



THE 7TH EDITION OF THE INTERNATIONAL CONFERENCE
**EUROPEAN INTEGRATION
 REALITIES AND PERSPECTIVES**

Protection of Personal Data – actual and proposed issues

Florina Mariana Olteanu (Homeghiu)¹, Mihaela Olteanu²

Abstract: “Personal data” means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. There are different ways in which an individual can be considered ‘identifiable’. A person’s full name is an obvious likely identifier. But a person can also be identifiable from other information, including a combination of identification elements such as physical characteristics, pseudonyms occupation, address etc. International and national authorities tried to adopt different types of regulations in order to protect individuals’ personal data and to inform them with respect to their rights. The legal provisions are continuously changing according to the new realities (society and economy are changing, individuals are using different kind of communications). In order to have a strong protection of personal data and unitary rules for all member states, the European Commission published in January 2012 a proposal for a General Data Protection Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which will supersede Directive 95/46/EC. A regulation was considered the most appropriate legal instrument to define the new framework for the protection of personal data in the European Union: is directly binding upon the Member States, is directly applicable within the Member States and as soon as a regulation is passed, it automatically becomes part of the national legal system. The document shall be discussed by the European Parliament and the EU Member States meeting in the Council of Ministers for discussion. *The rules will take effect two years after they have been adopted.*

Keywords: data protection; personal data; data transfer; EU law

The term “personal data” includes information touching the individual’s private and family life “*stricto sensu*”, but also information regarding whatever types of activity is undertaken by the individual, like that concerning working relations or the economic or social behaviour of the individual. It includes therefore information on individuals, regardless of the position or capacity of those persons (as consumer, patient, employee, customer, etc).

The definition contains four main building blocks:

- “any information”,
- “relating to”,
- “an identified or identifiable”,
- “natural person”.

From the point of view of the nature of the information, the concept of personal data includes any sort of statements about a person. It covers “objective” information, such as the presence of a certain substance in one’s blood. It also includes “subjective” information, opinions or assessments. This latter

¹ Phd Student, National School of Political Studies and Public Administration, Romania, Address: 6 Povernei str., Sector 1, Bucharest, Romania, Tel.:+4021.318.08.97, fax: +4021.312.25.35, Corresponding author: m_florinaolteanu@yahoo.com.

² Phd Student, National School of Political Studies and Public Administration, Romania, Address: 6 Povernei str., Sector 1, Bucharest, Romania, Tel.:+4021.318.08.97, fax: +4021.312.25.35, e-mail: mihaelaolteanu@ymail.com - Beneficiary of the project “Doctoral scholarships for the development of the knowledge-based society”, co-funded by the European Union through the European Social Fund, Sectorial Operational Programme Human Resources Development 2007-2013.

sort of statements makes up a considerable share of personal data processing in sectors such as banking, insurance or employment.

In general terms, information can be considered to “relate” to an individual when it is *about* that individual. In many situations, this relationship can be easily established. For instance the data registered in one’s individual file in the personnel office are clearly “related to” the person’s situation as an employee.

The legal provisions apply to information related to a natural person that is “identified or identifiable”. This raises the following considerations. In general terms, a natural person can be considered as “identified” when, within a group of persons, he or she is “distinguished” from all other members of the group. Accordingly, the natural person is “identifiable” when, although the person has not been identified yet, it is possible to do it. Identification is normally achieved through particular pieces of information which we may call “identifiers” and which hold a particularly privileged and close relationship with the particular individual. A person may be identified directly by name or indirectly by a telephone number, a car registration number, a social security number, a passport number or by a combination of significant criteria which allows him to be recognized by narrowing down the group to which he belongs (age, occupation, place of residence etc.).

The protection afforded by the rules applies to natural persons, that is, to human beings. The right to the protection of personal data is, in that sense, a universal one that is not restricted to nationals or residents in a certain country. The concept of natural person is referred to in Article 6 of the Universal Declaration of Human Rights, according to which “*Everyone has the right to recognition everywhere as a person before the law*”.

The activity of protection and processing the natural persons’ personal data represents a challenge for Romanian companies and their employees, but also for Romanian authorities, taking into consideration the fact that the applicable legal provisions shall be observed. In our country, Law No. 677/2001 regarding the protection of individuals with respect to processing of personal data and free movement of such data (hereinafter the “Law No. 677/2001”) represents the general background, but the legal provisions were influenced by different European regulations, such as:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter the “Directive 95/46/EC”);
- Commission Decision on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (hereinafter the “Decision 2001/497/EC”);
- Commission Decision amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (hereinafter the “Decision 2004/915/EC”).

Based on the provisions of Law No. 102/2005 was created the National Authority for the Supervision of Personal Data Processing as public authority, autonomous and independent from any authority of the public administration, as well as from any natural or juridical person from the private area, having as objective protection of the fundamental rights and freedoms of the natural persons, in connection with the processing of personal data and the free circulation of these data.

