LAW No.03/L – 172

ON THE PROTECTION OF PERSONAL DATA

Assembly of Republic of Kosovo,

Based on Article 65 (1) of Constitution of the Republic of Kosovo,

Approves

LAW ON THE PROTECTION OF PERSONAL DATA

CHAPTER I
GENERAL PROVISIONS

Article 1
Purpose of the Law

This Law determines the rights, responsibilities, principles and measures with respect to the protection of personal data and sets up an institution responsible for monitoring the legitimacy of data processing.

Article 2
Definitions

1. Terms used in this Law shall have the following meanings:

1.1 **Personal data** - any information relating to an identified or identifiable natural person (data subject); 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 or her physical, physiological, mental, economic, cultural or social identity;

1.2 **Processing of personal data -** any operation or set of operations which is performed upon personal data whether or not by automatic means such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

1.3 **Automated data processing -** the processing of personal data using information technology means;

1.4 **Data controller** - any natural or legal person from the public or private sector who individually or jointly with others determines the purposes and means of the processing of personal data, or a person designated by law that also determines the purposes and means of processing;

1.5 **The data processor**- any natural or legal person or another person from the public or private sector that processes personal data on behalf and for the account of the data controller;

1.6 **Data recipient**- any natural or legal person or any other person from the public or private sector to whom personal data are disclosed;

1.7 **Filing system**- any structured set of personal data which are accessible according to specific criteria irrespective of whether the set is centralized, decentralized or dispersed on a functional or geographical basis;

1.8 **Filing system catalogue** - a detailed description of the structure and the content of filing systems;

1.9 **Register of filing systems** - a register allowing a detailed overview of existing filing systems;

1.10 **The data subject's consent** - any unambiguous, freely given specific and informed indication of the data subjects wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed;

1.11 **Written consent of the data subject -** the consent from sub-paragraph 1.10 of paragraph 1 of this Article, with the addition that the data subject has to put his or her signature or sign under his or her written consent to process his or her data.

1.12. **Oral consent or other appropriate consent of the data subject -** the consent from sub-paragraph 1.10 of paragraph 1 of this Article given verbally, by means of telecommunication or by any other appropriate means from which it can clearly be concluded that the data subject has given his or her consent;

1.13. **Blocking** - the prohibition of further data processing. Decision to block personal data has to be properly indicated and has to remain attached to the personal data for as long as the reasons for blocking exist;

1.14. **Classification of personal data** - the labelling of personal data to indicate their sensitive nature. If data are classified conditions have to be laid down under which a user can process them. The classification has to remain with the sensitive personal data until they are deleted, erasured, destroyed or anonymized;

1.15 **Anonymity** -the alteration of personal data in such a way that they can no longer be linked to the data subject or where such a link can only be made by disproportionate efforts, expense or use of time;

1.16 **Sensitive personal data** - any personal information revealing racial or ethnic origin, political or philosophical opinions, religious beliefs, trade-union membership or any information on health status and sex life, any entries in or removals from criminal records or records on minor offences that are kept on the basis of the law. Biometric characteristics are also considered as sensitive personal data if they enable the identification of a data subject in connection with any of the aforementioned circumstances mentioned in this point;

1.17 **Connecting code** - a personal identification number or any other specific identification number defined by law relating to an individual that can be used to disclose or retrieve personal data from filing systems in which the connecting code is also processed;

1.18 **Biometric characteristics** - any physical, psychological and behavioural characteristics which all individuals have but which are unique and permanent for each individual if in particular they can be used for identification of an individual, such as finger prints, papillary ridges of a finger, iris, retina, facial characteristics and DNA.

1.19 **National Agency for the Protection of Personal Data (hereinafter the Agency) –** an independent agency, responsible for supervision of implementation of rules for personal data protection.

Article 3
Principles of Data Processing

1. Personal data shall be processed fairly and lawfully without violating the dignity of data subjects.

2. Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and /or further processed.

3. Personal data are collected only for specified, explicit and legitimate purposes, and may not be further processed in a way incompatible with these purposes, unless otherwise provided by law.

4. Personal data must be accurate and kept up to date. Prior to collecting personal data the data controller verifies the accuracy of personal data by examining an identity document or any other suitable public document of the data subject.

5. Personal data may only be stored for as long as necessary to achieve the purpose for which they were collected or further processed. On completion of the purpose of processing, personal data shall be erased, deleted, destroyed, blocked or anonymised, unless otherwise provided by the Law on Archive Material and Archives or any other relevant law.

Article 4
Scope of activity

1. This Law shall apply to the processing of personal data by public and private bodies. This Law shall not apply to the processing of personal data if it is done for purely personal purposes.

2. This law shall also be applied in diplomatic and consular offices as well as any other official representative offices of the Republic of Kosovo abroad.

3. This Law shall also apply to a data controller who is not established in the Republic of Kosovo but who for the purposes of processing personal data makes use of equipment, automatic or otherwise in the Republic of Kosovo, unless such equipment is used only for purposes of transit through the territory of Kosovo. In these circumstances the controller must designate a representative established in Kosovo.

4. Paragraph 2 of the Article 16, Articles 17, 18 and 20 and the Chapter V (five) of this Law shall not apply to personal data which are processed by media for the purpose of informing the public and for the purposes of artistic and literary expressions.

5. Articles 17, 18 and 20 of this Law shall not apply to personal data, which are processed by political parties, trade unions, associations or religious communities in relation to their members.

