BACK TO DATAGUIDANCE

DataGuidance GUIDANCE NOTES

Russia - Employment

Elena Kukushkina, Georgy Mzhavanadze and Nina Mogutova

18 May 2017

About The Authors

Elena Kukushkina is a Counsel and Coordinator of the Labor and Migration practice in the Moscow Office of Baker & McKenzie. She specialises in employment and immigration law issues.

In particular, Ms. Kukushkina has a wide experience of representing major Russian and international companies in multiple court disputes with former and current employees. She has also advised an American multinational technology and consulting corporation on a wide range of commercial, regulatory, privacy/data protection, encryption, corporate compliance, employment and corporate issues across Russia, Ukraine, Armenia, Azerbaijan and several Central Asian jurisdictions and advised Merck, Sharp & Dohme on Russian employment and migration issues related to its global merger with Schering Plough.

E-mail: elena.kukushkina@bakermckenzie.com

Georgy Mzhavanadze is an Associate in the Moscow office of Baker & McKenzie. He joined the Employment practice group as a Student in 2011 and was promoted to the position of Trainee Lawyer in 2013 and then to the position of Associate in 2014. Mr. Mzhavanadze is involved in litigation and pre-trial resolution of disputes with employees and provides advice on employee hires and terminations, corporate restructuring, staff redundancy, disciplinary enforcement, cooperation with trade unions and other employment-related issues. He also provides advice on personal data

1. Introduction

1.1 Key acts, regulations, guidelines and case law

- the Constitution of the Russian Federation as of 12 December 1993;
- the Federal Law of 27 July 2006 No. 152-FZ on Personal Data (**'the Personal Data Law'**), available in its most updated version in Russian here;
- the Labour Code of the Russian Federation of 30 December 2001 No. 197-FZ (**'the Labour Code'**);
- the Russian Code of Administrative Offences (**'the Administrative Offences Code'**);
- the Federal Law of 27 July 2006 No. 149-FZ on Information, Information Technologies and Information Protection, available in Russian here;

1.2 Other bylaws and regulations

- Decision of the Government of the Russian Federation of 4 March 2010 No. 125, available in Russian here;
- Decision of the Government of the Russian Federation of 1 November 2012 No. 1119, available in Russian here.

1.3 Key definitions

The Personal Data Law provides the following definitions:

- **Personal data** is any data related to a directly or indirectly identified or identifiable individual ('personal data subject'), including his/her first name, middle name and last name, the year, month, date and place of birth, marital and social status, welfare, education, profession, income, etc.
- **Personal data processing** is any action ie. operation, or aggregation of actions ie. operations with personal data, performed with or without computer equipment, including collection, recording, systematization, accumulation; storage; verification or updating and amending; extraction; use; transfer or dissemination or granting access; depersonalisation; blocking; deletion; and, destruction of personal data.
- **Operator** is a state body, municipal body, legal entity or an individual that, on its own or in cooperation with other person, organizes and/or performs processing of personal data and also determines the goals of personal data processing, content of personal data to be processed, and actions ie. operations performed with personal data.
- **Cross-border transfer** is a transfer of personal data to a foreign state body, foreign individual or foreign legal entity situated in the territory of a foreign state.

1.4 Regulators and supervisory authorities responsible for enforcing the regulations discussed

The Russian Federal Supervision Agency for Information Technologies and Communications (**'Roskomnadzor'**) is the primary data protection authority in Russia. Due to the latest political trends in Russia, the Roskomnadzor has become very active with an increasingly large scale of authority. The State Labour Inspectorate also has the authority to control employers' compliance with data protection requirements prescribed by the Russian Labour Code. In practice, however, Labour Inspectors rarely monitor the personal data issues over their audits, and compliance with the personal data legislation requirements is generally monitored by the Roskomnadzor.

2. Recruitment and selection

2.1 Legal framework

The key acts regulating the recruitment and selection process are the Constitution of the Russian Federation, the Labour Code, Law on the Employment of the Population of the Russian Federation and the Personal Data Law. Liability for failing to comply with the relevant obligations is provided by the Administrative Offences Code or by the Russian Criminal Code.

2.2 Advertising a position

Apart from the general requirement of non-discrimination, Russian legislation does not set any specific requirements for job advertisements.

Generally, when offering vacant positions, an employer shall indicate the main terms of employment, ie. job title, work place, main employment duties, etc., as well as the qualification requirements applicable to these positions. These requirements may not contain requirements which are not connected with the professional skills of the individual concerned. Requirements for a particular gender, race, nationality, language, social origin, age, property status, place of residence, religious beliefs and affiliations with social

protection and other matters.

