REPUBLIC OF ALBANIA
COMMISSIONER FOR PROTECTION OF PERSONAL DATA
OFFICE OF COMMISSIONER

DECISION

No 2, Dated 10/03/2010

ON

DETERMINING THE PROCEDURES FOR THE ADMINISTRATION OF REGISTRATION OF DATA, ENTERING THE DATA, THEIR PROCESSING AND RETRIEVAL

In reliance on the Law No 9887, dated 10.03.2008 *"On Protection of Personal Data"*, on decisions of the Parliament of Albania No 211, dated 11.09.2008 "*On election of the Commissioner for Protection of Personal Data"*, no 225, dated 13.11.2008 "*On the approval of the organic structure and categories of job positions of the office of the Commissioner for Protection of Personal Data"*, as well as abiding by the obligations set out in point 6 of Article 27, of the law mentioned above, I

DECIDED:

determining the procedures for the administration of registration on the data, entering of the data, their processing and retrieval in accordance with the requirements of the law No 9887, dated 10.03.2008 "On Protection of Personal Data", as follows:

I. Administration of registration

1. **Storing and preserving the data** shall be done only for one or many specific clear and legitimate aims.
   a) The data may be stored for one or many specific aims, for legitimate aims declared clearly, and their processing shall be done only based on these aims.
   b) In accordance with this rule:
      i. every individual has to know the reason of collection and storing his data;
      ii. the aim for which the data are collected should be legitimate;
      iii. you should be aware for the administration of the data you possess.

2. **The data shall be stored** in a correct and careful manner, being accurate, comprehensive and updated.
   a) The individual shall be granted all rights provided for in the law *"On Protection of Personal Data"*.
   b) In the interest of your activity or business, you should obtain accurate data for the effects of efficiency and effective decision-making.
   c) In accordance with this rule, you should make sure that:
      i. your official and computer based procedures be sufficient for appropriate verifications to ensure a high level of accuracy of data;

      ii. the general requirements for storing the updated personal data shall be considered completely;

      iii. appropriate procedures must be imposed, applied, implemented, including the periodic review and the control to ensure that all data had been kept updated.

3. **The data shall be kept no longer** than necessary for the purpose for which they have been collected or further processed.
   a) The controllers of the data are responsible and they should be clear about the time frame within which the data should be stored and the reason why the information is being kept;
   b) You should appoint a person responsible for ensuring that the files or databases are regularly monitored in order for the personal data not to be longer than necessary;
   c) You must have:
      i. a clear policy about the timeframe for keeping all the personal data in accordance with instructions of the Commissioner;

      ii. clear-cut and approved rules for the management, official procedures, computer procedures being applied for the implementation of such policy.

4. **The right to access** by the entity of the data

   a) every individual about whom you keep personal data shall be entitled:

      i. to be given a copy of the data that you keep about him or her;

      ii. to know the category of the data and the aim of their processing;

      iii. to know the identity of those to whom you have disseminated data;

      iv. to know the source of data, as long as this is not at variance with the public interest;

      v. to know the logic, and the arguments included in automatic decisions;

vi. to be informed about the data in the form of opinions, unless such opinions have been provided confidentially or in secrecy, even in cases where the fundamental human rights suggest that they should have access to the data in question.

b) The controllers shall have clear coordination procedures in order to make sure that all the manual files and the computer files have been controlled about data in connection with which the request to access has been made;
c) in order to file a request to access, the entity of the data shall:
   i. file a written application (which may include also application by mail);

   ii. provide any detail which may be necessary to assist in the identification and in finding out, localizing all information which you may keep about him/her;

d) In response to the request for access, you shall:
   i. provide individuals with information very accurately and within 30 days from receiving the request;

   ii. offer clear information about the persons, such as every code needs to be explained.

e) If you do not possess any information with regard to the request filed by the individual, you shall make this known to him within 30 days;
f) If you restrict the right of individuals to access in compliance if one of the few restrictions provided for in the law, you shall inform the entity of the data in writing within 30 days and included in that statement shall be the grounds of refusal. At the same time the individual shall be informed about his right to complain with the Commissioner of the protection of data with regard to the refusal or to file a request to control the exclusion in the concrete case.
g) Every individual about whom a controller of data keeps personal data shall also have other rights in addition to those foreseen in this law, that is the right to access. Included there shall be the right to request the deletion or correct indication of any inaccurate information, the right to oppose, the right to complain with the Commissioner for the protection of data etc.

5. Security of data **(Article 27)**

a) The appropriate security measures shall be taken against unauthorized access, disclosure or destruction of data, as well as against their accidental loss. High security standards are essential for all the personal data;
b) A minimum security standard shall include:
   i. the right of IT specialist to restrict the number of personnel in accordance with the appropriate procedures;

   ii. encoding the computer systems by passwords;

iii. keeping the information on the screen of the computers or in the manual files, hidden from unauthorized persons seeking to get to know the data;

iv. making all the technical arrangements to safeguard the data, guaranteed technical acts for finding, tracking and determining the acts with the data through the specific elements of the computer program being applied, as well as the awareness of the personnel about this;

v. appropriate destruction and disposal to the appropriate place of all acts and documentation containing unnecessary personal data, if the aim of collection, storing and processing them as well as the timeframe set to this effect has expired (it must be understood that the entire process from the collection to the destruction of data, including the latter, is considered to be processing and bears the same responsibility for the controllers in the event of violation of rules);

vi. appointing a certain person to be responsible for the safety of data and updating them;

vii. safeguarding the capability of general and specific instructions of the Commissioner for the protection of personal data about the safety of personal data.

6. Transfer of data

a) Where the issue is about the level of sufficiency of protection of personal data, the type of personal data shall be considered, as well as the aim of use and duration of processing of data, legislation of the transferring country and the legislation of the recipient country, including here issues about the protection of personal data of foreign citizens and the measures for the protection of personal data made use in these countries. The decision in these cases shall be based on the following points:
   i. whether the data have been used for the purpose for which they have been transferred, whether the aim may be changed, but only with the consensus of the controller of the data having transferred data, based on the consent of the person connected to the data;

   ii. whether the individual may learn the aim for which his/her data had been used, to whom the data had been given, and whether they can be rectified or deleted in appropriate cases, if they are collected carelessly or have not been updated, and in this case, due to confidentiality of the procedure, the implementation of an international agreement is needed;

   iii. whether a foreign controller applies the same procedure, means and measures for the protection of personal data;

   iv. whether and authorized person has been appointed, capable of providing information about this field;

v. whether a foreign recipient may transfer the data only under the condition that the other foreign country where the data transferred to ensure an efficient protection of the data of foreign citizens;

vi. whether an efficient legal protection has been insured for all the personal data that are transferred.

II. Entering the data (Articles 5,6,20,22,27)

1. **Reception, collection**, storing as well as entering the data into installed and specific computer programs or databases, as well as setting up the manual files, for the management of your activity, shall be conducted fairly.

2. **In order to obtain data** in the fair way, the entity of the data shall, at the time when the data are being collected, be informed about:

   a. name of controlling entity;
   b. purpose of collection of data;
   c. identity of any representative set for the purpose of the law;
   d. persons for categories of persons whose data may be discovered;
   e. existence of the right to access their personal data;
   f. the right to rectify the data being inaccurate or processed in an unfair way;
   g. cases when the personal data have not been taken from the entity of data, or they have not been taken at the time when the data of the entity had been processed for the first time, or at the time of declaration of a third party, and all these data should be insured to the entity of data;
   h. name of controlling entities of data by which these data have been received, as well as the name of controlling entities to whom these data are disseminated;

3. **The entering and processing of data** shall be determined as a priority subject matter of the contract entered into between the controlling entity and the processors, based on the aim for which they shall be requested, collected, entered or processed manually or electronically.

4. **The contract shall contain** the conditions and the criteria based on which the data are requested, collected, entered into or processed manually or electronically by the processor of the data provided for in the contract.

5. **The contract shall provide** for the technical conditions of the security of the data, as well as provide for these data to be deleted at the moment of expiry of the contract.

6. **The controlling entities** shall take the necessary measures of guaranteeing the implementation of conditions and criteria foreseen in the contract by the controllers.

III. Processing of data (Articles 5,6,7)

1. **To the effect of the fair processing**, the personal data shall be taken in a fair way and the entity of the data shall have given his consent for the processing.
2. **The data may be processed** even without the consent of entity of the data where the processing is necessary for one of the following reasons:
    a) enforcement of the contract where the entity of the data is a party;

    b) where processing is a legal obligation;

    c) to prevent impairing the health of the entity of the data;

    d) to prevent serious losses or damages to the property of the entity of the data;

    e) to protect the high interests of the entity;

    f) if processing is done within the legal framework of the activities of preventing and criminal prosecution as well as in the field of defence and nation security, where the processing is conducted by the competent authorities determined by law;

    g) for the accomplishment of another function of public nature for public interest by a person;

    h) for the purpose of legitimate interests of the controller of the data, unless in a separate case the processing of the data is not justified.

3. **To the effect of having a fair processing** of the sensitive data, these data shall be taken in a fair way and at least one of the following conditions shall be met:
    a) The entity of the data has expressed his own consent, readable and in written form for the processing of his sensitive data, after being informed in full and understandable way about the aim for the data. When these entities are not able to do such a thing, due to physical or mental impossibility or due to age, the consent shall be given by one of the parents or the legal custodian (**account shall be taken of the principle that the consent of the entity cannot legitimize which is forbidden by law**);
    b) where the entities have not expressed that consent, but processing is necessary for one of the following reasons:
        i. for meeting or performing an obligation or any right by the controlling entities in the field of employment provided for by law;

        ii. to prevent impairing the health of the entity of the data or another person, or violation of his personality;

        iii. to prevent the loss or damage to property, and to protect the high interests of the entity of the data, in those cases where consent cannot be provided due to different reasons;

iv. to prevent impairing the health of another person or violation of his personality, damages to the property of the third person, in those cases where the consent had been hidden;

v. upon being done by a non-profit making organization, within its members or persons having a connection to this organization;

vi. when the processed data are public as a result of the initiative of the entity of the data;

vii. to the effect of having legal advice, or having a connection to legal proceedings;

viii. for medical purposes;

ix. for the purpose of paying a tax obligations;

x. in connection with social well-being.

4. **The data shall be sufficient,** appropriate and not superfluous .

a) Make sure that you have requested and kept only the minimum of the personal data which you need for reaching the purpose;
b) Establish specific criteria by which you are going to evaluate what is appropriate, necessary and not superfluous and apply and use these criteria for each unit of information of personal data for the purposes that they have been collected or kept;
c) Make sure that the requested, collected, stored or processed information is:
   i. sufficient with regard to the purpose that you have requested;

   ii. appropriate with regard to the purpose for which you have requested it;

   iii. not superfluous with regard to the purpose for which you have requested it.

d) Undertake a periodic revision concerning the importance of the personal data requested by the entities of data through various channels through which the information has been collected, that this, the form, address, Internet etc. as well as an inspection has to be undertaken referring to the above basic criteria of any personal information already been kept.

IV. Disclosure (dissemination) of the data

1. **Disclosure or dissemination of the data** shall be in compliance with the aim for which they have been collected, or processed;

2. **The concrete evidence** of compliance may be:

a) whether the use of data is done referring to the purpose for which they are kept;

b) whether you disclose or disseminate the data according to this purpose or purposes;

c) whether you disclose or disseminate the data of the entity of the data or other controlling entities with the consent of the entity of the data;

d) whether disclosure or dissemination is done in accordance with requirements or seen in law;

e) whether the processor of the data appointed by you processes the data based on the law, on this decision and all the instructions of the Commissioner.

V. Confidentiality (Article 28)

The controllers, processors and persons being informed about the processed data, in the course of carrying out their functions, shall be obliged to preserve the confidentiality and reliability even after the completion of the function. These data shall not be disseminated, provided for the case is foreseen in the law.
In all the cases, this implies that they shall not disclose to any unauthorized person personal data which they know or learn about them in the course of work. The obligation to preserve the confidentiality lasts endlessly. The obligation does not end if persons do not assume their functions. The infringement of the obligation of confidentiality consists a criminal offence provided for in the Criminal Code (Article 23).

Responsible for abiding by the requirements of this decision shall be all public and private controllers.

This decision shall enter into effect on 10.03.2010 and shall be published in our official website, www.kmdp.al

COMMISSIONER

Flora ÇABEJ (POGAÇE)