

# Personal Data Protection

## COUNTRY FEATURES



## RUSSIA: New Personal Data Protection Regulations Due in July 2011

by Pavel Sadovsky, PhD, Senior Associate and Head of the IP/TMT Group in Russia at *Magisters*

**Russia prides itself in having adopted data protection laws that equal protection standards in the *European Union* states. Thus, access and processing of personal information in Russia are governed by the norms in the Federal law "On Personal Data" dated 27 July 2006 and partially by some other laws. The Russian data protection laws are relatively new, and information protection mechanisms are yet to be worked out in practice or receive adequate interpretation by the courts. Nevertheless, despite the novelty of the legal regime, most of its requirements are clear and yield straightforward legal guidance for companies that wish to be data protection compliant.**

When it comes to data preservation and access, a company must undertake technical and organizational measures to prevent unauthorized access to personal data. It was expected that the amendments to the Law on Personal Data ►

### IN THIS ISSUE

#### COUNTRY FEATURES

##### RUSSIA

New personal data protection regulations due in July 2011

##### UKRAINE

Encryption systems: licenses, permits and certification requirements

##### BELARUS

Recent developments in personal data protection

##### KAZAKHSTAN

Personal data are regulated by a number of laws

##### GEORGIA

Still unclear on data protection

#### DP\_NEWS@CIS

##### RUSSIA

Publication of personal data of debtors by bailiffs is now permitted

##### UKRAINE

Law on protection of personal data came into force

##### UKRAINE

Banks obliged to use local servers

with regard to IT systems compliance (information systems adjustment) would come into force since January 1, 2011<sup>1</sup>.

On December 28, 2010 the Russian President signed the bill under which the term of information systems adjustment is postponed until July 1, 2011.

What does personal data protection compliance mean with regard to IT systems? Under Russian law, software that is used to protect personal data is subject to certification by the State's *Federal Service for Technological and Export Control (FSTEC)*. This certification is necessary even if the software has a different primary function (e.g. management of personal data), but involves a security module or tool. *FSTEC* keeps a register of software and other IT products certified for the purpose of personal data and other information protection. Even if software is already included in the register, accelerated certification process is required for each copy of this software to ensure that this copy is identical to the software on the register. ■



President Medvedev's recent bill has prolonged grace period till mid-2011.

## UKRAINE: Encryption Systems: Licenses, Permits and Certification Requirements



by **Taras Kyslyy**, Senior Associate and Head of IP/TMT Group in Ukraine at *Magisters, DataGuidance.com* CIS Expert Panel member

**As in today's world most data is transferred via electronic communication channels, a considerable part**

**of this data is of confidential nature and its senders and recipients are keen to secure its confidentiality. This is achieved by various complex measures that usually include the use of encryption systems.**

In the world there are different approaches as to regulation of data encryption activities. Ukraine with its strong post-Soviet tradition of total state control over any secrecy issues has quite strict regulations as to encryption systems.

Those who would like to proceed with the encryption services may face requirements as to:

- import permits;
- certification; and
- licensing.

### Import permit for encryption equipment and software

The Law of Ukraine *On State Control over International Transfers of Military and Dual-Use Goods* of February 20, 2003 (hereinafter – Import Control Law) establishes import control requirements that apply to the relevant equipment and software. Provisions of the Import Control Law require obtaining a special permit or conclusion of the relevant state body for an international transfer of dual-use goods. The term<sup>2</sup> “dual-use goods”, includes “...specific types of goods, equipment, materials, software..., as well as works and services related thereto...”.

Article 9 of the Import Control Law refers to the list of dual-use goods subject to import control procedures (hereinafter – List of Dual-Use Goods) that is approved by the Resolution of the Cabinet of Ministers of Ukraine No. 86 of January 28, 2004 (hereinafter – Import Control Resolution). Under provisions of the Import Control Resolution the equipment for encryption protection of the data and software designed to be used in or to perform the functions of such equipment is treated as dual-use goods and its international transfer is subject to import control procedures.