Mr. Mzhavanadze has also successfully represented major IT companies in a number of disputes with their former employees and has advised a wide range of IT, pharmaceutical and other companies with regards to Russian data localisation provisions.

E-mail:
georgy.mzhavanadze@bakermckenzie.com

Nina Mogutova is a Trainee Lawyer in the Labor and Migration practice of Baker McKenzie's Moscow Office. She joined the Employment practice group as a Student in 2015 and was promoted to the position of Trainee Lawyer in 2016.

Ms. Mogutova specialises in employment and immigration law issues. Ms. Mogutova provides advice on employee hires and terminations, staff redundancy, employment benefits, disciplinary enforcement, cooperation with trade unions, labor safety, and other employment-related issues. Ms. Mogutova also advises on personal data-related issues, including data protection and processing and international data transfers.

E-mail:
nina.mogutova@bakermckenzie.com

associations, ie. political parties, trade unions, charity organisations, etc., are deemed to be discriminatory. Including discriminatory restrictions into job advertisements constitutes an administrative offence.

2.3 Obligations of the employer to protect candidate's right to privacy during interview process

Under the general requirements envisaged by Article 7 of the Personal Data Law, operators and other persons having access to personal data are forbidden from disclosing to third parties or disseminating personal data without the consent of personal data subjects, unless otherwise provided by law.

In addition, the processing the personal data of job applicants implies their written consent to the processing of their personal data during the potential employer's process of making a decision on hiring or refusing to hire the candidate. The consent may be confirmed in a separate document signed by the applicant. If a job applicant applies for employment through the special online system, 'click-through' consents will be sufficient for complying with the consent requirement.

At the same time, under the clarifications of the Roskomnadzor, a candidate's consent is not required if:

- the candidate places his/her CV on the internet so that it may be accessible by the general public;
- the candidate acts through a recruitment agency with which he/she has concluded a relevant agreement.

Nevertheless, if a Russian employer, including Russian subsidiaries of foreign companies, transfers candidate's personal data to a country that does not provide adequate protection of personal data, including the USA, a specific written consent will be required. For more information, see below.

2.4 Employer's right to ask questions/request references

The Labour Code envisages a list of documents that a newly hired employee has to provide to an employer upon hiring, in particular:

- Passport;
- Labour book;
- Insurance certificate of mandatory pension insurance;
- Military registration documents, for persons liable for military service or draft to military service;
- Document proving education and qualification or availability of special knowledge, if the employee is hired for work requiring special knowledge or special training;
- Reference note in respect of the presence, or absence, of a previous conviction or criminal prosecution. This is required for some positions, as persons who have or had a conviction or who were subject or are subject to criminal prosecution may not be admitted to particular job positions, eg. teaching employees, chief accountants in some companies, civil servants, heads of credit organisations, etc.;
- Other documents required by law.

It is prohibited for an employer to request a newly-hired employee to provide any documents except those specified in the legislation. However, an employer may ask a candidate to provide additional information and documents that may be relevant to the candidate's future employment and related to their qualifications and business acumen.

Pre-hire background checks are not required by law. However, in practice, employers often conduct them with respect to candidates subject to obtaining a candidate's prior written consent.

2.4.1 Criminal checks

Criminal checks are only allowed in certain cases set out in statute, provided that such information is necessary to consider whether a candidate may perform particular duties or work in a particular job position. This will only be the case for positions with access to sensitive information and valuables, for teachers and in some other specific cases. There is a database indicating all criminal convictions, but not arrests, which is maintained by the Ministry of the Interior. Note, however, that only a candidate themself can obtain a copy of such a record.

In Russia, employers may check if potential employees can occupy certain job positions. There is database available here https://service.nalog.ru/disqualified.do , which indicates all persons who are prohibited from holding particular jobs, managerial, medical, etc., as a result of an administrative disqualification. This check does not require the candidate's consent.

2.4.2 Reference checks

Pursuant to applicable legislation, these checks may only be carried out with a candidate's prior consent.

2.4.3 Medical checks

Russian labour legislation provides for mandatory medical checks prior to entering an employment contract and periodic medical checks for certain categories of employees. The list of such categories is approved by the Order of the Ministry of Health. It includes minor employees, employees engaged in dangerous or harmful activities, employees engaged in teaching, etc.

2.4.4 Other issues

If an employer intends to conduct a background check, it should not make an offer of

employment, enter into an employment agreement or admit a candidate to work, before the background check is completed. Otherwise, if the results of the background check are not satisfactory, a company will not be able to dismiss an employee on this ground. In addition, an employer generally cannot refuse to employ a candidate merely due to unsatisfactory background check results unless such unsatisfactory results prove a candidate's unsuitability to a particular job position, eg. due to their low qualification or work experience.

2.5 Candidate's obligation to reveal information

The candidate is not obliged to provide any information not related to their recruitment, as this is not required under the Labour Code.

2.6 Retention of information

The data of candidates may be retained while there are legitimate purposes for its processing. In particular, a candidate's personal data may be stored during the period of consideration of their job application. In the case of a refusal to hire a candidate, a candidate's data must be destroyed within 30 days, except for certain cases related to the personal data of civil servants.

In addition, employers may need to store candidate's data for the purposes of administration of a personnel reserve. According to clarifications from the Roskomnadzor, processing the personal data of candidates included in the personnel reserve shall be performed, subject to their consent. Moreover, candidates must be acquainted with the conditions of administration of the personnel reserve, the term of their personal data retention and the order of their expulsion from the reserve.

3. Employment records

3.1 Processing of employment records

A general requirement envisaged by the Labour Code sets out that while determining the extent of the employees' personal data to be processed, the employer must follow the Russian Constitution, the Labour Code and other federal laws. In addition, under the Labour Code, an employer may not receive and process special categories of employee's personal data, except if otherwise provided by law.

Generally, an employer may process employees' personal data without their consent. However, the employees' written consent is required for transferring the employees' personal data to any third parties to another entity within one group of companies, banks, insurance companies, HR and accounting providers, etc. The requirements to such consent are described in Section 3.2. below. The employee\s consent is not required for transfer of personal data to the Russian Social Insurance Fund and the Russian Pension Fund, and in other cases prescribed by law.

In addition, while processing the employees' data, an employer must comply with the following requirements:

- An employee's personal data may be processed exclusively for the purposes of securing compliance with the laws and other regulatory legal acts, assisting professional development and advancement, ensuring personal security of the employees, monitoring their workload and workmanship, and ensuring the safety of the operator's property;
- All of an employee's personal data should be received from the employee. If the employee's personal data can only be obtained from a third party, the employee concerned shall be notified accordingly beforehand, and shall be required to give the operator his/her written consent thereto;
- The operator has the right to receive and process data about the employee's membership of public associations and their trade union activity to the extent permitted by the legislation of the Russian Federation;
- Whenever decisions are made that affect the employee's interests, the operator shall not rely on personal data received exclusively as a result of their automated processing or exclusively by electronic means of data transmission;
- The operator shall protect the employees' personal data from improper and unauthorized use or loss at the operator's expense and in accordance with the procedures laid down by Russian legislation, etc.

3.2 Notification to the employee

As described above, in certain cases, the employers should obtain employees' consent to their personal data processing.

Certain rules apply if consent is to be given in writing eg. for the cross-border transfer of personal data or for its transfer to a third party. Written consent should include the full name of the personal data subject or its representative, if specially authorised by the data subject; passport, or other ID information; the name and address of the operator or of the person processing personal data in the name of the operator, the purpose of data processing; the list of personal data to which processing consent is granted; the list of actions which the operator can perform with respect to personal data; a description of data processing methods; the term of the consent and the procedure for recalling consent.

The consent must be in Russian or in a bilingual form in Russian, English or any other language, in addition to Russian, and should be signed by an employee with a hard-copy signature.

3.3. Retention of employment records

Russian law only sets out specific retention requirements to documentation in hard copies, and the specific retention period depends on the type of document. For instance, the most important HR documents, eg. employment agreements and internal HR orders, should be

kept for 75 years from the date of their creation, and employees' payroll documents should be kept for five years.

Russian law does not contain special retention requirements for personal data and documents stored electronically. Under the Personal Data Law, personal data contained in electronic databases must be retained for no longer than is necessary for the purposes of its processing. The personal data must then be destroyed or depersonalised once these purposes have been fulfilled.

In addition, according to data localisation law, effective as of 1 September 2015, Russian and foreign companies that collect the personal data of Russian nationals must ensure that the databases used to record, systemise, accumulate, store, amend, update and retrieve it are located in Russia. The law applies to personal data collected both online and offline, whether from employees, customers or third-party individuals, provided that the personal data subjects are Russian nationals.

4. Information about workers' health

4.1 General rules on processing of workers' health information and exceptions

The Personal Data Law establishes special protection for special categories of personal data, which include those related to the individual's race, nationality, political views, religious or philosophical beliefs, intimate life and health.

Generally, employers may need to process information on the employee's state of health for making a decision on whether the personal data subject will be able to perform their specific labour function.

4.2 Conditions for legitimate processing and consent issues

The Personal Data Law provides for a very limited number of grounds on the basis of which the special personal data, including information of employees' health, may be processed.

The most general ground is the prior written consent of the personal data subject to such processing, issued in accordance with the specific requirements of the Personal Data Law, as discussed above in Section 3.2.

No consent is required when information about workers' health is processed in accordance with statutory requirements. Such cases include mandatory medical checks, formalisation of a sick leave or maternity leave, payment of medical allowances, etc.

4.3 Employees' rights – to information, access, rectification, etc.

Employees have the following rights with respect to their personal data:

- to receive full information regarding their personal data and the processing thereof;
- to have access to their personal data free of charge, including the right to receive a copy of any record containing the personal data, except where Russian legislation provides otherwise;
- to request the removal or correction of incorrect or incomplete personal data as well as data processed in breach of the requirements of the Russian Federation legislation;
- to claim in court against any illegal actions from the employer or its failure to act in the processing and protection of their personal data, etc.

5. Employees' data transfers

5.1 Legal grounds

Under Russian law, data transfers by an employer to third parties, including affiliated companies, must be:

- directly envisaged by an employee's consent, or have other lawful grounds, such as performing a contract with the data subject;
- performed on the basis of a separate data transfer agreement or contractual clause that must (i) reasonably limit the data processing by the recipient, (ii) impose a duty of confidentiality and (iii) provide for the organizational and technical data protection measures to be taken by the data recipient;
- and, consistent with the purposes of personal data processing as such purposes were declared in the course of the initial collection of the data.

The rules regulating cross-border transfer of personal data are established in Article 12 of the Personal Data Law. The Personal Data Law distinguishes two types of the countries where personal data are transferred to:

1. countries that provide adequate protection of personal data. These are the countries that are member states to the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The Roskomnadzor may recognise other countries as providing adequate protection of personal data;
2. countries that do not provide adequate protection of personal data. These are all other countries not included in the convention in (i) above, including the USA.

Normally, a prior written consent of an employee, issued in accordance with the specific statutory requirements set forth in the Personal Data Law, is required for a cross-border transfer of personal data to any third parties, including those based in foreign countries.

The written consent requirement should not apply if personal data subjects transfer their personal data abroad themselves, via telephone, email or other communication means.

5.2 Mechanisms for the transfers of data, BCRs, CBPR, SCCs etc.

The main mechanism to transfer personal data under Russian law is a data transfer agreement.

BCRs could be applicable by Russian entities, subject to certain conditions. In particular, an addendum may be required to make the BCRs compliant with Russian legal rules if it contains any provisions that are not in line with Russian mandatory requirements.

Mechanisms such as CBPR and SCCs are not applicable to Russian entities.

5.3 Sensitive data

As described above, the Personal Data Law specifically establishes special categories of personal data ie. sensitive data, as well as biometric personal data for special protection, see Section 4.1. above. Transfer of sensitive data is allowed based on the written consent of a personal data subject, or other legal grounds, see Section 4.2. above, and on the grounds of a data transfer agreement.

5.4 Information provision requirements and employer's obligations with respect to employees' personal data transfer

As outlined in Section 4.3, employees have a right to receive full information regarding their personal data and its processing, including a personal data transfer. In particular, employees have a right to obtain the information on the legal basis of personal data processing; purposes and methods of personal data processing applied by the operator; the list of processed personal data; information about persons, having access to personal data or who may be given such access under the agreement with an operator, etc.

In addition, the Labour Code provides for requirements with regard to employees' personal data transfer. In particular, employers are obliged:

- not to provide employee personal data to a third party without the written consent of the employee, except for when it is necessary to prevent a threat to the employee's life or health, as well as in other cases envisaged by the Labour Code or other laws;
- not to disclose the employee's personal data for any commercial purposes whatsoever without the employee's prior written consent;
- to serve a warning on any party or parties receiving the employee's personal data from the operator to the effect that such data may only be used for the purposes for which it has been communicated thereto;
- to transfer employee personal data within one organisation or one individual entrepreneur in accordance with the local normative act, which must be made known to the employee against a signature, etc.

