

**Law No. 677/2001**  
of 21<sup>st</sup> of November 2001  
**on the Protection of Individuals with Regard to the Processing of  
Personal  
Data and the Free Movement of Such Data**  
(published in the Official Journal of Romania, Part I No. 790 of the 12<sup>th</sup> of December  
2001)

The Romanian Parliament adopts the present law.

**Chapter I: General Provisions**

**Article 1: Purpose**

- (1) The purpose of this law is to guarantee and protect the individual's fundamental rights and freedoms, especially the right to personal, family and private life, with regard to the processing of personal data.
- (2) The exercise of the rights stated by this law shall not be restricted except for the specified and limited cases stated by this law.

**Article 2: Scope**

- (1) The present law applies to personal data processing, performed, totally or partially, through automatic means, as well as to the processing through means other than automatic ones, which are part of, or destined to, a personal data filing system.
- (2) The present law applies to:
  - a) personal data processing, carried out within the activities of data controllers based in Romania;
  - b) personal data processing, carried out within the activities of Romanian diplomatic missions or consular offices;
  - c) personal data processing, carried out within the activities of data controllers not based in Romania, by using any means on Romanian territory, unless these means are only used for transiting the processed personal data through Romanian territory.
- (3) In the circumstance referred to in paragraph (2) letter c), the data controller must designate a representative which must be a person based in Romania. The provisions of this law, applicable to the data controller, are also applicable to his representative, without prejudice to legal actions which could be initiated before a court of law against the controller himself.
- (4) The present law applies to the processing of personal data, carried out by Romanian or foreign natural or legal persons of public or private law, regardless of the fact that the data processing takes place in the public or private sector.

(5) Within the limitations set out by the present law, it also applies to the processing and transfer of personal data, carried out within the activities of preventing, investigating and repressing criminal offences and maintaining public order, as well as other activities in the field of criminal law, with the limitations and restrictions imposed by law.

(6) The present law does not apply to personal data processing, carried out by natural persons exclusively for their use, if the data in question is not intended to be disclosed.

(7) The present law does not apply to personal data processing and the transfer of personal data, carried out within the activities in the field of national defense and national security, with the limitations and restrictions imposed by law.

(8) The provisions of this law do not infringe upon the obligations assumed by Romania through its ratified international legal instruments.

### **Article 3: Definitions**

For the purposes of this law, the following terms are defined as follows:

- a) personal data: - any information referring to an identified or identifiable person; an identifiable person is a person that can be identified, directly or indirectly, particularly with reference to an identification number or to one or more specific factors of his physical, physiological, psychological, economic, cultural or social identity;
- b) personal data processing: - any operation or set of operations that is performed upon personal data, by automatic or non-automatic means, such as collecting, recording, organizing, storing, adapting or modifying, retrieval, consultation, use, disclosure to third parties by transmission, dissemination or by any other means, combination, alignment, blocking, deletion or destruction;
- c) storage: - keeping the collected personal data on any type of storage support;
- d) personal data filing systems: - any organized personal data structure which may be accessed according to some specific criteria, regardless of the fact that this structure is distributed according to functional or geographical criteria;
- e) data controller: - any natural or legal person, including public authorities, institutions and their legal bodies, that establishes the means and purpose of the personal data processing; if the purpose and means of the personal data processing is set out or based on a legal provision, the data controller shall be the natural or legal person assigned as data controller by that specific legal provision;
- f) data processor: - a natural or legal person, of private or public law, including public authorities, institutions and their legal bodies, which processes personal data on the data controller's behalf;
- g) third party: - any natural or legal person, of private or public law, including public authorities, institutions and their local bodies other than the data subject,

- than the controller, or the processor who, under direct authority of the controller or of his processor, is authorized to process data;
- h) recipient: - any natural or legal person, of private or public law, including public authorities, institutions and their local bodies, to whom the data are disclosed, regardless of the fact that it is a third party or not; the public authorities which receive data in accordance with a special type of inquiry competence will not be considered consignees;
  - i) anonymous data: - data that, due to its specific origin or specific manner of processing, cannot be associated to an identified or identifiable person.

## **Chapter II: General Rules on Personal Data Processing**

### **Article 4: Characteristics of Personal Data**

- (1) Personal data which is intended to be processed must be:
  - a) processed fairly and in accordance with the existing legal provisions;
  - b) 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 this law, 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;
  - c) adequate, pertinent and non excessive in relation to the purpose for which they are collected and further processed;
  - d) accurate and, if necessary, updated; for this purpose, appropriate measures shall be taken in order to erase an/or rectify inaccurate or incomplete data, from the point of view of the purpose for which they were collected and later processed;
  - e) stored in such a manner that allows the identification of the data subject only for the time limit required to fulfill 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.
- (2) Data controllers have the obligation to observe the provisions of paragraph (1) and to ensure the implementation of these provisions by the data processor.