To obtain an import permit one should apply to the *State Export Control Service of Ukraine*. There are ►

<sup>1</sup> In a clarification to the draft, it is stated that adjustment of information systems in accordance with the Law will demand expenses from businesses and public bodies which were not planned and are difficult to accomplish during the financial crisis. So, it was decided to give to Russian companies more time in order to make all necessary arrangements (certification, etc.) and to provide full compliance with the personal data regulations. Moreover, the amendments excluded the obligatory demand of using cryptographic means of data security.

<sup>2</sup> defined in Article 1 of the Export Control Law of Ukraine.

relevant exceptions to the requirement to obtain import permit for encryption software and equipment all of which should be met and which are as follows:

- software/equipment's availability in retail trade;
- protection from easy change of encryption functions by users;
- software/equipment allows its installation by a user without further significant support by a distributor;
- detailed information about software/equipment is accessible upon request and can be submitted to respective authorized organization in the country of exporter for an inspection of the above requirements.

In any case, the decision on whether particular software/equipment qualifies the above exception is taken by the *State Export Control Service*.

### Certification of Encryption Equipment and Software

Ukrainian law provides for obligatory certification of encryption systems and tools (including software) that are used for protection of confidential information. Certification is carried out by companies authorized by the *State Service for Special Communication and Information Protection of Ukraine* as well as by the *State Committee of Ukraine on the Issues of Technical Regulation and Consumer Policy*. A general list of the authorized companies is available on the State Committee's website. In practice the only authorized organization to proceed with the certification is the *State Scientific-Research Institute of Special Communication and Information Protection of the Administration of the State Service for Special Communication and Information Protection of Ukraine*. The subject matter of certification expertise is compliance of the encryption systems and tools to the statutory acts, test of its protection and technological level.



A lot depends on the officials in charge of respective state authorities

### Business License for Encryption Services

The Licensing Law sets out the general terms for business activities involving encryption services. The Licensing Law requires a business license to perform specific operations with encryption systems in Ukraine. Such operations include: inter alia, import, sale, operation, use, development, production, testing of encryption systems as well as provision of encryption services. Ukrainian law specifies operations with encryption systems that require a business license, which are:

- import and export of encryption systems and tools;
- use and operation of encryption systems and tools;
- provision of services in relation to encryption systems and tools;
- sale of encryption systems and tools;
- development of encryption systems and tools, including software tools;
- production of encryption systems and tools, including software tools;
- certification, testing and expertise of encryption systems and tools; and
- theme search of encryption systems and tools.

From the above one may see the strict requirements of the Ukrainian law in regard to encryption systems. However, the laws provide for quite general and vague definitions, which allow regulating authorities to decide at their discretion whether particular equipment or activity is indeed subject to encryption regulations, or not. Thus a lot depends on the officials in charge of respective state authorities, which are rapidly changing these days in Ukraine. ■

## BELARUS: Recent Developments in Personal Data Protection



by **Dennis Turovets**, LL.M., Managing Partner (Minsk) at *Magisters* and **Irina Butko**, Associate at *Magisters*

**Although the importance of personal data protection has been raised in Belarus a number of times already, there is still a lack of specific regulation in this area.**

Regulation of personal data protection was introduced by the Law *On Information, Informatization, and Protection of Information* of November 10, 2008 (hereinafter – the “Law”). However, the Law does not provide for a definition of personal data. The legal definition of personal data shall be fixed in the Law On Population Register which comes into effect in July 2011. The Law on Population Register establishes a national population register, which is an automatic system containing personal data of the population of Belarus. The information of the Register will be accessible by authorized bodies according to the sphere of their activity and to individuals as well as their representatives and third parties provided with written consent from the individual - with regard to information about the individual in question.

Currently, the Law establishes a non-exhaustive list of data which is considered to be personal data: family privacy, privacy of telephone calls, mail and other types of messages, information about the state of health. According to the Law, personal data is defined as information of restricted access. As such, personal data is subject to protection by the data holder. The collection, storage, processing and use of personal data are allowed only upon consent of the owner. The order of collection, transfer, processing, accumulation, storage and distribution of personal data is established by law.

