precise meaning, giving rise to two possible interpretations..

The first interpretation is that the localisation requirement constitutes a ban on processing the personal data of Russian nationals anywhere outside the territory of Russia. This position also implies an absolute prohibition on conducting the target types of processing of personal data of Russian nationals in databases located abroad and excludes the possibility of processing copies of personal data for storage abroad. According to this interpretation personal data may be transferred and processed in databases abroad only by types of processing other than the target types and provided that all requirements on cross-border transfer are complied with.

The second interpretation is that the localisation requirement does not limit operators in transferring personal data for any further processing outside Russia if the requirements on cross-border transfers are complied with. Such interpretation allows copies of Russian nationals’ personal data to be stored abroad or after collection in databases in Russia their transfer and further processing in databases abroad (again if rules on cross-border transfer are complied with).

4. A Way to Comply with Data Localisation Requirements

At the moment, the second interpretation of the data localisation law is supported by the majority of businesses in Russia. Work groups within different business communities have

received many unofficial clarifications from Russian regulatory authorities. Most of these clarifications also support the second, optimistic, interpretation of the law.

Guided by the optimistic interpretation of the localisation law, companies having a legal presence in Russia should initially use databases located in Russia for the processing of Russian nationals' personal data and then can transfer the copies to or collect copies of this data in other jurisdictions. Along with this, rules on cross-border transfer of personal data must be complied with, and companies must take all necessary measures to comply with Russian rules on processing of personal data.

Implementation of the above scenario seems realistic, as the law does not require placing all IT infrastructure or servers in Russia. The law only requires that initial processing of personal data of Russian nationals is in databases located in Russia. Assuming that a database is any aggregated materials, organised in a way which allows their retrieval and processing by electronic computing equipment, compliance with localisation requirements can be achieved through the use of IT solutions.

There are some options with regard to the applicability of the localisation requirement to foreign-based websites. This is a topical issue for e-commerce businesses and social network and email service providers. There have been some unofficial clarifications by the representatives of state authorities confirming that the localisation requirement shall strictly cover the territory of Russia and does not have extraterritorial effect. This made some experts think that foreign-based websites might be exempted from the scope of the localisation requirement and it makes sense to re-register the website at a foreign internet registry to be out of the Russian internet domain. Nevertheless, such an approach seems to be inefficient if a website is targeted at Russian-based users. The criteria for targeting Russian-based users can be, for example, translating a website of a foreign company into Russian, having a '.ru' domain or offering the possibility of providing services to Russian customers.

The other important issue to take into account in order to comply with the localisation requirements is the identification of Russian nationals among other data subjects whose data is collected. A data operator must decide itself on the procedure for identifying Russian nationals. In our opinion the safest option would be to apply Russian data localisation requirements to all personal data collected in Russia.