### **Article 5: Conditions of Legitimacy Regarding the Data Processing**

- (1) Any personal data processing, except for the processing which refers to the categories mentioned in Article 7 paragraph (1) and Articles 8 and 10, may be

carried out only if the data subject has given his/her express and unequivocal consent for that processing.

- (2) The data subject's consent is not required in the following situations:
- a) when the processing is required in order to carry out a contract or an agreement previous to that contract to which the data subject is party of, or in order to take some measures, at his request, before signing that contract or previous agreement;
  - b) when the processing is required in order to protect the data subject's life, physical integrity or health or that of a threatened third party;
  - c) when the processing is required in order to fulfill a legal obligation of the data controller;
  - d) when the processing is required in order to accomplish some measures of public interest or regarding the exercise of public official authority prerogatives of the data controller or of the third party to which the data are disclosed;
  - e) when the processing is necessary in order to accomplish a legitimate interest of the data controller or of the third party to which the data are disclosed, on the condition that this interest does not prejudice the interests, or the fundamental rights and freedoms of the data subject;
  - f) when the processing concerns data which is obtained from publicly accessible documents, according to the law;
  - g) when the processing is performed exclusively for statistical purposes, historical or scientific research and the data remain anonymous throughout the entire processing;
- (3) The provisions of paragraph (2) do not infringe the legal texts that govern the obligations of public authorities to respect and protect intimate, family and private life.

## **Article 6: Ending the Processing Operations**

- (1) At the end of the data processing operations, if the data subject has not given his/her express and unequivocal consent for another destination, or for further processing, the personal data shall be:
- a) destroyed;
  - b) transferred to another data controller, provided that the former data controller guarantees the fact that the processing will have similar purposes to those of the former personal data processing;
  - c) transformed into anonymous data and stored exclusively for statistical, historical or scientific research;
- (2) In the case of processing operations performed under the terms stated under Article 5 paragraph (2) letters c) or d), within the activities described under Article 2 paragraph (5), the data controller may store the personal data for the required period of time, in order to achieve the specific followed goals, on the condition that adequate measures are ensured to protect the data, and shall

proceed afterwards to their destruction if the legal provisions on archive preservation are not applicable.

### **Chapter III: Special Rules on Personal Data Processing**

#### **Article 7: Processing Special Categories of Data**

- (1) Processing personal data regarding ethnic or racial origin, political, religious or philosophical beliefs or those of similar nature, trade-union allegiance, as well as personal data regarding the state of health or sex life, is prohibited.
- (2) The provisions of paragraph (1) do not apply in the following situations:
  - a) when the data subject has expressly given his/her consent for such data processing;
  - b) when the processing is required in order to meet the obligations or specific rights of the data controller in the field of labor law, in accordance with the legal guarantees; a possible disclosure to third party of the processed data may take place only if the data controller is legally required to do so, or if the data subject has expressly agreed to the disclosure;
  - c) when the processing is required in order to protect the data subject's life, physical integrity or health or that of another person which is legally or physically unable to express his/her consent;
  - d) when the processing is carried out as part of the legitimate activities of a foundation, association, or of any other non-profit organization with a political, philosophical, religious or trade-union profile, provided that the data subject is a member of that organization or has regular contacts with the organization in its activity profile, and provided that the data shall not be disclosed to a third party without the data subject's consent;
  - e) when the processing refers to data expressly made public in a clear way by the data subject;
  - f) when the processing is required in order to ascertain, exert or defend a right in a court of law;
  - g) when the processing is required for preventive medical care, to establish a medical diagnosis, to provide medical care or treatment in the interest of the data subject, or to manage health services that are in the best interest of the data subject, on the condition that the processing of that data is performed by, or under the supervision of medical staff pledged to professional secrecy or by or under the supervision of another person subject to a similar obligation regarding the secrecy;
  - h) where there is a specific legal provision, regarding the protection of an important public interest, on the condition that the processing is carried out in compliance with the rights of the data subject and other legal guarantees provided by the present law.

- (3) The provisions of paragraph (2) do not infringe the legal texts that govern the public authority's obligation to respect and protect intimate, family and private life.
- (4) The Supervisory authority may decide, based on justified grounds, the prohibition of the processing of data belonging to the categories stated in paragraph (1), even if the data subject has given his/her written, unequivocal consent, and the consent has not been withdrawn, on the condition that the prohibition stated in paragraph (1) should not be eliminated by one of the cases referred to in paragraph (2) letters b) – g).

#### **Article 8: Processing of Personal Data with an Identification Function**

- (1) The processing of the personal identification number or of other personal data with a general identification function may be carried out only if:
  - a) the data subject has given his/her express and unequivocal consent; or
  - b) the processing is expressly stated by a legal provision.
- (2) The supervisory authority may establish other situations in which the processing of data stated in paragraph (1) may be carried out, only after adequate guarantees have been provided in order to observe the data subject's rights.

#### **Article 9: Processing Personal Data Regarding the State of Health**

- (1) Except for the cases stated in Article 7 paragraph (2), the provisions of Article 7 paragraph (1) do not apply to the processing of health data in the following situations:
  - a) if the processing is necessary for the protection of public health;
  - b) if the processing is necessary for the prevention of an imminent danger, the prevention of a criminal offence or the prevention of the result of such an action or for the removal of the damaging results of such an action.
- (2) The processing of health data may be carried out only by, or under the supervision of, medical staff who are under a pledge of professional confidentiality, except for the cases when the data subject has given, in writing, his/her unequivocal consent and as long as the consent has not been withdrawn, as well as except for the cases when the data processing is necessary for the prevention of an imminent danger, the prevention of a criminal offence or the prevention of the result of such an action or for the removal of the damaging results of such an action.
- (3) The medical staff, health institutions and their staff, may process personal health data without the authorization of the supervisory authority only when the data processing is required in order to protect the data subject's life, physical integrity or health. When the mentioned purposes refer to other people or to the general public and the data subject has not given his/her written and

unequivocal consent, the preliminary authorization of the supervisory authority must first be demanded and obtained. The processing of personal data is forbidden beyond the limits of the authorization.

- (4) Except for emergency reasons, the authorization provided under paragraph (3) may be given only after consulting the Romanian Medical College.
- (5) Personal health data may only be collected from the data subjects themselves. Exceptionally, these data can be collected from other sources only when it is required in order not to compromise the processing's purpose, and when the data subject cannot or doesn't wish to provide them.

#### **Article 10: Processing Personal Data Regarding Criminal or Minor Offenses**

- (1) Processing personal data regarding criminal offenses committed by the data subject, or regarding previous criminal convictions, security measures or administrative or minor offense sanctions applied to the data subject, may be carried out only under the control of public authorities, within the limits of their powers given by law and under the terms established by the specific provisions in this field of law.
- (2) The supervisory authority may establish other cases in which the data processing stated under paragraph (1) may be carried out, only on the condition that adequate guarantees are put in place to observe the rights of the data subject.
- (3) A complete record of criminal convictions may be kept only under the control of a public authority, within its attributions, stated by law.

#### **Articles 11: Exemptions**

The provisions of Articles 5, 6, 7 and 10 do not apply to the situation in which the data processing is carried out exclusively for journalistic, literary or artistic purposes, or if the processing regards personal data that were expressly made public in a specific manner by the data subject or by the public character of the events that have taken place.

### **Chapter IV: The Rights of the Data Subject in the Context of Personal Data Processing**

#### **Article 12: Informing the Data Subject**

- (1) When personal data are obtained directly from the data subject, it is the data controller's obligation to provide the data subject the following information, except for the situations in which he/she already has this information:

- a) the identity of the data controller and, if required, of the data controller's representative;
  - b) the purpose of the data processing;
  - c) additional information, such as: the recipients, or the categories of recipients of the data; whether the requested information is compulsory, and the consequences of the refusal to provide it; the existence of the data subject's rights, stated by this law, notably the right of access, intervention and objection as well as the terms in which they may be exerted;
  - d) any other information which may be expressly requested by the supervisory authority, considering the processing's specific situation.
- (2) When the data are not obtained directly from the data subject, it is the data controller's obligation, at the moment of collecting data or at least before the first disclosure takes place, if he has the intention to disclose the data to a third party, to provide the data subject with the following minimum information, unless the data subject already possesses that information:
- a) the identity of the data controller and, if required, of the data controller's representative;
  - b) the purpose of the data processing;
  - c) additional information, such as: the recipients, or the categories of recipients of the data; whether the requested information is compulsory, and the consequences of the refusal to provide them; the existence of the data subject's rights, stated by this law, notably the right of access, intervention and objection as well as the terms in which they may be exerted;
  - d) any other information which may be expressly requested by the supervisory authority, considering the processing's specific situation.
- (3) The provisions of paragraph (2) do not apply when the processing of data is carried out exclusively for journalistic, literary or artistic purposes, if their enforcement might reveal the source of information;
- (4) The provisions of paragraph (2) do not apply when the processing of data is carried out for statistical, historical or scientific research, or in any other situations if providing such information proves to be impossible or would involve a disproportional effort towards the legitimate interest that might be damaged, as well as in the situations in which recording or disclosure of the data is expressly stated by law.