The authority supervises and controls the legality of the personal data processing which falls under the Law no. 677/2001. For this purpose, the supervisory authority has the following prerogatives:

- receives and examines the notifications on the processing of personal data;
- authorizes the data processing in the situations stipulated by law;
- can decide, if it ascertains the infringement of this law, the temporary suspension or the cessation of the data processing, the partial or entire erasure of the processed data and can inform the penal bodies or sue;

- informs the natural and/or juridical persons about the necessity of complying with the obligations and carrying out the procedures stipulated by Law No. 677/2001;
- cooperates with the public authorities and public administration bodies, centralizes and examines their annual reports regarding the people's protection concerning the processing of personal data;
- issues recommendations and approvals on any matter connected to the protection of fundamental rights and freedoms, concerning the personal data processing, at any person's request, including public authorities and public administration bodies.

According to Article 3 of Law No. 677/2001 the notion "personal data" represent "any information relating to an identified or identifiable natural person; an identifiable person is a person who can be identified, directly or indirectly, in particular with reference to an identification number or to one or more factors specific to his physical, physiological, psychological, economic, cultural or social identity."

The provisions of Law No. 677/2001 apply to:

- processing of personal data, carried out within the activities performed by operators established in Romania;
- processing of personal data, carried out within the activities performed by diplomatic missions or consular offices of Romania;
- processing of personal data, carried out within the activities performed by operators who are not established in Romania, using the means of any kind located on the Romanian territory, with the exception when these means are only used for the transit of the personal data on Romanian territory, which are subject to such processing.

Personal data which are intended to be processed must be:

- processed fairly and in accordance with the existing legal provisions;
- collected for specific, explicit and legitimate purposes; further processing of personal data for statistical, historical or scientific research, will not be considered incompatible with the purpose they were initially collected for, if it is carried out according to the provisions of Law No. 677/2001, including those referring to the notification submitted to the supervisory authority, as well as according to the guarantees regarding personal data processing, set out by the legal provisions on statistics' activity or the historical or scientific research;
- adequate, pertinent and non excessive in relation to the purpose for which they are collected and further processed;
- accurate and, if necessary, updated; for this purpose, appropriate measures shall be taken in order to erase and/or rectify inaccurate or incomplete data, from the point of view of the purpose for which they were collected and later processed;
- stored in such a manner that allows the identification of the data subject only for the time limit required to fulfil the purposes for which they are collected and later processed; the storage of data for a longer period of time than the one mentioned, for statistical, historical or scientific research purposes, shall be carried out in accordance with the guarantees regarding personal data processing, provided in the relevant legal framework, and only for the period of time required to achieve these purposes.

The personal data collected based on the previous notification registered with the authority may be processed and/or storage in Romania, but they may be transferred to different countries. The transfer to another state of personal data that are subject to processing or are destined to be processed after being transferred may take place only if the Romanian law is not infringed and the state of destination ensures an adequate level of protection.

Data transferred to another state shall always be subject to prior notification to the supervisory authority. The supervisory authority may allow the data transfer to another state which does not offer

at least the same protection level as the one offered by the Romanian legislation, provided that the data controller offers enough guarantees regarding the protection of fundamental individual rights. These guarantees must be established through contracts signed by the data controllers and the natural or legal person(s) who have offered the transfer.

The above mentioned provisions do not apply when the data is processed exclusively for journalistic, literary or artistic purposes, if the data were made public expressly by the data subject or are related to the data subject's public quality or to the public character of the facts he/she is involved in.

The level of protection will be, in all cases, assessed by the supervisory authority from Romania taking into account all the circumstances in which the transfer is to be performed, especially:

- the nature of the data to be transferred;
- the purpose and the period of time proposed for the processing;
- the state of origin and the state of final destination;
- as well as the legislation of the state of final destination.

In case the supervisory authority notices that the level of protection offered by the state of destination is unsatisfactory, it may prohibit the data transfer or may authorize it provided that the operators offers enough guarantees regarding the protection of fundamental individual rights. These guarantees must be established through agreements signed by the operators and the natural or legal person(s) who have disposed the transfer.

In case the legal persons intend to process and/or storage and/or transfer the employee's name, address, contact details, date of birth, they are required to obey the legal regulations regarding the operation of the personal data. Therefore, the company has the obligation (i) to inform the new employees, according to Article 12 of the Law No. 677/2001, with respect to the transfer of their personal data abroad; (ii) to obtain their explicit consent for the transfer of data in different countries outside the European Union (hereinafter "EU"). The explicit consent of the employees with respect to the transfer of their data abroad shall be obtained in written, as mentioned in Article 30, letter a) of the Law No. 677/2001.

The Romanian legal provisions were influenced by Directive 95/46/EC, applicable to countries of the European Economic Area (hereinafter "EEA"), which includes all EU countries and in addition, non-EU countries Iceland, Liechtenstein and Norway. The Directive 95/46/EC protects the rights of everyone, irrespective of nationality or place of residence, the personal data being protected from misuse and from falling into unauthorised hands. We give our name, photograph, telephone numbers, birth date and address on a daily basis, whether to open a bank account, book a flight, apply for a job or to get a library card. Personal data is collected and processed for a variety of legitimate and necessary purposes. However, the data that we provide directly or indirectly should not be used for purposes other than originally intended. Nor should it be passed on to entities we haven't chosen to be involved with.