CHAPTER II
LEGITIMACY OF DATA PROCESSING

Subchapter A
Legal grounds and purposes

Article 5
Lawful processing of personal data

1. Personal data may only be processed if:

1.1 the data subject has given his or her consent;

1.2 the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

1.3 the processing is necessary for compliance with a legal obligation to which the controller is subjected;

1.4 the processing is necessary in order to protect the vital interests of the data subject;

1.5 the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

1.6 the processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

Article 6
Processing of sensitive personal data

1. Sensitive personal data may only be processed in the following cases:

1.1 if the data subject has given the consent;

1.2 if the processing is necessary for the purposes of fulfilling the obligations and specific rights of a data controller in the field of employment in accordance with relevant laws which also provide appropriate safeguards for the rights of the data subject;

1.3 if the processing is necessary to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving his or her consent pursuant to point 1 of this paragraph;

1.4 if they are processed for the purposes of legitimate activities by institutions, societies, associations, religious communities, trade-unions or other non-profit organizations with a political, philosophical, religious or trade-union aim, but only if the processing concerns their members or data subjects in regular contact with them in connection with such aims, and if they do not disclose such data to others without the written consent of the data subject;

1.5 if the data subject has made them public without evidently or explicitly restricting their use;

1.6 if they are processed by health-care workers and health-care staff in compliance with relevant laws for the purposes of protecting the health of the public and individuals and the management or operation of health services;

1.7 if the processing is necessary for asserting or opposing a legal claim;

1.8 if they are processed in accordance with relevant law for reasons of substantial public interest.

Article 7
Protection of sensitive personal data

1. Sensitive personal data must be specifically protected and classified to prevent any unauthorized access and use, except in instances from sub-paragraph 1.5 of paragraph 1 of Article 6 of this Law.

2. When sensitive personal data are transmitted over telecommunications networks they shall be considered as suitably protected if they are encrypted to ensure their illegibility and non-recognition.

Article 8
Automated Decision-Making

1. Automated decision-making which might produce legal effects or significantly affect the data subject and which is solely based on automated data processing intended to evaluate certain personal aspects, especially the data subject's performance at work, credit-worthiness, reliability, conduct or compliance with certain conditions, shall only be permitted if the decision:

1.1 is taken during the conclusion or performance of a contract, provided that the request to conclude or implement a contract submitted by the data subject has been satisfied or if there exist appropriate measures to protect his or her legitimate interests, such as arrangements enabling the data subject to object to such decisions or to express his or her position;

1.2 is provided by law which also provides measures to protect the legitimate interests of the data subject, particularly the possibility of legal remedy against such decisions.

Article 9
Processing for historical, statistical and scientific-research purposes

1. Irrespective of the initial purpose of collection, personal data may be further processed for historical, statistical and scientific-research purposes.

2. If personal data are further processed for purposes mentioned under paragraph 1 of this Article they shall be anonymized unless otherwise provided by law or if the data subject has given his or her prior written consent.

3. Personal data disclosed to data recipients in accordance with paragraph 2 of this Article shall on completion of processing be destroyed or deleted, unless otherwise provided by law. Following the destruction or deletion the data recipient shall without delay inform in writing the data controller who disclosed the data about when and how the data were destroyed or deleted.

4. The results of processing from paragraph 1 of this Article, shall be published in anonymised form, unless otherwise provided by law, unless the data subject has given his or her prior written consent for the publication in a non-anonymised form or unless the prior written consent for such publication has been given by the legal heirs of the deceased individual under this Law.

Article 10
Information to be given to the data subject

1. If personal data are collected directly from the data subject, the data controller or his representative must provide the data subject at the moment of collecting the data with at least the following information, except where the data subject is already acquainted with it:

1.1. identity of the data controller and his or her possible representative such as personal name(s), title or respectively official name, address or seat and where applicable electronic address and phone number;

1.2. the purpose of the processing;

1.3. information of whether the replies to the questions are compulsory or voluntary as well as consequences in case of failure to reply;

1.4. information on the right to access, transcription, copy, supplement, correction, block and erase of personal data.

2. If in view of the special circumstances of collecting personal data from paragraph 1 of this Article there is a need to ensure lawful and fair processing of personal data, the data controller from paragraph 1 of this Article, must also provide the data subject with the additional information, if the data subject is not yet acquainted with it, as following:

2.1 information as to the recipients or the categories of recipients of the personal data;

2.2 the legal basis of the processing operations;

3. If personal data were not collected directly from the data subject, the data controller or his representative must provide the data subject with the following information, except where the data subject is already acquainted with it:

3.1 identity of the data controller and his or her possible representative such as personal name(s), title respectively official name and address or seat and where applicable electronic address and phone number;

3.2 the purpose of the processing;

3.3 information on the right to access, transcribe, copy, supplement, correct, block and erase personal data;

3.4 the origin of the data.

4. If in view of the special circumstances of collecting personal data from paragraph 3 of this Article, there is a need to ensure lawful and fair processing of personal data the data controller from paragraph 3 of this Article must also provide the data subject with the following additional information and in particular:

4.1 information on the categories of personal data collected;

4.2 information as to the recipients or the categories of recipients of the personal data;

4.3 the legal basis of the processing operations.

5. Information from paragraphs 3 and 4 of this Article shall not be given if for historical, statistical or scientific-research purposes it would prove impossible or would incur large costs or disproportionate efforts or would require a large amount of time, or if the processing or disclosure of personal data is expressly provided for by law.

Article 11
Use of connecting codes

1. Personal data contained in filing systems in the areas of health must not be collected and processed by using only a connecting code.

2. The connecting code may exceptionally be used to obtain personal data if this is the only data element in a specific case to protect the life or body of data subjects. Following the use of a connecting code an official annotation or other written record attached to the personal data must be made thereof without delay.

3. Personal data in the land register and the commercial register may be collected and processed by using only the connecting code.

Article 12
Disclosure of personal data

1. A data recipient shall carry forward the cost for any legal disclosure of data by the data controller if not provided otherwise by law.

2. Information from Central Population Register and the Register of Records of Permanently and Temporarily Registered Residents shall be disclosed to recipients showing a legitimate interest. The following information contain: personal name and permanent or temporary address of a data subject.

3. When disclosing such information the data controller must ensure that the following information is registered: which personal data were disclosed, to whom, when and on what legal basis. Such information about the disclosure has to be kept with the data subject's data for as long as they are stored.

Article 13
Protection of personal data of deceased individuals

1. Personal data of deceased individuals may only be disclosed to recipients authorized by law.

2. Irrespective of paragraph 1 of this Article, personal data of deceased individuals may be disclosed to their legal heirs, if they demonstrate a legitimate interest and the deceased individuals did not prohibit in writing the disclosure of such personal data.

3. Personal data of deceased individual may be disclosed for historical, statistical or scientific-research purposes if the deceased individual has preliminarily allowed in writing the disclosure of such data, unless otherwise provided by law

4 If the deceased individual had preliminarily allowed the disclosure of his/her data, the legal heirs may allow in writing the disclosure of such data, unless otherwise provided by law.

Subchapter B
Obligations of data controllers and data processors

Article 14
Security of data processing

1. Security of personal data comprises appropriate organizational, technical and logic-technical procedures and measures to protect them and to prevent any accidental or deliberate unauthorized destruction, disclosure, modification, access or use of data or their accidental or deliberate loss:

1.1 by protecting premises, equipment and systems software, including access control;

1.2 by protecting software applications used to process personal data;

1.3 by preventing any unauthorized access to or reading of personal data during their storage and transmission including the transmission via telecommunications means and networks;

1.4 by ensuring effective methods of blocking, destruction, deletion or anonymization of personal data;

1.5 by enabling subsequent determination of when personal data were entered into a filing system, accessed, modified, disclosed, destroyed, used or otherwise processed, and who did so, for the whole storage period.

2. If personal data are processed via telecommunications networks it must be ensured that the processing takes place within the limits foreseen by law. Also the hardware, the systems software and the software applications must ensure an appropriate level of data protection.

3. The procedures and measures to protect personal data must be adequate and kept up to date taking into account the nature of the personal data to be protected and the risks represented by the processing of such data.

4. Functionaries, employees and other individuals performing tasks related to the processing of data including the data controller are obliged, that during and after the contracted work, to protect the confidentiality of personal data with which they become familiar.

Article 15
Contractual processing

1. A data processor may be entrusted with the processing of personal data by written contract if he or she is registered in the Republic of Kosovo to perform such activities pursuant to procedures and measures foreseen by Article 14 of this Law.

2. A data processor may only act within the limits of the data controller’s authorizations and may not process personal data for any other purpose. Mutual rights and obligations shall be arranged by written contract which must also contain a detailed description of the procedures and measures pursuant to Article 14 of this Law.

3. The data controller shall oversee the implementation of procedures and measures pursuant to Article 14 of this Law. This may also include ad-hoc visits to the premises where the personal data processing takes place.

4. In the event of a dispute between the data controller and the data processor, the data processor shall immediately at request of the data controller return all data in his or her possession. The data processor is not allowed to keep copies and to process them any further.

5. In the event of cessation of a data processor's activities, personal data shall immediately be returned to the data controller.

Article 16
Obligation to secure personal data

1. Data controllers and data processors shall care at any time that personal data are protected in the manner set out in Article 14 of this Law.

2. Data controllers and data processors shall describe in their internal acts the procedures and measures established for the security of personal data and shall nominate in writing competent persons who are responsible for filing systems and those who, due to the nature of their work, shall process personal data.

Subchapter C
Filing systems

Article 17
Filing system catalogue

1. A data controller shall establish for each filing system a detailed description called filing system catalogue containing:

1.1 title of the filing system;

1.2 identity of the data controller and his or her representative. For natural persons: personal name(s), permanent or temporary address where activities are performed or permanent or temporary address of residence, and where applicable phone number and email address. For independent traders: their official name(s), registered office, seat and registration number and where applicable, phone number and email address. For legal persons: name of the founder, title or registered office, address or seat, registration number and where applicable, phone number and email address;

1.3 legal basis for the data processing;

1.4 the categories of data subjects

1.5. the categories of personal data in the filing system;

1.6 purpose of processing;

1.7 intended duration of storage of personal data;

1.8 restrictions of the rights of data subjects and the legal basis for such restrictions;

1.9 data recipients or categories of data recipients contained in the filing system;

1.10 information on whether personal data have been or are to be transferred to another country, where, when and to whom, and the legal grounds for such transfers;

1.11 a general description of the procedures and measures pursuant to Article 14 of this Law;

1.12 data of linked filing systems from official records and public books.

2. The data controller must ensure that the content of the filing system catalogue is accurate and kept up to date.

Article 18
Notification of the Agency

1. Data controllers shall provide the Agency in writing or by electronic means with information from the points of paragraph 1 of Article 17 of this Law at least twenty (20) days prior to establishing a filing system or prior to the entry of new categories of personal data.

2. Data controllers shall inform the Agency about any modifications to the information from paragraph 1 of this Article no later than eight (8) days from the date of modification.

Article 19
Prior checking

1. Following the receipt of the notification, the Agency checks whether the processing operation is likely to present specific risks to the rights and freedoms of the data subjects by virtue of the nature of the personal data being processed and the scope or the purposes of the data processing.

2. The Agency shall deliver its opinion within three (3) weeks following receipt of the notification. This period may be suspended until the Agency has obtained any further information that it considers necessary. Depending on the complexity of the matter, this period may be extended up to three (3) months by decision of the Agency which has to be notified to the data controller prior to the expiry of the three (3) month period.

3. If the opinion has not been delivered by the end of the three (3) month period or any extension thereof, it shall be deemed to be favourable.

4. If the Agency is of the view that the notified processing may involve a breach of data protection rules, it shall make appropriate proposals to avoid such breaches.

5. The data controller has to respect any proposals and decisions issued by the Agency to ensure lawful data processing.

Article 20
Register

1. The Agency shall establish and maintain a Register of Filing Systems containing information from Article 18 of this Law defined in accordance with its internal procedures.

2. The Register shall be managed by using information technology means and shall be published on the website of the Agency.
3. The rules on the internal procedures from paragraph 1 of this Article shall be defined in a sub-legal act.

CHAPTER III
RIGHTS OF THE DATA SUBJECT

Article 21
Consultation of the Register

Every person has the right to consult the Register of Filing Systems kept by the Agency and make copies or transcribe details free of charge.

Article 22
Right of access

1. Every data subject can consult the filing system catalogue kept by the data controller. The data controller shall provide the data subject at his or her request with the following information:

1.1 personal data stored about him or her;

1.2 the purposes of the processing and the categories of personal data being processed;

1.3 the legal basis for the processing ;

1.4 the origin of the data;

1.5 data recipients or categories of data recipients and when and on which basis and for what purposes the data subject's data were disclosed including data recipients in other countries;

1.6 technical procedures and information regarding the logic included in decision-making, if applicable.

