Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

Volume 13, Number 1 January 2013

Ukraine's New Data Protection Law Amendments and Other Important Recent Developments

By Olga Belyakova, of CMS Cameron McKenna LLC, Kyiv.

Some two-and-a-half years have passed since Ukraine enacted its Data Protection Law[1] (*see analysis by the author at WDPR, August 2010, page 17*).

Although the ideas behind the Data Protection Law were really positive and progressive, during its short life, the law has received a lot of criticism. Much of this criticism relates to a number of unclear and unenforceable provisions, as well as some burdensome procedures that businesses were required to follow.

Given the imperfections of the Data Protection Law, not only companies but also governmental bodies, in particular the State Service of Ukraine for Protection of Personal Data (the "Data Protection Authority"), have suffered. The Data Protection Authority was required to process millions of applications for the registration of databases, a demand with which it has not been able to cope.

Significantly, the New Law eliminates the requirement for Data Protection Authority approval of data transfers abroad.

Having learned from the experience of the Europe Union, as well as that of neighboring countries, the Parliament of Ukraine decided to follow the rest of the progressive world, and in late December 2012 substantially amended the Data Protection Law[2] (the "New Law") (*see report in this issue*).

The New Law became effective from January 1, 2013.

This article considers the most important amendments of the Old Law brought about by the New Law, and reviews some other changes in Ukrainian legislation from the past year that impact data protection procedures.

The New Law — What's New?

Coverage

Unlike before, when the Old Law quite narrowly protected only personal data contained in certain databases, the New Law covers all personal data, irrespective of their location. This is an important step toward international practice, and means that a data subject does not have to clarify whether his or her personal data is contained in a database before he or she can claim protection.

Consent of Data Subjects

One of the most controversial aspects of the Old Law involved the form in which a data subject had to give consent to the processing of his or her personal data. The wording offered by the Old Law was very vague,

and in fact envisaged only a "documented form" of consent. This meant that collecting electronic or web consents was quite an issue, and, in practice, to be safe, companies tended to collect paper consents, which was quite burdensome.

The New Law clarifies this requirement, and now a data subject can give his or her consent in any form that can be confirmed. From a practical standpoint, this amended definition makes life much easier for data controllers, as they can now lawfully collect consents from data subjects in a more "modern" way, *i.e.*, via emails, web resources, video records, *etc.*, provided they can technically confirm that such consent was really granted.

Employment Relations

Until recently, another difficult issue related to the registration of databases containing personal data. The Old Law required all such databases to be registered with the Data Protection Authority, irrespective of the nature of the relations between data subjects and data controllers. Thus, even employers' databases, which naturally contained employees' personal data, were subject to mandatory registration.

That requirement led to a situation in which the Data Protection Authority had to review and process an enormous number of applications for the registration of employers' databases from all over Ukraine. Consequently, the regulator became so overloaded that currently it is more than a year behind in processing applications[3] .

The New Law corrects this ridiculous situation, exempting data controllers from having to register those databases connected to employment relations.

As a matter of practice, those data controllers whose employment-related databases have not yet been registered by the Data Protection Authority are recommended to withdraw their applications. This will ease the burden on the Data Protection Authority and also enable those databases which are still subject to mandatory registration to be registered in a shorter time.

Registration of Databases

The New Law extends the term for registration of databases to 30 business days (it had been 10 days under the Old Law) and removes the obligation of the Data Protection Authority to notify applicants about the receipt of their applications.

In addition, the New Law supplements the list of information to be disclosed by data controllers when applying for registration by adding three more points: 1) information about the content (*i.e.,* the type of information processed, not the personal data itself) of the personal data processed; 2) information about third parties to which personal data are transferred; and 3) information about cross-border transfers of personal data.

It is worth noting that the first additional point has already been included in the standard application form developed by the Data Protection Authority, and the requested information is, in fact, being disclosed by applicants. However, the two other points are new, and they are to be added to notifications from January 1, 2013.

Cross-Border Transfers

While the Old Law contained very vague and sometimes ambiguous provisions regarding international data transfers (for instance, concerning the necessity to seek approval of the transfer by the regulator), the New Law clarifies this issue to a certain extent.

Significantly, the New Law eliminates the requirement for Data Protection Authority approval of data transfers abroad.

Although the New Law still requires that personal data be transferred only to countries which provide an adequate level of data protection, it now clarifies what those countries are. Specifically, the New Law refers to member states of the European Economic Area (EEA), as well as all other countries that have joined the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the "Convention").

The above list is not exhaustive, and the New Law provides that other countries which provide an adequate level of data protection (*i.e.,* non-EEA members and non-members of the Convention) will be defined separately by the Cabinet of Ministers of Ukraine. This is really important in terms of business activity in Ukraine, as important business relations have been developed with, *inter alia*, the United States and Canada, which are not members of the EEA or the Convention. There is a chance they will be included in the additional list.

Another amendment regarding cross-border data transfers relates to the grounds for transfers. Grounds for transfers were not directly defined as regards international data transfers, and it was only implied that the data subject should provide his or her consent to such an action.

The New Law offers five alternative actions which may serve as legal grounds for cross-border data transfers, and gives business entities more room to process personal data internationally. These five actions are: 1) providing unambiguous consent by the data subject; 2) concluding or fulfilling an agreement between the data controller and a third party for the benefit of the data subject; 3) protecting vital interests of the data subject; 4) protecting the public interest or pursuing legal remedies; and 5) providing relevant guarantees by the data controller regarding non-interference into the private and family life of the data subject.

Controlling Functions of the Data Protection Authority

The New Law brings clarity regarding controlling functions of the Data Protection Authority by officially granting it the right to conduct both on-site and off-site inspections. Inspections, in turn, will be initiated by the Data Protection Authority based on the Order of the Ministry of Justice of Ukraine adopted in mid-2012[4] .

Given the above official right of the Data Protection Au-

   ISSN 1473-3579

thority, it is recommended that companies check their existing internal data protection rules and make sure they fully comply with the data protection law. In particular, it is advisable to check whether consents to the processing of personal data have been duly collected from all data subjects, whether the company developed and approved its own data protection policy (be it reflected in a separate document or in the company's charter), whether databases which are subject to mandatory registration have been really registered/notified, *etc.*

It is worth recalling that, from July 1, 2012, liability for infringements in the data protection sphere have been substantially strengthened, and now it is not limited to monetary penalties, but may result in up to five years' imprisonment (*see report by the author and Olexander Martinenko, of CMS Cameron McKenna LLP, Kyiv, at WDPR, February 2012, page 43*).

Other Amendments

The New Law provides a legal ground for relations between data controllers and data processors. Now it is finally established that their relations are regulated by contractual agreement.

Under the New Law, data processors, in processing personal data, may not go outside the purpose of processing and the volume of personal data as agreed in the relevant contract. Although no mandatory requirements for agreements between data controllers and data processors have been established, this provision means that the agreement between a data controller and a data processor should at least contain the purpose and the volume of the processing.

At the same time, the parties are free to agree on other terms and conditions of their cooperation.

Another amendment relates to a range of data subjects' rights. In fact, the New Law establishes in law certain rights which had always been implied but had been absent as law. As a result, data subjects now can legally recall previously provided consents to data processing, make reservations while providing consents, make complaints about data processing to the Data Protection Authority, *etc.*

The New Law also introduces some new general elements of data processing, such as protection of vital interests of data subjects, conclusion or fulfillment of the agreement to which a data subject is a party, and the necessity to protect the legitimate interests of data controllers and/or third parties, with certain exceptions. Thus, unlike earlier, when data controllers almost always had to seek data subjects' consent before processing certain personal data, now they will have an opportunity to avoid it in relevant cases.

Over the past year it became popular to discuss and adopt codes of conduct regarding data protection in different business sectors. Such discussions took place, for instance, in the IT and direct marketing sectors. The New Law leaves this right intact, but now requires professional bodies to obtain approval of the Data Protection Authority for such codes.

Data Protection in the Banking Sector

It is worth noting that, in mid-2012, the National Bank of Ukraine (the "NBU") made important amendments to the existing Rules of Storage, Protection, Use and Disclosure of Banking Secrets[5] (the "New Rules"). The New Rules, *inter alia*, touched upon data protection issues.

The amendments set strict rules for the processing of personal data relating to bank secrecy (such data are defined as data or a range of data about an identified or identifiable individual made available to a bank 1) while providing banking services to such an individual and 2) during relations with him/her or with a third party).

According to the New Rules, banks (and other institutions which deal with personal data relating to bank secrecy, together "banks") are required:

- to register all relevant databases that contain personal data relating to bank secrecy; and
- adopt internal regulations regarding personal data processing, such regulations necessarily to contain, *inter alia*, the purpose of the processing and the structure of personal data; the order for inclusion, modification, renewal, use, dissemination, or depersonalization of personal data in the relevant database; the order for personal data protection, *etc.*

The New Rules also established specific requirements for the form of consent provided by the data subject. Specifically, consent may be made in a free form, but must be personally signed by the data subject with his/her signature to be certified by a notary or by the head of the bank and (in the latter case) stamped by the bank seal.

Alternatively, consent may be 1) included in the body of the agreement for banking services between the bank and the client, or 2) confirmed by electronic digital signature, or 3) provided via web resources.

Recommendations from the Data Protection Authority

During 2012 the Data Protection Authority was quite active in providing its views on different issues related to data protection.

On its website[6] it uploaded a range of recommendations, which may be quite useful in business activities. However, it must be stressed that those recommendations are not recognized as rule of law, but rather are considered to be guidance in certain cases.

Among other things, the Data Protection Authority clarified what to do with data in case of the liquidation of a legal entity, and provided its recommendations as regards drafting a data protection policy.

One of the Data Protection Authority's most important analyses related to video surveillance. Both the Old Law and the New Law are silent on this issue, but, in practice, many entities have faced problems with properly organizing their business activities when using video sys-

tems. Supermarkets, shops, and business centers were among the first types of businesses to use video surveillance.

The regulator developed a number of recommendations regarding video surveillance[7], which may be summarized as follows.

Those who intend to introduce video surveillance must notify data subjects by placing a notice of this fact. Such notice must be located in a public place and must be clearly visible, so that a data subject can easily see it before processing of his/her personal data begins.

Moreover, it is recommended that such notice include the following information:

- a warning about the use of video surveillance;
- the name and address of the data controller that conducts the video surveillance;
- the purpose of the video surveillance;
- contact details to enable the data subject to claim modification or destruction of his/her personal data from the system; and
- contact details of the Data Protection Authority which can be used by the data subject for purposes of complaining in case his/her rights have been infringed.

The data controller must also equip video surveillance systems with necessary technical tools in order to prevent illegal access to them. In addition, video surveillance systems must maintain the correct time and date.

Conclusions

Obviously, the New Law provides answers to some old questions, but at the same time gives rise to new ones. It is still necessary to sort out in a legal manner a range of issues, such as a general algorithm for cross-border transfers, an exhaustive list of countries that provide an adequate level of data protection, *etc.*

However, it is also clear that many issues may be resolved only based on Ukraine's own steps toward the practical application of data protection law.

Hopefully, Ukraine will build up its data protection system quickly in a way that will suit both the state and businesses.

NOTES

[1] Law of Ukraine On Protection of Personal Data No. 2297-IV, dated June 1, 2010.

[2] By the Law of Ukraine On Amending the Law of Ukraine on Protection of Personal Data No. 5491-IV, dated December 20, 2012 (the "New Law"). The Data Protection Law is hereinafter referred to as the "Old Law".

[3] According to information contained on the Data Protection Authority's official website, http://zpd.gov.ua/dszpd/uk/index.

[4] Order of the Ministry of Justice of Ukraine On Adoption of the Order of Conduction by the State Service of Ukraine for Protection of Personal Data of State Control for Compliance with the Data Protection Legislation No. 947/5, dated June 22, 2012.

[5] Approved by National Bank of Ukraine Order No. 292, dated July 11, 2012.

[6] Available, in Ukrainian, at http://zpd.gov.ua/dszpd/uk/publish/category/36425.

[7] Available, in Ukrainian, at http://zpd.gov.ua/dszpd/uk/publish/article/39649.

The text of Ukraine's new data protection law, in Ukrainian, can be accessed at http://op.bna.com/wdpr.nsf/id/jmsn-936lbm/$File/law%205491.pdf.

Olga Belyakova is a Senior Lawyer with CMS Cameron McKenna LLC, Kyiv. She may be contacted at olga.belyakova@cms-cmck.com.

   ISSN 1473-3579