

Setting Up Personal Data Protection System in Company: Key Requirements and Practical Solutions

Vladyslav Podolyak
Vasil Kisil & Partners

Experience shows that foreign companies' subsidiaries have proved to be better prepared, if not legally, then at least ideologically, for the entry into force of Law of Ukraine No. 2297-VI "On Personal Data Protection", dated June 1, 2010 (the "Personal Data Protection Law"), compared to Ukrainian business entities.

The thing is that the legal concept of personal data protection came to us from the EU legislation and from international public law. That is why Western organizations often just need to borrow personal data protection policies from their parent companies and adjust them for their Ukrainian affiliates, while Ukrainian business entities have to draft the necessary documents from scratch. A major problem associated with the drafting of good-quality documents (to be outlined below in this article) is the lack of empirical experience. The Personal Data Protection Law governs respective legal relations in a rather general manner and gives rise in practice to a number of questions, from the notion of personal data to the specific aspects of its protection in various sectors of economy, such as financial services, medicine, recruiting, telecommunications.

In this article, we want to comment on some provisions of the Personal Data Protection Law and share practical advice on compliance with relevant regulatory requirements.

What to Begin With?

Making a brief digression into theory, let us comment on the notion of "personal data" to identify the target of our research. Article 2 of the Personal Data Protection Law defines personal data as any or all information relating to an identified or identifiable individual. It should be mentioned at once in this context that a great many critical remarks are made about the very general nature of this definition, as it is not possible to clearly separate personal data from other information.

We should say that we do not share this criticism for the reasons outlined below. Since individuals, modern life and the information society are highly versatile and the means of registering, using and processing information do not have any clearly defined boundaries, it is practically impossible to provide an exhaustive list of information qualifying as personal data. They can include biometric data, any other background, biographical, family, professional and other data. Therefore, like its European counterparts, the Ukrainian Personal Data Protection Law has the necessary level of legal abstraction from a perspective standpoint and replaces any clearly defined list with certain criteria suggested to be used in each particular situation to determine whether certain information qualifies as personal data or not.

Such criteria deduced from the Personal Data Protection Law include the following two criteria: first, relevant information always relates to an individual, and second, such information can be used in each particular situation to identify the respective individual (personal data subject). If information relates to legal entities, it can be protected using other methods, such as a trade secret. If the available information is not sufficient to identify an individual, such information does not qualify as personal data. Meanwhile, the Law does not specify whether its requirements involve the general possibility of identification or the identification by a specific group of persons (such as the personal data subject's friends). If any personal data is linked to a coded name of an individual and access is forbidden in the available circumstances to the deciphering of such coded name into the real name of the individual, such data does not qualify as personal data with respect to persons processing such data without being able to decode them.

We also suggest introducing an additional criterion of the availability of a personal database where personal data are fully or partially processed. In other words, the Personal Data Protection Law covers the processing of data in a database, i.e. a named collection of systematically arranged personal data in an electronic form and/or in the form of card index files (see Articles 1 and 2 of the Personal Data Protection Law).

Therefore, the company should first of all determine whether it processes personal data or not. We can say at once that most companies do indeed process personal data, at least employees' personal data, in the context of HR, management and social matters, as well as in the context of labor remuneration and taxation. But often it is not just the employee personal data that are processed within a company. Companies providing services for private individuals also often use their personal data. Possible examples include the issue of personal sports club membership cards, the sale of air tickets, the servicing of individual deposits, the invitation of clients to a corporate party event, the personalized polling of clients regarding the quality of services provided to them. None of these are possible without the required minimum content of personal data.

Therefore, having identified its need to process personal data, the company should clearly define the purpose for which such personal data is processed. We do not rule out that information about individuals can be used for a great many different purposes in the foreseeable future, and so we recommend the broadest possible approach to this question. Article 2 of the Personal Data Protection Law provides that the individual, whose personal data are to be processed, must give his or her consent for the processing of such personal data for a particular purpose, and should the purpose of processing change in the future, a new consent is required to be obtained from such individual (part 1 of Article 6 of the Personal Data Protection Law). Thus, for example, if personal data are received from an individual client for the purpose of issuing a sports club membership card, such purpose of processing does not cover the use of such personal data for the purposes of a “get-a-free-gift” campaign or a promotional list of “The Club’s Famous Members”.

Once the categories and purpose of personal data processing are determined, the company should document the purpose of personal data processing (part 1 of Article 6 of the Law). We propose that a local document entitled “Regulations on Personal Data Processing and Protection” should be adopted. These Regulations may be approved by an order of the company’s executive body, e.g. the company’s director. Alternatively, the purpose of personal data processing may be laid down in the company’s Charter. This option is, however, more time-consuming and costly as it requires the holding of the general participants (shareholders) meeting of the company, the state registration of amendments to the Charter, and related capital expenditure.