The personal data may be collected and used only under strict conditions and individuals must always be informed about the intention to collect and use your data. The Directive 95/46/EC creates obligations for the persons or entities which collect your personal data ("data controllers") who must respect individuals' rights while processing personal data entrusted to them.

Under EU rules, the natural persons have the following rights vis à vis data controllers:

- to be informed when they collect personal data;
- to be informed about the name of the controller, what the processing is going to be used for, to whom the data may be transferred;
- to receive the information whether the data was obtained directly or indirectly, unless this information proves impossible or too difficult to obtain, or is legally protected;
- to ask the data controller if he or she is processing the personal data;
- to receive a copy of this data in intelligible form;

- to ask for the deletion, blocking or erasing of the data.

Special precautions need to be taken when personal data is transferred to countries outside the EEA that do not provide EU-standard data protection. The Directive 95/46/EC states that personal data can only be transferred to countries outside the EU and the EEA when an adequate level of protection is guaranteed. Also, it requires that data transfers should not be made to non-EU /non-EEA countries that do not ensure adequate levels of protection. However, several exceptions (or “derogations”) to this rule could be applicable.

Personal data are increasingly being transferred across borders – both virtual and geographical – and stored on servers in multiple countries both within and outside the EU. The globalised nature of data flows calls for a strengthening of the individual’s data-protection rights internationally. This requires strong principles for protecting individuals’ data, aimed at easing the flow of personal data across borders while still ensuring a high and consistent level of protection without loopholes or unnecessary complexity.

To respond to these challenges, the Commission is proposing a system which will ensure a level of protection for data transferred out of the EU similar to that within the EU. This will include clear rules defining when EU law is applicable to companies or organisations established outside the EU, in particular by clarifying that whenever the organisation’s activities are related to the offering of goods or services to EU individuals or to the monitoring of their behaviour, EU rules will apply.

The Commission is proposing a streamlined procedure for so-called “adequacy decisions” that will allow the free flow of information between the EU and non-EU countries. An adequacy decision is an acknowledgement that a given non-EU country ensures an adequate level of data protection through its domestic law or international commitments. Such adequacy decisions will be taken at European level on the basis of explicit criteria which will also apply to police cooperation and criminal justice.

Businesses operating globally will benefit from clear and explicit rules for making use of binding corporate rules, as well as from the fact that prior authorisation will no longer be needed for transfers covered by binding corporate rules or standard contractual clauses. The proposal will promote effective international cooperation for data protection enforcement between the Commission, European data protection authorities and authorities outside the EU, through investigative assistance, information exchange and complaint referral.

Data subjects would have more rights, such as:

- Wherever consent is required for data to be processed, it would have to be given explicitly, rather than assumed;
- Individuals would have a “right to data portability” which would allow them to transfer personal data from one service provider to another more easily;
- Individuals would have a “right to be forgotten” which would allow them to obtain the deletion of the data that they furnished online if there are no legitimate grounds for retaining it (with exceptions);
- Individuals would be able to refer to the data protection authority in their country, even when their data is processed by a company based outside the EU.

Organizations would have more obligations and responsibilities, such as:

- Organizations would be required to notify the national supervisory authority of data security breaches *if feasible* within 24 hours; and if the breach would adversely affect the protection of the personal data or privacy of individuals, the controller would be required to communicate the personal data breach to the data subjects without undue delay;
- Organizations would only have to deal with a single national data protection authority in the EU country where they have their main establishment;

- Organizations would no longer have to notify their data protection practices to national data protection authorities, but would still have to obtain permission for some categories of processing;
- Instead of notification, there would be increased responsibility and accountability for those processing personal data; including significant disclosure and record keeping requirements.

EU rules would apply if personal data were handled abroad by companies that are active in the EU market and offer their services to EU citizens. Organizations would be exposed to penalties of up to €1 million or up to 2% of the global annual turnover of a company in case of breaching the applicable legal provisions.

The Commission intends to guarantee free and easy access to individuals personal data, making it easier for individuals to see what personal information is held about them by companies and public authorities, and make it easier for transfer their personal data between service providers – the so-called principle of “data portability”.

Conclusion

In case the proposed Regulation will be adopted, new rules regarding the protection of personal data will become applicable and legislative changes will take place. The new provisions will apply also on the territory of Romania, the legal persons and authorities will have the obligation to observe their content. The new rules related to data protection impose new responsibilities for those who hold and process personal details, intend to offer a better protection to individuals and a unitary application of the legal provisions. Also, the EU rules include new sanctions applicable to companies in case of using personal data, transferring personal data.

References

Hill, David G. (2009). *Data Protection: Governance, Risk Management, and Compliance*. CRC Press/Taylor & Francis Group.

Carey, Peter (2009). *Data Protection: A Practical Guide to UK and EU Law*. Third Edition. Oxford.

Solove Daniel J. & Schwartz, Paul M. (2011). *Privacy, Information, and Technology*. Third Edition. Wolters Kluwer Law & Business.

***Law No. 677/2001 regarding the protection of individuals with respect to processing of personal data and free movement of such data.

***Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

***Commission Decision on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC.

***Commission Decision amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries.