



## Country or jurisdiction report

### **ROMANIA**

Website: [www.dataprotection.ro](http://www.dataprotection.ro)

- I The transmission of personal data by a credit bureau type system without observing the conditions imposed by law:

A complaint was received from a citizen in which he claimed that the bank at which he had opened an account had transmitted his personal data (data referring to the accounts opened on his name) to a credit bureau type system, without his consent or a preliminary notice.

Legal grounds and solution: Personal data may be processed based (in principle) on the data subject's consent or on other grounds provided by Article 5 paragraph 2 of Law No. 677/2001 (as an exception). Also, in all situations in which personal data are collected directly from the data subject, the data controller has the obligation, according to Article 12 of Law 677/2001, to provide information to the data subject, including information referring to the transmission of data to other data controllers.

From the investigation performed at the premises of the bank, it could be ascertained that the complaint was well grounded as the bank was not able to provide any evidence that it had indeed informed the data subjects in accordance with Article 12, even though it had a legitimate interest to send the complainant's personal data to the credit bureau, in order to assess his payment behaviour and to avoid a burdensome credit.

- II One of the **preliminary controls** carried out by the National Supervisory Authority in 2006, in accordance with the provisions of Decision 89/2006, was aimed at verifying the conditions under which data referring to the individuals' health were to be collected and processed within an automated system. The data processing was notified by a foundation specialized in monitoring patients with chronic diseases and providing them with treatment and also providing financial support for treatments and the development of clinics and hospitals within a programme

approved by the Ministry of Public Health and carried out under the guidance of the Ministry of Education and Research with the participation of several university hospitals throughout the country. As a result of the preliminary control a Decision was issued through which the data controller was allowed to begin the data processing, with the obligation, however, to adopt the following measures:

- The data controller, its collaborators and contractual partners must take the necessary measures in order to ensure the quality and accuracy of the personal data entered into the system;
- The form used to obtain the consent of the data subjects for processing their personal data has to be modified in order to observe the requirements of Law no. 677/2001, modified and amended, as follows: the consent must be expressed freely and unaltered, it must also be unequivocal and informed; the data subject must be informed, when his data are collected, with regard to: the identify of the data controller, the processing's purpose, the recipients of the personal data, the possibility not to provide personal data or the consent, rights provided by Law 677/2001, modified and amended, especially the rights of access, intervention, and opposition, the way in which these rights may be exercised, as well as the rights they benefit from as patients according to Law No. 46/2003;
- The persons which express their consent must have full exercise of their rights and, in the case of those individuals with restricted exercise of their rights or without it, their consent will be obtained through their legal representatives;
- Personal data must be used only by physicians or other persons under the obligation of professional secrecy. This is why, the persons which have access to personal data have the obligation to sign a confidentiality clause, observing the rights of patients in accordance with the provisions of Law No. 677 and Law No. 46/2003;
- Observing the minimal security measures for personal data processing provided by Order No. 52/2002, will be carried out by adopting a written security policy, by effectively implementing security measures, including regularly training users by the data controller, its' collaborators, contractual partners and employees of the data processor;
- The rights of the data subject must be observed both at the time of the collection of personal data, as well as throughout the entire data processing;
- The data controller, its collaborators and contractual partners must observe the legal provisions in the fields of medical scientific research and carrying out clinical studies;
- The data controller must establish the retention period for the personal data manually or automatically, with regard to the purpose of the processing and bearing in mind the legal provisions on personal data protection, those referring to the medical field, as well as the provisions on keeping archives;
- Processed personal data may be included in reports on scientific research only after transforming them into anonymous data;
- Personal data which make up the medical file of the patient must be processed distinctly from other categories of data referring to administrative and financial management.

The data controller submitted to the preliminary control (the foundation that monitors various patients) has complied with the Decision issued by the Supervisory Authority.

III. An **investigation** was carried out in the case of a video surveillance system installed on the highway as a means of monitoring the traffic and to prevent and control the infringement of legal provisions in this field. The video surveillance and speed camera system used on the highway is connected to the system of national records of driving licenses' owners as well as the records of the owners of registered vehicles, in order to identify offenders. Capturing video images of the vehicles' number plate leads to the indirect identification of natural persons and as a result the dispositions of Law No. 677/2001, modified and amended, are applicable. As the personal data processing had never been notified prior to its beginning, the data controller was sanctioned for failure to notify its data processing. The data controller was also forced to adopt specific measures to properly inform the data subjects and to establish a determined period for storing the images in cases in which no offence had been noticed.