Each company should determine for itself the content of the abovementioned Regulations since the Law does not impose any other requirements, except for the necessity to lay down the purpose of personal data processing therein. We recommend that you take a complex approach to the personal data protection issue and structure the Regulations as follows:

- 1) *General provisions: basic terms and scope of application of the Regulations;*
- 2) *Personal data processing procedure: receipt of a person’s consent; notice of the person’s rights and personal data handling practices;*
- 3) *Personal data processing purpose;*
- 4) *Personal database location: address; address of database processor (if any);*
- 5) *Conditions of personal data disclosure to third parties;*
- 6) *Data security: protection methods; personal data protection officers; data on children; data storage period;*
- 7) *Rights of personal data subjects;*
- 8) *Procedure for handling requests from personal data subjects;*
- 9) *State registration of personal databases.*

We recommend that the Regulations be communicated to personal data processing officers. We believe that this will enhance their awareness of the said information relations and will make them more responsible when dealing with personal data available to them.

Besides, in order to streamline the personal data collection process, we recommend you to approve the template of the consent given by a person to the processing of the personal data collected from such person. In addition, a standard notice containing information on the rights of the personal data subject, the data processing purposes and the personal data recipients should be elaborated. According to part 2 of Article 12 of the Law, such notice should given/sent in writing to the person concerned after his/her personal data have been included into a personal database. We do not rule out the possibility that, in order to save time, such notice may be delivered to the personal data subject immediately after the collection of personal data, i.e. before such data are physically entered into the database.

Database Registration and Staff-Related Issues

Article 9 of the Law requires the registration of the personal database. The registration had not been performed for half a year since the effective date of the abovementioned Law. For the time being, the registration is carried out in accordance with Resolution No. 616 of the Cabinet of Ministers of Ukraine, dated May 25, 2011, which approved the Regulations on State Register of Personal Databases and Procedure for Keeping thereof, and in accordance with Order No. 1824/5 of the Ministry of Justice of Ukraine, dated July 8, 2011, which approved the forms of applications for registration of personal databases and for amending the data contained in the State Register of Personal Databases and also approved the procedure for filing such applications.

According to part 5 of Article 24 of the Law, state authorities and local-self government bodies, organizations, institutions and enterprises of all forms of ownership shall designate a structural unit or a responsible officer to organize the protection of personal data in processing, as required by the law. The responsible officer may be appointed, or a special department may be authorized, by issuing a relevant order. We believe it expedient to confer or impose such functions on an IT Department or a HR Department.

Personal Data Collection

Thus, once in-house documents have been prepared, personal data processing may begin. A reservation should be made here. The foregoing logical sequence is an ideal but unlikely scenario. In practice, personal data appears to be already collected and being processed, as is the case in many instances. Therefore, the logical sequence will be fully applied only to the processing of data coming later.

So what should be done with the data obtained without a documented consent of the personal data subject while the Law has not been enacted yet (before January 1, 2011)? The Law itself gives no answer to this question. Thus, we put forward two options. As the first one suggests, initially it would be needed to obtain the person's post-factum consent to his/her personal data processing. After that, the person would be advised of his/her legal rights related to inclusion of the personal data into the database. The second option would only be to notify the person of the fact that his/her personal data were collected before the enactment of the Law which first envisaged the obligation to document the person's consent to the personal data processing and to notify the person in writing about the purpose of the data processing, third parties having access to such personal data and the person's rights provided in Article 8 of the Law. In particular, such rights include the right to raise a motivated claim regarding the alteration or removal of his/her personal data by any data controller or processor, if such data are processed illegally or are unreliable. Should the concerned person who has been duly notified about his/her rights raises no claim for removal of the personal data within a reasonable period of time, this may imply that the data obtained before January 1, 2011 are allowed to be used. However, the key to a uniform understanding of the current situation lays in the future law enforcement practice.

Therefore, the first step of compliance with the formalities regarding the personal data processing is to obtain, under the general rule, the person's documented consent to the personal data processing as per the specific purpose of such processing (Article 6 of the Law). The documented consent shall be understood as both written and electronic form of consent. The latter is often more convenient, especially when the person individually communicates his/her personal data via Internet, for instance, when sending a CV to a recruiting company or when signing in for participation in a promotion campaign on a shop's website.

Notifying the Person

Part 2 of Article 12 of the Law provides that the data controller is to notify the personal data subject, within ten business days after his/her personal data are included into the personal database, about the rights of such personal data subject which are provided in the Law, the purposes of the data collection and the persons to whom the personal data are transferred, which notification shall be solely in writing. As it was mentioned above, we suggest elaborating and providing the personal data subjects with a standard notice. Implementation of this provision of the Law may be problematic when giving notification to a person who had electronically communicated his/her personal data but had not specified the mailing address.

Pursuant to part 3 of Article 12 of the Law, no notification shall be made if the personal data are collected from public sources.

Summing up the above, it should be pointed out that part 10 of Article 6 of the Law stipulates that a standard procedure for personal data processing within personal databases is to be approved by the authorized state body which is competent in personal data protection (State Service of Ukraine for Personal Data Protection). The rules regulating the processing of personal data attributable to banking secrecy is to be approved by the National Bank of Ukraine. Currently, no such regulations have been adopted yet. However, we expect that, when elaborated, they will contribute to the personal data safety without imposing any burden on the business operations of the companies using personal data of individuals.