### **Article 13: The Right of Access to Data**

- (1) Every data subject has the right to obtain from the data controller, upon request, and free of charge, once a year, the confirmation of the fact that the data concerning him/her are or are not being processed by the data controller. The data controller, in case he has processed any personal data concerning the petitioner, is obliged to communicate to the petitioner, along with the confirmation, at least the following:

- a) information regarding the purposes of the data processing, the categories of data concerned, and the recipients or the categories of recipients to whom the data are to be disclosed;
  - b) communication in an intelligible form of the processed data and of any other available information regarding the source of origin of the respective data;
  - c) information on the technical principles and mechanisms involved in the data processing concerning that data subject;
  - d) information concerning the existence of the right of intervention upon the data, and the right to object, as well as the conditions in which the data subject can exert these rights;
  - e) information on the possibility of consulting the Register of personal data processing, stated under Article 24, before submitting a complaint to the supervisory authority, as well as to dispute the data controller's decisions in court, according to the provisions of this law;
- (2) The data subject may request from the data controller the information stated under paragraph (1) through a written, dated and signed petition. The petitioner may underline his desire to be informed at a specific address, which may also be an electronic mail address, or through a mail service that ensures confidential receipt of the information.
  - (3) It is the data controller's obligation to communicate the requested information, within 15 days of receipt of the petition, while complying with the petitioner's option as provided in paragraph (2).
  - (4) Regarding personal health data, the petition mentioned in paragraph (2) may be filled in by the data subject him/herself, or by medical staff who will mention the person on whose behalf the request has been made. Upon the data controller's or the data subject's request, such communication as mentioned in paragraph (3) may be carried out by a member of the medical staff, appointed by the data subject.
  - (5) If the personal health data are processed for scientific research purposes, if the risk of infringing the rights of the data subject does not exist and if the data are not to be used in order to take measures against a person, the communication mentioned in paragraph (3) may be dispatched within a period of time longer than the one mentioned in that paragraph, if that might affect the process or the outcome of the research, but it should not be delayed after the research has been completed. Such a situation is only allowed if the data subject has given his/her express and unequivocal consent for the data to be processed for the purpose of scientific research, as well as for the possible delay of the communication mentioned in paragraph (3);
  - (6) The provisions of paragraph (2) shall not apply when the processing of personal data is carried out exclusively for journalistic, literary or artistic purposes, if their application might affect confidentiality as to the source of the information.

#### **Article 14: The Right of Intervention upon the Data**

- (1) Every data subject has the right to obtain from the data controller, upon request, and free of any charge:
  - a) as the case may be, rectification, updating, blocking or deletion of data whose processing does not comply with the provisions of the present law, notably of incomplete or inaccurate data;
  - b) as the case may be, transforming into anonymous data the data whose processing does not comply with the provisions of the present law;
  - c) notification to a third party to whom the data were disclosed, of any operation performed according to letters a) or b), unless such notification does not prove to be impossible or if it does not involve a disproportionate effort towards the legitimate interest that might thus be violated.
- (2) In order to exert the right stated in paragraph (1), the data subject shall fill in a written, dated and signed petition. The petitioner may state his/her wish to be informed at a specific address, which may also be an electronic mail address, or through a mail service that ensures confidential receipt of the information.
- (3) The data controller has the obligation to communicate the measures taken, based on the provisions of paragraph (1), as well as, as the case may be, the name of a third party to whom the data concerning the data subject were disclosed, within 15 days from the date of the petition's arrival, whilst complying with the petitioner's possible option, according to paragraph (2).

#### **Article 15: The Right to Object**

- (1) The data subject has the right to object at any moment, based on justified and legitimate reasons linked to his particular situation, to a processing of data regarding him/her, unless there are contrary specific legal provisions. In case of justified opposition, the processing may no longer concern the respective data.
- (2) The data subject has the right to object at any moment, free of charge and without any justification, to the processing of the data concerning his/her person for overt marketing purposes on behalf of the controller or of a third party, or to be disclosed to a third party for such a purpose.
- (3) In order to exercise the rights stated under paragraphs (1) and (2), the data subject shall fill in and submit to the data controller a written, dated and signed petition. The petitioner may specify if he/she wishes to be informed at a specific address, which may also be an electronic mail address, or through a mail service that ensures confidentiality.
- (4) The data controller has the obligation to inform the data subject of the measures taken, based on the provisions of paragraph (1) or (2), as well as, as the case may be, the name of the third party to whom the data concerning the

data subject were disclosed, within 15 days of the date of the petition's arrival, in compliance with the petitioner's option, according to paragraph (3).

#### **Article 16: Exemptions**

- (1) The provisions of Articles 12, 13, Article 14 paragraph (3) and Article 15 do not apply for such activities as mentioned in Article 2 paragraph (5), if their enforcement affects the efficiency of the action or the objective followed in order to fulfill the legal obligations of the public authority.
- (2) The provisions of paragraph (1) are applicable solely for the period of time necessary for the achievement of the goal intended by carrying out the activities mentioned in Article 2 paragraph (5).
- (3) As soon as the reasons that justified the enforcement of paragraphs (1) and (2) no longer exist, the controllers who accomplish the activities stated by Article 2 paragraph (5) shall take all necessary measures in order to ensure the compliance with the data subject's rights.
- (4) Public authorities shall make a record of such cases and inform periodically the supervisory authority on the way these cases have been solved.

#### **Article 17: The Right Not to be Subjected to an Individual Decision**

- (1) Any person has the right to demand and receive the following:
  - a) the withdrawal or the cancellation of a decision that produces juridical effects concerning him/her, adopted exclusively on a personal data processing basis, carried out through automatic means, destined to evaluate some aspects of his/her personality, such as professional competence, credibility, behavior or any other similar aspects;
  - b) re-evaluation of any decisions regarding him/her, that affect him/her in a significant manner, if the decision was adopted exclusively on a basis of data processing that meets the requirements stated under letter a).
- (2) Respecting the other guarantees stated by the present law, a person may be subjected to a decision of the nature mentioned in paragraph (1), only in the following situations:
  - a) the decision is taken in the context of entering into or carrying out a contract, on the condition that the request to close or to bring the contract to conclusion, filled in by the data subject, has been satisfied or that some adequate measures to safeguard his/her legitimate interest have been taken, such as arrangements allowing him/her the possibility of sustaining his point of view in order to guarantee the protection of its own legitimate interest;
  - b) the decision taken is authorized by a law which states the measures that guarantee the protection of the data subject's legitimate interests.

### **Article 18: The Right to Refer to a Court of Law**

- (1) Without prejudice to the possibility of addressing the supervisory authority, the data subject has the right to refer to a court of law in defense of any rights, guaranteed by the present law, that have been infringed.
- (2) Any person that has suffered a prejudice as a consequence of unlawful processing of personal data may address a competent court of law in order to obtain compensation for the prejudice suffered.
- (3) The competent court of law is the one whose territorial jurisdiction covers the complainant's domicile. The complaint addressed to the court of law is exempt from stamp tax.

## **Chapter V: Confidentiality and Security of Processing**

### **Article 19: Confidentiality of Data Processing**

Any person who acts under the authority of the data controller or of the data processor, including the data processor, who has access to personal data, may process them only in accordance with the data controller's specific instructions, except when the above-mentioned person's actions are based on a legal obligation.

### **Article 20: Security of Data Processing**

- (1) It is the data controller's obligation to apply the adequate technical and organizational measures in order to protect the data against accidental or unlawful destruction, loss, alteration, disclosure or unauthorized access, notably if the respective processing involves the data's transmission within a network, as well as against any other form of illegal processing.
- (2) These measures shall ensure, depending on the state of the art techniques employed and the costs, adequate security against processing hazards as well as observing the nature of the data that must be protected. The minimum security requirements shall be issued by the supervisory authority and shall be periodically updated, according to the technological progress and the accumulated experience.
- (3) When appointing a data processor, the data controller has the obligation to assign a person who presents enough guarantees regarding technical security and the organizational measures concerning the data to be processed, as well as the obligation to ensure that the assigned person complies with these measures.

- (4) The supervisory authority may decide, in individual cases, that the data controller should adopt additional security measures, except such measures that regard the guaranteed security of telecommunication services.
- (5) Data processing performed by an appointed data processor shall be initiated following a written contract which should necessarily contain the following:
  - a) the processor's obligation to act strictly in accordance with the instructions received from the data controller;
  - b) the fact that accomplishing the obligations set out in paragraph (1) also applies to the data processor.

## **Chapter VI: Supervising and Control Of Personal Data Processing**

### **Article 21: The Supervisory Authority**

- (1) The supervisory authority, in the terms of the present law, is the National Supervisory Authority for Personal Data Processing.
- (2) The supervisory authority carries out its activity completely independent and impartial.
- (3) The supervisory authority shall monitor and control with regard to their legitimacy, all personal data processing, subject to this law. In order to achieve this purpose, the supervisory authority exerts the following attributions:
  - a) issues the standard notification forms and its own registers;
  - b) receives and analyses the notifications concerning the processing of personal data and informs the data controller on the results of the preliminary control;
  - c) authorizes personal data processing in the situations set out by law;
  - d) may dispose, if it notices the infringement of the provisions of the present law, temporarily suspending the data processing or ending processing operations, the partial or total deletion of processed data and may notify the criminal prosecution bodies or may file complaints to a court of law;
  - d') informs the natural or legal persons that work in this field, directly or through their associative bodies on the need to comply with the obligations and to carry out the procedures set out by this law;
  - e) keeps and makes publicly accessible the personal data processing register;
  - f) receives and solves petitions, notices or requests from natural persons and communicates their resolution, or, as the case may be, the measures which have been taken;
  - g) performs investigations –*ex officio*, or upon requests or notifications;
  - h) is consulted when legislative drafts regarding the individual's rights and freedoms are being developed, concerning personal data processing;
  - i) may make proposals on the initiation of legislative drafts or amendments to legislative acts already enforced, in the fields linked to the processing of personal data;

- j) collaborates with the public authorities and bodies of the public administration, centralizes and analyzes their yearly activity reports on the protection of individuals with regard to the processing of personal data, issues recommendations and assents on any matter linked to the protection of fundamental rights and freedoms regarding the processing of personal data, on request of any natural person, including the public authorities and bodies of public administration; these recommendations and assents must mention the reasons on which they are based and a copy must be transmitted to the Ministry of Justice; when the recommendation or assent is requested by the law, it must be published in the Official Journal of Romania, Part I;
  - k) co-operates with similar foreign authorities in order to ensure common assistance, as well as with foreign residents for the purpose of guaranteeing the fundamental rights and freedoms that may be affected through personal data processing;
  - l) fulfills other attributions set out by law;
  - m) the manner in which the National Supervisory Authority for Personal Data Processing is organized and functions is set out by law.
- (4) The entire staff of the supervisory authority has the obligation of permanently keeping the professional secrecy, except for the cases set out by law, regarding the confidential or classified information they have access to in carrying out their duties, even after termination of their legal employment relations with the supervisory authority.

## **Article 22: The Notification Addressed to the Supervisory Authority**

- (1) The data controller is obliged to notify the supervisory authority, either personally or through a representative, before initiating any kind of data processing which has a similar or related purpose(s) to previous data processing activities.
- (2) Notification is not necessary in the event that the sole purpose of the data processing is to keep a record available for public reference, open for consultation to the general public or to any person who proves a legitimate interest, provided that the data processing is strictly limited to such data that are necessary to the above mentioned record.
- (3) The notification shall contain the following information:
  - a) the name, address or premises of the data controller and of his representative, as the case may be;
  - b) the purpose(s) of the data processing;
  - c) a description of the category/categories of the data subjects and of the data, or the categories of data, that are to be processed;
  - d) the recipients or the categories of recipients to whom the data is intended to be disclosed;
  - e) the guarantee accompanying the disclosure to a third party;

- f) the manner in which the data subjects are informed of their rights, an estimate date on ending data processing operations and the future destination of the data;
  - g) transfers aboard of personal data intended to be carried out;
  - h) a general description that allows a preliminary assessment of the measures taken in order to ensure data processing security;
  - i) mention of any data filing system related to the processing, and of possible relation to other processing or other data recording systems, irrespective of the fact that they are situated on Romanian territory or not;
  - j) the reasons that justify the enforcement of the provisions of Articles 11 and 12 paragraph (3) or (4), or of Article 13 paragraph (5) or (6), in cases that the data processing is performed exclusively for journalistic, literary, artistic or statistical purposes, or for historical or scientific research.
- (4) If the notification is incomplete, the supervisory authority shall demand its completion.
- (5) Within its investigative powers, the supervisory authority may demand other information, notably regarding the data's origin, the automatic processing technology used and details about the security measures. The provisions of this paragraph do not apply in the situations in which the data is processed exclusively for journalistic, literary or artistic purposes.
- (6) If the processed data is intended to be transferred abroad, the notification shall consist of:
- a) the data categories subject to the transfer;
  - b) the country of destination for each data category.
- (7) The notification is subject to a fee that must be paid by the data controller to the supervisory authority.
- (8) The public authorities that carry out personal data processing related to the activities described in Article 2 paragraph (5), based on the law or in compliance with the obligations assumed through ratified international agreements, are exempt from the fee set out in paragraph (7). The notification shall be sent within 15 days from the entering into force of the legislative act that sets out the obligation in case and shall only contain the following elements:
- a) the name, address/premises of the data controller;
  - b) the purpose and the legal basis of the data processing;
  - c) the personal data categories subject to processing.
- (9) The supervisory authority may establish other situations in which the notification is not required, other than those provided in paragraph (2), or situations in which the notification may be submitted in a simplified manner as well as the content of such a notification, in the following cases:
- a) in situations in which, considering the nature of the data which are processed, the processing may not infringe, at least apparently, the rights of the data subject, on the condition that the purposes of that processing, the data or

- categories of processed data, the data subjects or categories of data subjects, the recipients or categories of recipients and the period for which the data are stored are all precisely mentioned;
- b) in situations in which the processing is carried out in accordance with the provisions of Article 7 paragraph (2) letter d).

### **Article 23: Preliminary Control**

- (1) The supervisory authority shall establish the categories of processing operations that may present special risks for the person's rights and freedoms.
- (2) If based on the notification, the supervisory authority assesses that the data processing belongs to one of the categories mentioned in paragraph (1), it shall decide on a preliminary control before the data processing in case begins, and accordingly informs the controller.
- (3) The data controllers who have not been informed within 5 days of notification upon a preliminary control being ordered may start the data processing.
- (4) In the situation provided in paragraph (2) the supervisory authority has the obligation, within no longer than 30 days from notification, to inform the data controller on the results of the control carried out, and on the decision issued thereupon.

### **Article 24: Personal Data Processing Record**

- (1) The supervisory authority keeps a personal data processing register, of the recorded processing under the provisions of Article 22. The registry shall contain all the information set out Article 22 paragraph (3).
- (2) Each data controller is given a registration number. The registration number must be mentioned on every document through which personal data are collected, stored or disclosed.
- (3) Any change affecting the accuracy of the registered information will be communicated to the supervisory authority within 5 days. The supervisory authority will immediately make the necessary amendments to the register.
- (4) The processing activities of personal data which started before the present law has come into force will be notified in order to be registered within 15 days of the date when the present law enters into force.
- (5) The personal data processing register is available for public reference. The supervisory authority shall establish the accessibility procedures.

### **Article 25: Complaints Addressed to the Supervisory Authority**

- (1) In order to defend the rights set out by the present law, the persons whose personal data are processed under the terms of this law may file in a complaint to the supervisory authority. The complaint may be addressed directly or

through a representative. The data subject may empower an association or a foundation to represent his/her interests.

- (2) The complaint submitted to the supervisory authority is invalid if a complaint, concerning the same matter and parties, was previously submitted to a court of law.
- (3) Except for the cases in which a delay would cause imminent or irreparable damage, the complaint submitted to the supervisory authority cannot be addressed earlier than 15 days from submitting a similar complaint to the data controller.
- (4) In order to solve the complaint the supervisory authority may, if considered necessary, hear the data subject's view, the data controller's view and the views of the empowered person or that of the association or foundation which represents the interests of the data subject. These persons have the right to file in the requests, documents and memoirs. The supervisory authority may order an expertise.
- (5) If the complaint is considered to be grounded, the supervisory authority may decide upon any of the measures set out in Article 21 paragraph (3) letter d). Temporary interdiction of the data processing may be ordained only until the reasons that have determined such measures have ended.
- (6) The decision must be grounded and shall be brought to the involved parties' attention within 30 days of registering the complaint.
- (7) The supervisory authority may order, if necessary, some or all data processing operations to be suspended until the complaint has been solved, under the provisions of paragraph (5).
- (8) The supervisory authority may appeal to a court of law in order to defend the rights of the data subjects as guaranteed by the present law. The competent court of law is the Court of Bucharest. The complaint addressed to the court of law is exempted from stamp taxes.
- (9) Upon request of the data subjects, for grounded reasons, the court may decide suspending the data processing until the complaint addressed to the supervisory authority has been solved.
- (10) The provisions of paragraphs (4) to (9) also apply to the situation in which the supervisory authority finds out, by any other means, about a violation of the rights of the data subjects, as recognized by the present law.

#### **Article 26: Appeals against the Decisions of the Supervisory Authority**

- (1) The data controller or the data subject may submit an appeal against any decision made by the supervisory authority based on the provisions of the present law, within 15 days from communication, under the sanction of the loss of right, to the competent administrative court. The matter is judged urgently after both parties have been called in front of court. The court's resolution is permanent and irrevocable.

- (2) Personal data processing carried out within the activities set out in Article 2 paragraph (5) are exempted from the provisions of paragraph (1), and also of Articles 23 and 25.

#### **Article 27: Exerting the Investigative Powers**

- (1) The supervisory authority may investigate *ex officio* or as a result of a complaint, any infringement of the data subject's rights, of the controller's obligations and, as the case may be, those of the processors, in order to protect the fundamental rights and freedoms of the data subjects.
- (2) The supervisory authority may not exercise its investigative powers in case a complaint was previously submitted to a court of law, concerning the same infringement and parties.
- (3) In the exert of its investigative powers, the supervisory authority may request any information linked to the processing of data from the data controller and may verify any document or record regarding the processing of personal data.
- (4) The state and professional secrets cannot be invoked in order to prevent the exercise of the supervisory authority's powers, set out by the present law. When the protection of the state or of the professional secrets is invoked, the supervisory authority has the obligation to keep the respective secrets.

#### **Article 28: Rules of Conduct**

- (1) The professional associations have the obligation to elaborate and submit for approval, to the supervisory authority, codes of conduct that contain adequate rules in order to protect the rights of persons whose personal data may be processed by the members of the associations.
- (2) The rules of conduct must contain measures and procedures able to ensure satisfactory protection, taking into account the nature of the data that may be processed. The supervisory authority may impose other specific measures and procedures for the period of time during which the rules of conduct are not adopted.