5.5 Notification requirements

The Personal Data Law establishes a mandatory requirement for operators to notify Roskomnadzor of the operator's personal data processing activities, which must be submitted to Roskomnadzor before the actual start of personal data processing.

Russian law establishes several exemptions from the notification requirement, in accordance with which an operator may not be required to notify Roskomnadzor if the personal data: (i) is processed in accordance with labour law of the Russian Federation; (ii) was received by an operator in connection with execution by an operator of a contract, a party to which is a personal data subject, however only if personal data is not distributed, and are not provided to, third parties without a personal data subject's consent and is used by an operator exclusively for performance of that agreement and execution of agreements with a personal data subject; (iii) was made public by a personal data subject; (iv) personal data includes only family names, first names and patronymics of a personal data subject; and in some other specific cases.

Since Russian labour law does not directly require data sharing between companies of one group, in practice, processing of personal data by the subsidiaries of multinational companies, operating in Russia, does not fall under the above exemptions.

The notification should contain the company name, address of the operator, the purpose of personal data processing, categories of personal data, legal grounds for personal data processing, information on providing security of personal data in accordance with the requirements for personal data protection established by Russian Government, etc. A standard form of notification can be found on the official website of Roskomnadzor here http://rsoc.ru. An English version of the website is available here http://eng.rkn.gov.ru/.

6. Sanctions & penalties

6.1 Criminal, administrative and civil liabilities

The illegal collection and processing of personal data may result in civil, administrative and even criminal liability. The burden of proof that the persons consented to the processing of their personal data lies with the recipient of the information.

6.1.1 Civil liability

An individual may claim recovery of damages caused from the operator, including direct damage, lost profit and moral suffering. However, it will be the claimant's burden to prove the facts of breach, the damages and the causal link between them. In practice, it would be quite difficult for an individual to meet this burden of proof. As far as moral suffering is concerned, Russian court practice is not very supportive of compensation for moral suffering.

6.1.2 Administrative liability

Pursuant to Article 13.11 of the Administrative Offenses Code, for violating the procedure for acquisition, storage, use or dissemination of personal data, officers of an operator ie. a company may be subject to a fine in the amount up to RUB 1,000 (approximately €16) and/or the company may be subject to a fine of up to RUB 10,000 (approximately €160). On 27 January 2017, the Russian Parliament adopted a federal law increasing the liability of legal entities and their officers for violating legislation on personal data. The new law does not entail any new violation types or punishments, but differentiates liability depending on the type of violation eg. processing personal data without the consent of the personal data

subject, the operator's failure to ensure the safety of personal data if it has led to unlawful access to personal data, etc. The fines will be different depending on the violation and will amount to a maximum of RUB 75,000 (approximately €1170) for a company and RUB 20,000 (approximately €310) for officers. The law will enter into force on 1 July 2017.

In addition, the Administrative Offenses Code provides for liability for other violations of personal data legislation eg. using uncertified information systems, failing to notify the Roskomnadzor of the personal data processing, etc.

If a responsible officer or a CEO is a foreign national, the imposition of an administrative fine may jeopardise their Russian work permit and visa status.

6.1.3 Criminal liability

The illegal collection or dissemination of information on an individual's private life, without the individual's consent and committed with the use of official capacity, may be subject to (i) a fine on the relevant operator's officer in the amount of up to RUB 300,000 (approximately €4700); (ii) a fine in the amount of his/her salary or other income for the period up to two years; (iii) prohibition from holding certain positions for a term from two to five years; (iv) compulsory labour for the term up to four years with or without prohibition from holding certain positions for a term of up to five years; (v) arrest for up to six months; or (vi) imprisonment for up to four years with or without prohibition from holding certain positions for a term of up to five years. Only guilty individuals are subject to criminal liability under Russian law, and this crime requires proving direct intent on the part of a guilty person.

6.2 Enforcement from regulatory authorities

The Roskomnadzor has a wide range of powers with respect to operators violating personal data legislation. In particular, the Roskomnadzor is authorised to: (i) conduct compliance audits and inspections; (ii) impose administrative sanctions for violating data protections laws; (iii) initiate inclusion of a website violating personal data requirements into the special register of prohibited information (access to such websites via Russian providers shall be blocked); (iv) take measures on suspension or termination of personal data processing conducted in violation of Russian legislation on personal data; (v) request the operator to correct, block or destroy inaccurate data or data received by illegal means; and (vi) file court claims for the protection of the general public, etc.