2. An extract issued by the data controller about the personal data stored by him or her shall not replace the document or certificate, and this is indicated on the extract.

Article 23
Procedure for access

1. Data subjects can ask data controllers in regular intervals to consult, transcribe and copy information related to them pursuant to Article 22 of this Law and can ask for an extract or a copy of this information. This request can be lodged orally, in writing or by electronic means.

2. Within fifteen (15) days data controllers have to confirm in writing the receipt of the data subject's request, or within the same period of time they have to inform the data subject in writing of the reasons why the request cannot be accommodated.

3. Within thirty (30) days following receipt of the request data controllers shall provide the data subject with an extract or a copy of any information requested according to paragraph 1 of Article 22 of this Law.

4. If the data controller fails to act in accordance with paragraphs 1, 2and 3 of this Article the data subject can consult the Agency.

5. Costs relating to any requests lodged by data subjects from this Article shall be borne by the data controller.

Article 24
Right to supplement, correct, block, destroy, erase, delete and object

1. At the data subject's request the data controller must supplement, correct, block, destroy, delete or erase personal data which the data subject proves as being incomplete, inaccurate or not up to date, or if they were collected or processed contrary to law.

2. At the data subject's request the data controller must immediately inform all data recipients and data processors to whom personal data were disclosed about the measures taken according to paragraph 1 of this Article. The data controller is not obliged to do this if this would incur large costs.

3. Data subjects whose personal data are processed in accordance with sub-paragraphs 1.5 and 1.6 of Article 5 of this Law shall have the right to object at any time to the processing of their data. The data controller shall accept the objection if the data subject demonstrates that the conditions for processing have not been fulfilled pursuant to sub-paragraphs 1.5 and 1.6 of Article 5 of this Law. In this case the personal data of the data subject may no longer be processed.

4. If the data controller does not accept the objection from paragraph 3 of this Article, the data subject may ask the Agency to decide on whether the processing is in accordance with sub-paragraphs 1.5 and 1.6 of Article 5 of this Law. The data subject may lodge such request within fifteen (15) days upon receipt of the data controller's objection.

5. The Agency shall decide on requests from paragraph 4 of this Article within two (2) months upon receipt. The lodging of the request shall suspend the processing of the personal data.

6. Costs for measures from paragraph 5 of this Article shall be borne by the data controller.

Article 25
Procedure of supplementing, correction, blocking, erasure, destruction, deletion and objection

1. Any request or objection according to Article 24 of this Law can be lodged orally, in writing or by electronic means.

2. Within fifteen (15) days data controllers shall supplement, block, correct, erase, destroy or delete personal data in question following receipt of the request. They shall inform in writing the data subject within the same period of time about the reasons of refusal. Within the same period of time data controllers shall decide on an objection raised by the data subject regarding the processing of his or her data.

3. If data controllers fail to act pursuant to paragraph 2 of this Article, the data subject can consult the Agency.

4. If the data controller concludes on his or her own that the personal data are incomplete, inaccurate or not up to date, he or she shall supplement or correct them and inform the data subject accordingly, unless otherwise provided by the law.

5. All costs relating to the completion, correction, blocking, destruction, erasure and deletion of personal data and of the notification or decision regarding the objection shall be borne by the data controller.

Article 26
Judicial protection of the rights of the Data Subject

1. Data subjects who find that their rights provided for by this Law have been violated may request judicial protection for as long as such violation lasts. This is without prejudice to the data subject's right to consult and complain with the Agency according to this Law.

2. If the violation from paragraph 1 of this Article ceases, the data subject may file a suit in the competent Court to rule that the violation existed if he or she is not provided with other judicial protection in relation to the violation.

Article 27
Temporary Prohibition of Processing the Personal Data

In a suit submitted due to violations of rights from Article 24 of this Law, data subjects may ask the court until a final decision is issued, to bind the data controller, to prevent any kind of processing of the disputed personal data, if their processing could cause irreparable damage to the data subject, while the postponement of processing should not be contrary to public interests and neither is there any danger of greater irredeemable damage being done to the opposing party.

Article 28
Restrictions and exemptions

1. The rights of the data subject from Article 10, Articles 22 and 24 of this Law and the obligation to publish the register of filing systems from paragraph 2 of Article 20 of this Law may exceptionally be restricted by law for reasons of:

1.1 national security;

1.2 national defence;

1.3 public security;

1.4 the prevention, investigation, detection and prosecution of criminal offences, or for breaches of ethics for regulated professions;

1.5 an important economic or financial interest of the Republic of Kosovo including monetary, budgetary and taxation matters;

1.6 the monitoring, inspection or regulatory functioning connected even occasionally with the exercise of official authority in cases referred to sub-paragraphs 1.3, 1.4 and 1.5 of this paragraph;

1.7 the protection of the data subject or of the rights and freedoms of others.

2. Measures from paragraph 1 of this Article may only be taken to the extent necessary to achieve the purpose for which the restrictions were introduced.

CHAPTER IV
INSTITUTIONAL PROTECTION OF PERSONAL DATA

Subchapter D
National Agency for the Protection of Personal Data

Article 29
The Status of the Agency

1. The National Agency for the Protection of Personal Data is an independent agency in charge of supervising the implementation of data protection rules. Its members act independently in accordance with this Law and must not take any instructions from third parties. It shall respond to the Kosovo Assembly.

2. The Agency shall in particular:

2.1. give advice to public and private bodies on data protection related questions;

2.2. decides on complaints of the data subject;

2.3. carry out inspections and audits;

2.4. inform the public about issues and developments in the field of data protection; and

2.5. promote and uphold the fundamental right to data protection.

Article 30
Organization of the Agency

1. The Agency is presided by a Council consisting of the Chief State Supervisor and four (4) National Supervisors. (Hereinafter: the Supervisors). At least one of the Council members must have a university degree in law. Decisions of the Council shall be taken by simple majority.

2. The Chief State Supervisor shall represent the Agency, organize and coordinate its work.

Article 31
Appointment of the Chief National Supervisor

1. The Chief State Supervisor may be appointed a person who has university education and five (5) years of professional working experience.
2. The Chief State Supervisor shall be appointed by the National Assembly on the proposal of the Kosovo Government for a period of five (5) years and may be reappointed once.