### **Chapter VII: The Transfer Abroad of Personal Data**

#### **Article 29: Conditions for the Transfer Abroad of Personal Data**

- (1) The transfer to another state of data that are subject to processing or are destined 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.
- (2) The protection level will be assessed by the supervisory authority 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 latter state. In case the supervisory authority notices that the protection level offered by the state of destination is unsatisfactory, it may ban the data transfer.

- (3) Data transferred to another state shall always be subject to preliminary notification to the supervisory authority.
- (4) The supervisory authority may authorize 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. The guarantee must be established through contracts signed by the data controllers and the natural or legal person(s) who have offered the transfer.
- (5) The provisions of paragraphs (2), (3) and (4) do not apply in case the data transfer is based on a special law or on an international agreement ratified by Romania, notably if the transfer is done to the purpose of prevention, investigation or repressing a criminal offense.
- (6) The provisions of the present article 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.

### **Article 30: Situations in which the Transfer is Always Allowed**

The data transfer is always allowed in the following situations:

- a) when the data subject has explicitly given his/her consent for the transfer; if the data transfer is linked to any of the data provided in Articles 7, 8 and 10 the consent must be written;
- b) when it is required in order to carry out a contract signed by the data subject and the data controller, or to apply some pre-contractual measures taken upon the request of the data subject;
- c) when it is required in order to sign or carry out a contract concluded or about to be concluded between the controller and a third party, in the data subject's interest;
- d) when it is necessary for the accomplishment of a major public interest, such as national defense, public order or national safety, carrying out in good order a criminal trial or ascertaining, exercising or defending a right in court, on the condition that the data is processed solely in relation with this purpose, and only for as long as it is required;
- e) when it is required in order to protect the data subject's life, physical integrity or health;

- f) when it is a consequence of a previous request for access to official documents that are open to the public or of a request for information that can be obtained from registers or any other documents of public access.

## **Chapter VIII: Minor Offenses and Sanctions**

### **Article 31: Failure to Notify and Malevolent Notification**

Failure to submit the compulsory notification under the terms set out by Article 22 or Article 29 paragraph (3), as well as incomplete notification or one that contains false information, if the respective maladministration falls short of a criminal offense, are considered minor offenses liable to a fine of 5 million to 100 million ROL (Romanian currency – lei).

### **Article 32: Illegal Processing of Personal Data**

The processing of personal data by a controller or by an empowered person of the data controller, breaching the provisions of Articles 4-19, or while disregarding the rights set out in Articles 12- 15 or in Article 17 is considered a minor offense if the respective maladministration falls short of a criminal offense and is fined from 10 million to 250 million ROL.

### **Article 33: Failure to Fulfill the Obligations Regarding the Confidentiality and Enforcement of Security Measures**

Failure to fulfill the obligations regarding the enforcement of the security measures provided by Articles 19 and 20 and the confidentiality is a minor offense, if the respective maladministration falls short of a criminal offense and is liable to a fine of 15 million to 500 million ROL.

### **Article 34: Refusal to Supply Information**

The refusal to supply the requested information or documents to the supervisory authority in the exercise of his investigative powers set out by Article 27 is considered a minor offense, if the respective maladministration falls short of a criminal offense and is liable to a fine of 10 million to 150 million ROL.

### **Article 35: Ascertaining Minor Offenses and Applying Sanctions**

- (1) Ascertaining a minor offense and applying sanctions are carried out by the supervisory authority, which may delegate these powers on to a member of

staff and also by the empowered representatives of the bodies with supervising or control powers in their legal competence.

- (2) The provisions of the present law regarding the minor offences are complementary to those of the Government Ordinance No. 2/2001 on the legal framework of minor offenses, when the present law does not state otherwise.
- (3) The minutes that report minor offenses and establish the sanctions may be appealed against in the administrative section of a court of law.

## **Chapter IX: Final Provisions**

### **Article 36: Entering into force**

The present law enters into force on the date of its publication issue in the Official Journal of Romania, Part I and will be enforced within three months of its entering into force.

The Senate adopted the present law during the session of the 15<sup>th</sup> of October 2001, in accordance with the provisions of Article 74 paragraph (2) of the Romanian Constitution.

President of the Senate  
**NICOLAE VĂCĂROIU**

The present law was adopted by the Chamber of Deputies in the session of the 22<sup>nd</sup> of October 2001, in accordance with the provisions of Article 74 paragraph (2) of the Romanian Constitution.

President of the Chamber of Deputies  
**VALER DORNEANU**

Published in the Official Journal of Romania, Part I, No. 790/12 December 2001

