



EMERGENCY LEGAL KIT FOR BUSINESS SERIES

Year 3, Issue 2, February 2015

Personal Data Protection In Romania: An Overview

Main legal framework

The Data Protection Act, Law no. 677/2001, as further amended and supplemented in May 2005 and October 2007, transposes the provisions of Directive 95/46/EC as of October 24, 1996 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and sets the general framework for processing of data protection in Romania.

The Data Protection Act defines personal data and data processing, regulates consent rules, data transfer, the obligation of data controllers and the rights and remedies of the data subjects.

In addition to the Data Protection Act, there is Law no. 506/2004 on personal data processing and privacy protection in the electronic communications sector ("**Law 506/2004**"), which provides the conditions required for the protection of data that is being processed by the electronic communication providers, the confidentiality of such data as well as the regime of the traffic data. Law 506/2004 transposes Directive 2002/56/EC as of July 12, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

Main aspects on the concept of personal data

Personal data means any information relating to a natural person and any reference drawn from such information. The Data Protection Act does not provide an exhaustive list of such personal data.

There are several main requirements that data controllers must observe, such as:

- the personal data must be processed in good faith;
- the personal data must be collected for explicit and legitimate purposes only;
- the personal data must be adequate, relevant and not excessive with regard to the scope for which it is collected and processed;
- the personal data must be accurate and updated when necessary;
- the personal data must be stored only for a specific period of time, as necessary for the processing of the personal data.

Consent

Personal data may be processed as a matter of principle only with the data subject's prior, voluntary and informed consent.

The data subject may give such consent either in writing or electronically. For the processing of sensitive personal data the written consent of the data subject is required.

The data controller must be able to prove at all times that the consent of the data subject has been provided properly and lawfully.

Notwithstanding, there are several cases when the processing of personal data can be performed without the data subject's consent, *e.g.* if the processing is performed for statistical, historical or scientific purposes, provided that the data remains anonymous, or if the processing is related to data resulting from publicly available documents / information.

Special categories of personal data

The processing of personal data referring to racial, national or ethnic origin, political opinions and any affiliation with political parties, religious or philosophical beliefs, trade-union membership, data concerning health or addictions is in principle strictly forbidden.

The law sets forth several cases where such personal data may nonetheless be processed, however only subject to certain conditions, such as:

- the data subject has given its consent;
- the processing of the data is necessary as per the labour law;
- the processing of the data is necessary for the protection of the data subject, etc.

Other categories of personal data for which there are special requirements in terms of data processing include identification data (*e.g.*, personal numerical code), data referring to data subject's health or data with regard to the data subject's criminal record.

Rights of the data subject

If personal data is obtained directly from the data subject, the data controller must provide to the latter at least the following information:

- the identity of the data controller or its representative;
- the scope of the processing of the personal data; and
- any other information, as required by the law.

In addition to the above obligations, if the personal data is not obtained directly from the data subject, the data controller is obliged to inform the data subject with regard to the collection and processing of the personal data.

The data subject also has the following rights with respect to the collection / processing of the personal data:

- the right to access the data which is being processed;
- the right to intervene over the data – rectify, remove or block the personal data;
- the right to object against the processing of its personal data.

Registration

Data controllers must register with the Data Protection Agency (*Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal*) with regard to its intention to process personal data, prior to carrying out any data processing activities.

Security measures

The data controller must take all necessary technical measures in order to protect the personal data. Personal data must be protected against unauthorized access, alteration, transfer or disclosure, accidental or unlawful destruction and loss.

These protection measures must ensure a level of protection appropriate to the data that is being processed.

Transfer of personal data abroad

The transfer of personal data abroad by the data controller is subject to a prior notification to the Data Protection Agency. In such cases the Data Protection Agency will assess the adequate level of protection of personal data on a case by case basis, by taking into consideration, the nature of the data to be transferred, the processing scope and the proposed duration of the processing.

According to the Data Protection Act, provides the data may be transferred abroad only provided that the State towards which the transferred is made ensures an adequate level of protection.

The Data Protection Agency may approve the transfer of personal data to another State that does not provide the same level of protection as Romania only if satisfactory guarantees with regard to a person's fundamental rights are provided by the data controller.

Electronic communications

Law 506/2004, which sets the legal framework with respect to processing of personal data in the electronic communications sector, mainly contains provisions with respect to:

- security measures an electronic communication provider must comply with;
- procedures for accessing of personal data;
- confidentiality of communications;
- traffic data;
- location data.

According to Law 506/2004, the interception or surveillance of communications and related traffic data may be made only by the relevant public authorities as per the applicable statutory provisions, unless parties to the communication consent thereto in writing.

Interceptions may be made upon the request of intelligence and security agencies made under Law 51/1991 regarding Romania's national security, *i.e.* where there are threats to the national security.

In addition, pursuant to Decision no. 987/2012 of the National Authority for Management and Regulation in Communications ("ANCOM") on the general authorization regime for the provision of electronic communications networks and services, service providers must set up at their own cost the necessary technical means

and take all other necessary technical measures required to immediately enforce the lawful authorizations or warrants issued for interception of communications.

As per ANCOM's Decision no. 987/2012, the service provider is *inter alia* obliged to:

- technically allow the relevant authorities to perform interceptions;
- duly cooperate with the relevant authorities involved in interceptions;
- cooperate with the relevant authorities to implement security and audit criteria of national communications interception system developed by them;
- take all necessary technical measures to enable interceptions in general and immediately enable the enforcement interception warrants in particular;
- place at the disposal of the relevant authorities the interception management servers and the administration and operation consoles it holds, as required to ensure interceptions; and
- bear the costs of the interception interface.

In July 13, 2012, Law no. 82/2012 on retention of data processed by the electronic communication providers and by the public communication networks ("**Data Retention Law**") amended Law 506/2004. The Data Retention Law transposes Directive 2006/24/EC as of March 15, 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

On July 8, 2014 the Constitutional Court of Romania ("**CCR**") declared the Data Retention Law unconstitutional on grounds that provisions thereof violate the citizens' rights to privacy as provided by the Romanian Constitution and the European Convention for the Protection of Human Rights and Fundamental Freedoms, in that they interfere with and create a disproportion between the measures taken and the publicly protected interest.

This publication contains general information only, and it should not be considered as legal, tax, accounting opinion or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

For additional information, you may contact:



Alina Popescu

Co-Managing Partner

alina.popescu@maravela.ro



Sonia Fedorovici

Associate

sonia.fedorovici@maravela.ro