According to the Decision of the Council of Ministers “*On Certain Issues of Information Protection*” No. 675 of May 26, 2009 special data protection systems must be developed and certified by the authorized organizations to ensure security of information of restricted access and information containing state secrets stored in information systems.

Data protection systems may be developed only using the certified means of protection and only by organizations authorized by the special *Center of the President*

*of the Republic of Belarus* with subsequent certification by authorized organizations.

Although development of data protection systems is required by law with regard to information systems accumulating all kinds of information of restricted access, including personal data information, in practice the development of such systems has been launched only with regard to state information systems used for accumulation of information containing state secrets of the Republic of Belarus. The main reason for this is the absence of an explicit legal definition of personal data. It is likely that after the Law on Population Register enters into force, development of the respective data protection systems shall be required with regard to information systems accumulating personal data as well.

Specific protection is granted in the Republic of Belarus to personal data attributed to the “privacy of private life”. The right to the privacy of private life is secured by the Constitution of the Republic of Belarus (Art. 28), and its protection is required inter alia by the Civil Code of the Republic of Belarus (Art. 151) and Criminal Code of the Republic of Belarus (Art. 179).

A detailed definition of “privacy of private life” is provided by the Regulations on the Regime of Access to Documents Containing Information Relating to the Secret of Personal Life of Natural Persons, approved by the Order of the Committee of Achieves and Record Keeping No. 21 of July 3, 1996. According to the Regulations, “privacy of private life” includes data on individuals, if use of such data without the consent of the individual would damage their moral state or property interests, namely, the data on health, family, intimate relations; circumstances of birth, adoption, divorce; personal habits and preferences; personal correspondence; information from diaries, telephone, telegraph, video, audio and other sources; material position, sources of income and other types of information. The list is not exhaustive. Unauthorized disclosure of such information is illegal. ■



## KAZAKHSTAN: Personal Data are Regulated by a Number of Laws



by Viktoriya Alzhanova, Associate at *Magisters*

**In Kazakhstan, the transfer and protection of data is not currently regulated by any specific law, though data protection provisions are provided in various legislative acts.**

*The Constitution* of Kazakhstan sets forth the fundamental rights of its citizens. Under the Constitution, every person has the right to protection of personal privacy and family secrets. In addition, they have the right to confidentiality of deposit and savings accounts, correspondence, telephone, postal, telegraph and other communications<sup>3</sup>. These basic rights are further expounding in the Civil, Criminal, and Labor Codes.

*The Civil Code* expresses the inviolability of private life, personal and family secrets as personal non-property privileges and rights<sup>4</sup> of every person. The rights to privacy in one's correspondence, telephone conversations, diaries, notes, information concerning birth and adoption, etc are also conveyed in this document. Accordingly, the publishing of diaries, notes and other documents is allowed only upon consent of the author; publishing of letters is allowed upon consent of their author and addressee<sup>5</sup>.

*The Criminal Code* classifies illegal acts and the prescribed punishments for commission of those acts. Thus, in reference to data protection, the Criminal Code states that the act of gathering information on a person's private life without their consent, which in turn caused damage to his/her rights and legal interests, is a crime against privacy and therefore subject to punishment. Further, if such a crime is committed by an official using their position of authority, or distribution of such information is through mass media or other publicly available means, a stricter penalty is deemed necessary<sup>6</sup>.

*The Labor Code* defines personal data of an employee as information regarding the employee that is necessary for initiation, continuation and termination of labor relations. The Code sets certain requirements for employers concerning personal data processing and disclosure:

- personal data must be presented by an employee personally;
- employers are not entitled to request information on an employee's religious, political, other views, or private life;
- an employer is not entitled to request information on an employee's participation and activity in public associations;
- while making decisions which affect the interests of an employee, employers do not have a right to base their decisions on personal data received by automated or electronic processing;
- protection of personal data shall be provided according to legislation of the Republic of Kazakhstan;
- personal data shall not be disclosed to third parties without the written consent of the employee;
- access to personal data of employees shall be given to specially authorized personnel only; authorized persons shall be entitled to have access to the data necessary for execution of definite functions only, and must keep that information confidential; and
- disclosing an employee's personal data within the organization shall be executed upon the employer's needs with which the employee shall be acquainted<sup>7</sup>.

In order to protect personal data disclosed to an employer, employees have the right to:

- free access of their personal data, including the right to receive copies of such data, except under circumstances covered by the laws of Kazakhstan;
- exclude or correct data that is incorrect or incomplete, or data which was processed in violation of the Labor Code;
- request the employer to inform individuals to which the incorrect or incomplete data was disclosed about respective corrections; and
- bring a claim in court against actions or inactivity of an employer that occurred while processing the employee's personal data<sup>8</sup>.

Along with personal data protection, Kazakhstani laws provide for protection of some other kinds of personal privacy/corporate confidentiality: secrecy of a will, secrecy of insurance, medical secrecy, undisclosed corporate information, bank secrecy, etc. ■

<sup>3</sup> Constitution of the Republic of Kazakhstan, Article 18

<sup>4</sup> Civil Code, Article 115

<sup>5</sup> Civil Code, Article 144

<sup>6</sup> Criminal Code, Article 142

<sup>7</sup> Labor Code, Articles 64, 65, 67

<sup>8</sup> Labor Code, Article 68

## GEORGIA: Still Unclear on Data Protection



by **Irakli Sokolovski**, Lawyer at *Mgaloblishvili Kipiani Dzidziguri (MKD)*

**It is almost two decades since Georgia has undertaken the revolutionary steps aiming the fundamental reforms of Georgian legislation and its compliance with the newly emerged tendencies. Legislative measures have concerned almost all vital spheres of social, economical and political life. However, the said is not true for the issue of data protection. It seems that business or ethical rationale behind the comprehensive scheme of data protection is not well understood yet in Georgia.**

### Existing Georgian privacy law

There is little specific privacy law in Georgia. As the country has not enacted the *lex specialis* legislation on data protection, the issue is mainly dealt in general manner. The Constitution of Georgia refers to the general right of privacy stating that private information of the person shall not be accessible without the consent of such person. Likewise, the Civil Code of Georgia makes no specific mention of privacy only referring to the general notion of non-materials rights of the person and establishing the general right of the person to have access to his/her private data. General regulation of data protection is also envisaged in General Administrative Code of Georgia. However, the latter is only applicable in vertical relationships and may be invoked only in relations of public law kind.



Sector-specific approach to data protection matter can be found in exceptional cases and in statutes such as the Tax Code of Georgia, Law of Georgia on Commercial Banks, Decree of National Commission of Communications of Georgia on Provision of Services and Protection of Consumers' Rights in the Sphere of Electronic Communications. However, the scope of application of these statutes is very narrow and covers the specific spheres for which these regulations have been enacted. As far as the definition of personal data is concerned, only two statutes provide the specification in this respect. According to General Administrative Code of Georgia personal data (information) means public information allowing identification of a person.

Further Decree of National Commission of Communications of Georgia on Provision of Services and Protection of Consumers' Rights in the Sphere of Electronic Communications defines private data as information concerning the name of consumer, the address of the technical medium location, telephone number, received services and paid amounts, as well as other information which allows the identification of the consumer.



### Consent or notification?

The huge controversy persists concerning preconditions for the disposal of personal data as Georgian legislation does not address this issue in explicit manner. The matter mainly arises upon collection or procession of personal data whereby it shall be ascertained whether consent of the concerned person is incumbent or mere notification would suffice for such collection or procession. Only Administrative Code of Georgia explicitly states that in these cases administrative body shall inform concerned person about the objectives and legal grounds for processing personal data. However, as ►

ambit of General Administrative Code is restricted to public law relations, the issue remains unclear for example in labor relations, whereby the collection or disposition with personal data is of the frequent character.

In the absence of clear cut regulation, said matter is scrutinized in the light of general legal principles applicable within the Georgian law. Based on that, it is argued that collecting or processing of personal data can be undertaken only by virtue of the consent given from the concerned individual. This conclusion is particularly due to the principle of “ownership” enjoyed by the individual in relation to his/her private nonmaterial rights (*inter alia* the personal data), such ownership may be interfered only with the permission of that individual or without such permission based on explicit exemptions foreseen by the legislation.

Moreover, Georgian legislation is uncertain about the specific form of the arrangement envisaging the consent of the individual. It is still ambiguous whether verbal consent or unilateral declaration of the individual would be sufficient for the disposal of personal data. In any case, for the data controller to have “safe harbor” the written arrangement envisaging the consent of the individual is recommended (for example, ad hoc contract envisaging the preliminary unambiguous consent of the party on processing the personal data by the company). Such mechanism accommodates binding force and legal enforceability of disposal with data.

On the other hand, Georgian legislation does not envisage data protection principles to which the data controllers (e. g. employees) shall comply with in order to ensure that processed, collected or stored data is maintained in safe conditions. Accordingly, the absence of code of conduct for the data controllers entails the potential risk related with the abuse of personal data.

### Cross border transfer of personal data

Another issue lacking the express regulation under Georgian law is the cross border transfer of the personal data. In the absence of specific regulation, the consent based system of processing of personal data, as mentioned above, shall be applicable.

However, there is no same provision under the Georgian law as envisaged by EU legislation that transfer of personal data shall be limited to the jurisdictions not providing the “adequate” protection for personal data. Accordingly, the risk of the abuse of personal data exported in countries without “adequate protection” of personal data seems very problematic.

## Complication may arise where the export of personal data from EU is at stake

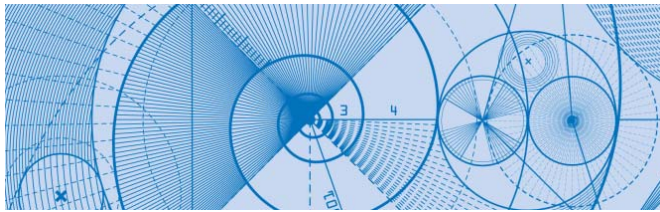
### Conclusion

In data protection area the winds of changes are not blowing across and it is unlikely that situation in this respect to be changed in nearest the future. Although certain international projects have been initiated to prompt the adoption of respective legislation, still there is no universal consensus over the need for comprehensive data protection law. The absence of respective legislation has predominantly two-fold impact:

- the privacy rights of the individuals are jeopardized as the current state of legislation is not sufficient to ensure the effective protection of personal data;
- it puts Georgia outside the out-sourcing tendencies, as the latter entails the transfer of great quantities of personal data.

Nonexistence of specific laws on data protection matters can pose a major challenge for the multinational companies that manage the human resources where the personal information is transferred cross-border. Particularly, the complication may arise where the export of personal data from EU is at stake, as the latter precludes such transfer if the transferee state does not provide the “adequate” protection for personal data. With regard to the contemporary state, Georgia is not deemed “adequate” by EU. ■





# DP\_News@CIS

## RUSSIA: Publication of Personal Data of Debtors by Bailiffs is now Permitted

In November 2010, the bill on publication of personal data of debtors on the Internet was introduced into the Russian parliament. According to this bill, the *Federal Bailiff Service* is allowed to publish personal data related to debtors on the web site of the *Bailiff Service*. Earlier, in August 2010 the *Bailiff Service* was given the authority to request from any third parties information containing personal data.

These changes don't affect the rights of private companies with regard to their debtors. There have been previously a number of cases in which Russian companies not only have been fined for handing over data to collectors, but also for the fact that they published lists of debtors on their websites. ■



The Federal Bailiff Service (FSSP of Russia) is a federal body of executive authority responsible for the orderly functioning of courts of law, fulfillment of court rulings and acts of other bodies and officials, and enforcement of law, control, and supervision in its sphere.

## UKRAINE: New Law On Protection of Personal Data Came into Force



The new law was adopted by the Verkhovna Rada almost unanimously.

Regulations on personal data issues have for many years remained vague and controversial and respective rules were of general nature and diluted in a number of laws. At the same time rapid development of personal data operations required more straight and clear rules. It was necessary for both citizens as bearers of the data, and companies/state as main users of the data. It was also required in the course of harmonization of Ukrainian legislation with EU laws.

The new law On Protection of Personal Data, which became effective on January 1, 2011, becomes the cornerstone for legislative regulations to personal data issues. Based on the text of the law one may come to a conclusion that it has both strong and weak sides. Speaking of the first, the law finally provides for certain rules in the areas where businesses had to make guesses in the past. This is an important step forward.

### The law restricts the use even of name and age of a person

As to weak sides of the law, it is for instance too general definition of personal data, which results in restriction for use even of name and age of a person. The law also provides for too limited circle of public persons, whose personal data should be easily accessible by the public. The law also has a number of terms not defined in Ukrainian legislation, which will be interpreted by authorities at their discretion. This may result in inconsistent application of the law and corruption practices.

Anyway the adoption of the law even in the current version is still a positive change for both people and businesses. ■

## UKRAINE: Banks Obligated to Use Local Servers

Starting from January 1, 2011 all banks having their branch offices in Ukraine have to use servers actually located inside Ukraine for processing and storage of operational data.

The state decided to change the rules in June of 2010, when the *National Bank of Ukraine (the NBU)* amended its *Order on Organization of Operational Activities of Banks in Ukraine* and ruled that "processing of information on operations and its storage shall be maintained at servers and/or other hardware, which shall be in fact located in the territory of Ukraine".

After a half-year grace period, the NBU can punish those banks that disobey



The National Bank of Ukraine is the state regulator that establishes rules for all the banks that operate in Ukraine.

By the time of the adoption of the new rules, a significant part of the banks in Ukraine, especially those with international ownership, preferred to process and store banking data on servers outside Ukraine. This was being done for various reasons. For instance, some international banks preferred to process and store data centrally, in a limited number of countries. Some did it because the lack of trust in Ukrainian authorities and in order to prevent sudden seizure or leaks of financial data.

Having granted 6 months to the banks to reorganize their data processing and storage, the NBU now has the right to punish those banks, if any, that failed to do so, with monetary and other sanctions. ■

### BULLETIN PRODUCTION TEAM

CHIEF EDITOR: Pavel Sadovsky

CONTRIBUTORS: Taras Kyslyy, Dennis Turovets, Pavel Sadovsky, Viktoriya Alzhanova, Irina Butko, Irakli Sokolovski

SUPPORTING EDITORS: Andy Hunder, Lesia Nychyporenko, Igor Kalenichenko

POST-PRODUCTION AND DISTRIBUTION: Sergey Novikov

Pictures: Shutterstock, Roads Less Traveled Photography gallery at Flickr, President Medvedev's official website.

**MAGISTERS** is the leading pan-CIS law firm with around 100 lawyers in its Astana, Kyiv, Minsk and Moscow offices and a representative office in London. Recently endorsed as the "Russia and the CIS Law Firm of the Year" at *The Lawyer European Awards 2010*, Magisters has a full-service offering and often acts as single point of contact for multinational clients doing business across the CIS. The firm's CIS reach is complimented by its "best friends" network of top-ranked local counsels from Armenia, Azerbaijan, Georgia, Kyrgyzstan, Moldova and Uzbekistan. Leading legal guides including *Chambers*, *Legal 500*, *IFLR 1000*, *Who's Who Legal*, *Managing IP*, *AsiaLaw Profiles*, and *PLC Which Lawyer* recommend Magisters for doing business in the CIS. Find out more at [www.magisters.com](http://www.magisters.com).

### SUBSCRIPTION

If you have received this bulletin by mistake, please accept our apologies. If you wish to (un)subscribe then please send a blank email to [moscow@magisters.com](mailto:moscow@magisters.com) with "Subscribe to [Unsubscribe from] DP newsletter" in the subject line.

### DISCLAIMER

© 2011 Magisters. All rights reserved.

Any republishing of materials from this bulletin, without a written permission from Magisters, is strictly prohibited. The information given is for your consideration only; it cannot be treated as legal advice or a recommendation. Please consult with a specialist before taking any actions on the basis of this information.