Article 32
Appointment of the National Supervisors

1. Persons who have university education and three (3) years of professional working experience may be appointed as National Supervisors.

2. National Supervisors shall be appointed by the Assembly of Kosovo on the proposal of the Government of Kosovo for a period of five (5) years. They may be reappointed once.

Article 33
The deputy of the Chief National Supervisor

The Chief State Supervisor shall choose among the National Supervisors his or her deputy, who shall replace him or her during his or her absence or temporary incapacity.

Article 34
Dismissal of the Supervisors

1. The members of the Council may be released from their duties only in the following cases:

1.1 if they tender a statement of resignation to the Kosovo Assembly;

1.2 if they are convicted with a final decision of a criminal offence with prison of over six (6)months;

1.3 neglect of official duty;

1.4 if they cannot perform their duties for health or other important reasons for more than six (6) months;

1.5 if they become permanently incapable of performing their duties.

2. The members of the Council shall be released from their duties early and their position shall cease on the day the Kosovo Assembly determines the reasons from paragraph 1 of this Article.

Article 35
Independence of Supervisors

1. In the performance of their tasks the members of the Council act in complete independence and are only bound by this Law, the Constitution and other relevant laws. They shall refrain from any action incompatible with their duties and cannot exercise any other occupation whether gainful or not.

2. The members of the Council shall closely work together and shall assist each other in the performance of their duties.

Article 36
The Internal Organization of the Agency

1. The Chief State Supervisor shall define in accordance with the relevant law in force the sub-legal act on the internal organization and functioning of the agency.

2. At the Agency may be assigned to perform legal tasks or ancillary work, Civil servants of state bodies on the basis of a proposal of the Chief State Supervisor. Judges or state prosecutors may be assigned to perform such tasks pursuant to the provisions of the law on courts and prosecutor's office.

3. Civil servants and officials from paragraph 2 of this Article may not conduct inspections but shall assist the Supervisors in preparing and carrying out such inspections.

Article 37
Funds for the work of the Agency

1. The Agency has its own budget, administered independently in accordance with the law..

2. Funds for the work of the Agency shall be provided from the Kosovo Budget. The Budget of the Agency shall be determined by the Kosovo Assembly on the proposal of the Chief State Supervisor

Subchapter E
Tasks of the Agency

Article 38
Providing advice to public and private institutions

1. The Agency shall advise the Kosovo Assembly, the Government, local governing community bodies, other state bodies and holders of public powers in all matters regarding data protection including interpretation and application of relevant laws.

2. The Agency shall also advise private institutions on all data protection related matters where requested to do so including the interpretation and application of relevant laws.

Article 39
Obligation to Consult

The Kosovo Assembly and the Kosovo Government would inform the Agency when drawing up legislative and administrative measures relating to the processing of personal data. The Agency would be consulted prior to the adoption of such measures.

Article 40
Right to start legal procedures

1. The Agency files a request with the Constitutional Court of Kosovo to assess the constitutionality of laws, regulations and other acts where it believes that they are not compatible with the right to data protection as enshrined in Article 36 of the Kosovo Constitution.

2. The Agency files a suit with competent court, in cases where it believes that the right to data protection has been infringed.

Article 41
Right to complain

1. Every person has the right to lodge a complaint with the Agency if he or she believes that his or her right to data protection has been violated.

2. Complaints can be lodged orally, in writing or by electronic means.

Article 42
Handling of Complaints

1. The Agency shall immediately inform the complainant of the outcome and action taken following the investigation of the complaint.

2. The procedure regarding complaints will be regulated by sub-legal act by the Agency.

Article 43
Cooperation with other bodies

The Agency shall cooperate with national, international and European Union bodies regarding issues considered important for the protection of personal data.

Subchapter F
Publicity of work

Article 44
Annual work activities

1. The Agency shall submit an annual activities report on its work to the Kosovo Assembly and should publish it, not later than by 31 March of the coming year.

2. The annual activities report shall give an overview of the work of the Agency and the developments in the field of data protection in the previous year and shall spell out assessments and recommendations regarding the protection of personal data.

Article 45
Publicity concerning work

1. The Agency may publish on its website or in another appropriate manner:

1.1 an internal journal and professional literature;

1.2 any advise given according to paragraph 1 of Article 38 of this Law, in particular if laws or other regulations concerning the processing of personal data have been adopted and published in the Official Gazette;

1.3 any requests from Article 40 of this Law, after the Constitutional Court has received them;

1.4 any decisions of the Constitutional Court on requests from Article 40 of this Law;

1.5 any decisions of courts of general jurisdiction relating to the protection of personal data. However, in such cases there should be no indication of personal data of parties, injured parties, witnesses or experts involved;

1.6 opinions on the compliance of codes of professional ethics, general terms of business or drafts thereof with regulations in the area of data protection;

1.7 opinions, clarifications and positions on issues in the area of data protection;

1.8 any instructions and recommendations regarding the protection of personal data in individual fields;

1.9 public statements on inspections undertaken in individual cases;

1.10 any other important announcements.

2. The Agency shall hold regular media conferences relating to its work and publish transcripts of statements or recordings of statements on its website or in any other way considered appropriate. It may also hold seminars and organize awareness raising campaigns as considered appropriate.

3. The Agency may for the performance of its tasks encourage the cooperation with representatives of associations and other nongovernmental organizations in the area of data protection, privacy and consumer protection.

Subchapter G
Inspections and audits

Article 46
Scope of inspections

1. The Agency may carry out inspections and audits on its own initiative to monitor the compliance with data protection rules. Within the framework of inspection powers the Agency shall:

1.1 monitor the legitimacy of data processing;

1.2 monitor the suitability of procedures and measures taken for the protection of personal data pursuant to this Law;

1.3 monitor the implementation of the provisions of this Law regulating the filing system catalogue, the register of filing systems and the recordings of the disclosures of personal data to recipients;

1.4 monitor the implementation of provisions regarding the transfer of personal data to other countries and international organizations.

Article 47
Direct performance of inspections

1. Inspection and audits shall be carried out directly by the Supervisors within the limits of their competences.

2. Supervisors when carrying out inspections and audits, shall identify themselves with an official identity card containing a photograph of the Supervisor, his or her personal name, professional or scientific title and other necessary information.

3. The Government of Kosovo shall issue the official identity cards of the Supervisors according to sub-legal act upon the proposal of the Agency detailing the format and the content of the cards.

Article 48
Responsibility of the Supervisors

1. In performing inspection and audits, the Supervisors shall be entitled:

1.1 to examine and confiscate any documentation relating to the processing of personal data, irrespective of their confidentiality or secrecy, and the transfer of personal data to other countries and international organizations as well as the disclosure to foreign recipients;

1.2 to examine the contents of filing systems, irrespective of their confidentiality or secrecy, and the filing system catalogues;

1.3 to examine and confiscate any documentation and instructions regulating the security of personal data;

1.4 to examine premises in which personal data are supposed to be processed and they are entitled to examine and confiscate computers and any other equipment and technical documentation;

1.5 to verify measures and procedures intended to secure personal data, and the implementation thereof;

1.6 to perform any other matters considered necessary for the carrying out of inspections and audits as provided by this Law.

Article 49
Inspection measures

1. If a Supervisor notices a violation of this Law or any other law or regulation governing the processing of personal data he or she shall have the right to immediately:

1.1 order the elimination of irregularities or deficiencies he or she notices in the manner and within the terms he or she has previously defined. This may include the erasure, blocking, destruction, deletion or anonymization of data in compliance with the Law.

1.2 impose a temporary or definite ban on the processing of personal data by controllers and processors in the public or private sectors who have failed to implement the necessary measures and procedures to secure personal data;

1.3 impose a temporary or definite ban on the processing of personal data, their anonymity, classification and blocking whenever he or she concludes that the personal data are being processed in contravention of legal provisions;

1.4 impose a temporary or definite ban on the transfer of personal data to other countries or international organizations, or their disclosure to foreign recipients if they are transferred or disclosed in contravention of legal provisions or international agreements;

1.5 in minor cases of violations the Supervisor can warn or admonish the data controller or data processor in writing.

2. In case of irregularities or deficiencies the data controller or data processor shall immediately correct them by following the written instructions or advice of the Supervisor to ensure lawful data processing.

3. There shall be no appeal against a final decision of the Supervisor from paragraph 1 of this Article, but an administrative dispute shall be permitted in the competent Court.

Article 50
Protection of confidentiality

1. The Supervisors shall be obliged to protect the confidentiality of personal data they encounter in performing their tasks also after ceasing to perform their duties.

2. The obligation from paragraph 1 of this Article shall apply to the all members working at the Agency.

CHAPTER V
TRANSFER OF PERSONAL DATA

Subchapter H
Transfer of personal data to other Countries and international organizations

Article 51
General provisions

The transfer to other countries and international organizations of personal data that are processed or are intended to be processed after transfer may take place only in accordance with the provisions of this Law and if the country or the international organization in question ensures an adequate level of data protection.

Article 52
Procedure for determining an adequate level of data protection

Countries and international organizations are considered as ensuring an adequate level of data protection if the Agency has taken a formal decision and they are included in the respective list established by the Agency in accordance with this Law.

Article 53
List of countries and international organizations with an adequate level of data protection

1. The Agency shall maintain a list of countries and international organizations for which it finds that they ensure an adequate level of data protection in the meaning of this Law

2. The list can contain the Member States of the European Union and the European Economic Area. As to other countries the Agency can take over any decisions taken by the competent body of the European Union as to whether such countries and international organizations ensure an adequate level of data protection or it can take a formal decision according to Article 54 of this Law.

3. The Agency shall publish the list from paragraph 1 of this Article in the Official Gazette and on its website.

Article 54
Decisions on the adequate level of data protection of other countries and international organizations

1. In its decision-making on the adequate level of protection of personal data of another country or an international organization, the Agency shall determine all circumstances relating to the transfer of personal data. In particular, it shall take account of the type of personal data, the purpose and duration of the proposed processing, the legal arrangement in the country of origin and the recipient country, including legal arrangement for protection of personal data of foreign citizens, and measures to secure personal data used in such countries and international organizations.

2. In its decision-making from paragraph 1 of this Article the Agency shall in particular take account of:

2.1 whether the transferred personal data are used solely for the purpose for which they were transferred, or whether the purpose may change only on the basis of a permission of the data controller supplying the data or on the basis of personal consent of the data subject;

2.2 whether the data subject has the possibility of determining the purpose for which his or her personal data have been used, to whom they were supplied and the possibility of correcting or erasing inaccurate or outdated personal data, unless this is prevented due to the secrecy of the procedure by binding international treaties;

2.3 whether the foreign data controller or data processor performs adequate organizational and technical procedures and measures to protect personal data;

2.4 whether there is an assigned contact person authorized to provide information to the data subject or to the Agency on the processing of personal data transferred;

2.5 whether the foreign data recipient may transfer personal data only on the condition that another foreign data recipient to whom personal data will be disclosed ensures adequate protection of personal data also for foreign citizens;

2.6 whether provide legal protection is ensured for data subjects whose personal data were or are to be transferred.

Article 55
Criteria for Decision Making

The Agency defines in greater detail which information is necessary to decide whether another country or an international organization provides an adequate level of data protection in the meaning of this Law.

Article 56
Special provisions

1. Irrespective of Article 51 of this Law, personal data may be transferred and disclosed to a country or international organizations not ensuring an adequate level of data protection , if:

1.1 it is so provided by another law or binding international treaty;

1.2 the data subject has given his or her consent and is aware of the consequences of the transfer;

1.3 the transfer is necessary for the performance of a contract between the data subject and the data controller or for the implementation of pre-contractual measures taken in response to the data subject's requests;

1.4 the transfer is necessary for the conclusion or performance of a contract concluded in the data subject's interests between the data controller and a third party;

1.5 the transfer is necessary and legally required on important public interest grounds;

1.6 the transfer is necessary to protect the life and body of the data subject;

1.7 the transfer is necessary for the establishment, exercise or defence of legal claims;

1.8 the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down for consultation are fulfilled in this particular case.

Article 57
Authorization for data transfers

1. Without prejudice to Article 51 of this Law the Agency may authorize a transfer or a set of transfers of personal data to another country or an international organization not ensuring an adequate level of data protection within the meaning of this Law where the data controller adduces adequate safeguards for the protection of personal data and the fundamental rights and freedoms of individuals as regards the exercise of adduces rights. Such safeguards may result from the provisions of the contract or the general terms of business activities governing the transfer of personal data.

2. The data controller may transfer personal data only upon receipt of the authorization according to paragraph 1 of this Article. In his or her request for authorization the data controller shall provide the Agency with all information necessary regarding the required transfer of personal data. This includes in particular the categories of data, the purpose of the transfer and the safeguards in place for the protection of personal data in the other country or international organization.

3. The Agency shall decide on the application from paragraph 2 of this Article without delay and shall define in a sub-legal act the details and internal procedures for filing such requests. The above mentioned decision is final in administrative procedure but an administrative dispute shall be permitted in the competent court.

Article 58
Registration of authorizations

The authorizations concerning the transfer of personal data to another country or international organization granted by the Agency shall be registered in accordance with sub-paragraph 1.10 of paragraph 1 of Article 17 of this Law.

CHAPTER VI
RIGHTS AND SUPERVISION

Subchapter I
Direct marketing

Article 59
Rights and responsibilities of data controllers

1. Data controllers may use personal data they obtained from publicly accessible sources or within the framework of the lawful performance of activities for the purposes of offering goods, services, employment or temporary performance of work through the use of postal services, telephone calls, electronic mail or other telecommunications means (hereinafter: direct marketing) in accordance with the provisions of this Chapter, unless otherwise provided by relevant law.

2. For the purposes of direct marketing, data controllers may use only the personal data collected in accordance with paragraph 1 of this Article: personal name(s), permanent or temporary address, telephone number, e-mail address and fax number. Based on the data subject's prior consent data controllers may process other personal data but may only process personal sensitive data if they possess the written consent.

3. When data controllers do direct marketing, data controllers must inform data subjects of their rights according to Article 60 of this Law.

4. If data controllers intend to disclose personal data from paragraph 2 of this Article to other data recipients for the purposes of direct marketing or to data processors, they shall inform the data subject and get his or her written consent before disclosing such data. The notification of the data subject regarding the intended disclosure must contain all information that is intended to be disclosed as well as to whom and for what purposes. The costs of notification shall be borne by the data controller.

Article 60
Right to object

1. A data subject may at any time in writing request that data controllers permanently or temporarily cease to use his or her personal data for the purposes of direct marketing. Within eight (8) days following the receipt of the data subject' objection, data controllers shall refrain from using the personal data for direct marketing and within the subsequent five (5) days they shall inform the data subject in writing confirming the data subject's wishes.

2. Any costs regarding the data controller's activities as to requests from paragraph 1 of this Article shall be borne by the data controller.

Subchapter J
Video surveillance

Article 61
General provisions

1. The provisions of this Subchapter shall apply to the installation of video surveillance systems unless otherwise provided by relevant law.

2. Public or private sector persons intending to install video surveillance systems must set up a notice to that effect. Such a notice must be plainly visible and made public in a way that data subjects can easily acquaint themselves with the measures at the latest where the video surveillance begins.

3. Through the correct notification from paragraph 2 of this Article, the data subject shall be deemed to have been informed of the processing of personal data pursuant to Article 10 of this Law.

4. The video surveillance system and the recordings of the monitoring must be adequately protected against unauthorized access and use.

Article 62
Monitoring of official and business premises

1. Public and private sector persons may install video surveillance systems to monitor their premises if this is considered necessary for the safety of people and the security of property. Video surveillance may in particular be required to monitor the entrance of premises or where due to the nature of their work there exists a potential threat to employees.

2. The competent functionary, director or other competent or authorized person of the public or private sector shall take the necessary decisions.

3. The decision must contain the reasons for setting up the video surveillance systems.

4. Video surveillance systems may monitor the outside and the entrance(s) of premises but not the entrance and the interior of apartments.

5. Persons working in public or private premises under video surveillance are adequately informed in writing about the installation of such systems and their rights.

6. Each data controller shall establish a filing system for the recording of video surveillance systems. The filing system shall contain apart from the recordings (images and/or sound), date, place, time of the recording and where the recordings are stored.

7. The recordings from paragraph 6 of this Article may be stored for up to six (6) months unless required otherwise for legitimate purposes.

Article 63
Monitoring of apartment buildings

1. For the installation of video surveillance systems in apartment buildings at least 70% of the owners have to agree in writing to such measures.

2. Video surveillance systems may only be installed if this is necessary for the safety of people and the security of property.

3. Video surveillance systems in apartment buildings may only monitor the entrance and common areas. Monitoring of the housekeeper's apartment and his or her workshop shall be prohibited.

4. The transmission of video surveillance recordings through internal cable television, public cable television, the internet or other telecommunications means whether at the same time or later on shall be prohibited.

5. Entrances to individual apartments may only be monitored by video surveillance systems if the owner decides so. The owner may keep the recordings only for his or her own purposes.

Article 64
Video surveillance in the employment sector

1. Video surveillance systems at work places may only be done in cases where this is necessarily required for the safety of people, the security of property and the protection of confidential information if these purposes cannot be achieved by milder means.

2. Video surveillance must be strictly limited to those areas where the interests from paragraph 1 of this Article are at stake.

3. Video surveillance shall be prohibited outside work places particularly in changing rooms, lifts and sanitary areas.

4. Prior to the installation of video surveillance systems the employer must inform in writing the data subjects about their rights and the reasons for the surveillance. The monitored areas have to be indicated by the employers through appropriate signs.

5. Prior to the installation of video surveillance systems in the public or private sectors, the employer informs the trade union representatives, if applicable.

6. The paragraphs 4 and 5 of this Article shall not apply to areas of national defence, national intelligence – security activities in places where the secret data are protected.

Subchapter K
Use of biometric features

Article 65
Processing of biometric features

The determination and use of a data subject's biometric characteristics and their comparison to allow his or her identification shall be governed by the provisions of this Law.

Article 66
Use of biometric features in the public sector

1. The public sector may only use biometric features if this is necessarily required for the safety of people, the security of property or the protection of confidential data and business secrets if this cannot be achieved by milder means.

2. Irrespective of paragraph 1 of this Article, the use of biometric features may be allowed in compliance with obligations arising from binding international treaties or for the identification of persons crossing state border.

Article 67
Access Control

Biometric features may be used in the public sector for reasons of access control. In this case the provisions of the paragraphs 2, 3 and 4 of Article 68 of this Law shall be applied mutatis mutandis.

Article 68
Use of biometric features in the private sector

1. The private sector may only use biometric features if this is necessarily required for the performance of activities, for the safety of people, the security of property or the protection of confidential data or business secrets. Employees have to be informed in writing prior to the use of their biometric characteristics, about the intended measures and their rights.

2. If not provided otherwise by relevant law the data controller shall prior to the introduction of measures using biometrics provide the Agency with a detailed description of the intended measures including the information to be given to data subjects, the reasons for their introduction and the safeguards for the protection of personal data.

3. Upon receipt of the information from paragraph 2 of this Article, the Agency shall decide within thirty (30) days whether the intended introduction of measures complies with the provisions of this Law.

4. Data controllers may implement measures using biometrics upon the receipt of an authorization from the Agency.

5. There shall be no appeal against a decision from paragraph 3 of this Article, but an administrative dispute shall be permitted in the competent court.

Subchapter L
Records of entry to and exit from premises

Article 69
Recording

1. Public and private sector bodies may for reasons of protecting the safety of people and the security of property ask persons entering or leaving premises to give them the information from paragraph 2 of this Article. If considered necessary the personal data may be verified by examining identification documents.

2. The records registering persons entering or leaving premises may only contain the following personal data: personal name(s), number and type of identity document, permanent or temporary address, date and time as well as the reason for entering the premises.

3. Records from paragraph 2 of this Article shall be regarded as official documents if the collection of data is required for the purposes of police and intelligence-service activities.

4. Personal data contained in the records from paragraph 2 of this Article may be stored for a maximum period of three (3) years starting from the day of their recording and than shall be deleted or destroyed, unless otherwise provided by law.

Subchapter M
Public books and protection of personal data

Article 70
Public books

Personal data contained in public books regulated by relevant law may only be used in accordance with the purposes for which they were collected or processed, if the statutory purpose of their collection or processing is defined or definable.

Subchapter N
Linking filing systems

Article 71
Official records and public books

1. Filing systems from official records and public books may be linked if so provided for by law.

2. A data controller or data controllers who intend to link two or more filing systems kept for different purposes shall prior to doing so notify in writing the Agency.

3. If at least one of the filing systems to be linked contains sensitive data or the linking would result in the disclosure of sensitive data or if the implementation of the linking requires the use of a connecting code, linking shall not be permitted without the prior authorization of the Agency.

4. The Agency may authorize with decision the linking from paragraph 3 of this Article if it determines that the data controller ensures an adequate level of data protection.

5. There shall be no appeal against a decision from the paragraph 4 of this Article but an administrative dispute shall be permitted in the competent court.

Article 72
Prohibition of linking filing systems

The linking of filing systems from criminal records and minor offence records to other filing systems and the linking of filing systems from criminal records and minor offence records shall be prohibited.

Article 73
Special provisions

Personal data contained in filing systems from official records and public books shall be kept separately in the Register of Filing Systems.

Subchapter O
Data Protection Official

Article 74
Official of Data Protection

1. All public bodies processing personal data shall choose and appoint in writing an internal data protection official.

2. Only persons who possess the specialized knowledge and demonstrate the reliability necessary for the performance of the duty concerned may be appointed as data protection officials.

3. The data protection official shall be subordinated to the head of the public body. He or she shall suffer no disadvantage through the performance of his or her duties.
4. The data protection official shall maintain the confidentiality of personal data he or she shall be informed with during the performance of his or her duties.

5. The public body shall support the data protection official in the performance of his or her duties and shall in particular to the extent necessary make available equipment and other recourses.

6. If the data protection official no longer fulfils the conditions mentioned in paragraph 2 of this Article he or she shall be released from his or her duties.

Article 75
Duties of the Data Protection Official

1. The data protection official shall assist the public body in ensuring that relevant data protection rules are observed and properly implemented. For this purpose he or she may consult at any time the Agency.

2. The data protection official shall regularly monitor the proper use of data processing programs and the measures and procedures in place to ensure secure data processing.

3. The data protection official shall be informed on a regular basis all persons employed by the public body in the processing of personal data with relevant rules and provisions. He or she shall also regularly inform all employees of their rights and obligations pursuant to this Law and inform them about developments in the area of data protection.

Article 76
Control

1. The data protection official may carry out controls on his or her own initiative.

2. The data protection official shall have the right to consult, extract, transcribe or copy personal data he or she encounters during the controls. He or she shall respect the confidentiality of personal data.

3. The data protection official shall report in writing to the head of the public body of the results of the controls.

Article 77
Information to the data subject

1. When carrying out controls the data protection official may inform the data subject in writing about the performance of his or her duties. He or she may also inform the data subject that he or she will provide the public body with his or her opinion about the control.
2. The data subject from paragraph 1 of this Article may disclose to the data protection official additional information that might be necessary to carry out the control.

Article 78
Sensitive personal data

If in the performance of a control sensitive personal data are processed, the data protection official shall make an official annotation in the file of the data subject.

CHAPTER VII
PENAL PROVISIONS

Article 79
General violations of the provisions of this Law

1. A fine between four thousand (4.000) and ten thousand (10.000) Euros shall be imposed for minor offences to a legal or independent trader:

1.1 if he or she processes personal data without any legal basis or the consent of the data subject according to paragraph 1 of Article 3 and paragraph 1 of Article 5 of this Law;

1.2 if he entrusts an individual task relating to the processing of personal data to another person without concluding a written contract in accordance with paragraph 2 of article 15 of this Law;

1.3 if he processes sensitive personal data in contravention of Article 6 of this Law, or does not protect them in accordance with Article 7 of this Law;

1.4 if he processes personal data in contravention of Article 10 of this Law;

1.5 if he collects personal data for purposes that are not clearly defined and unlawful, or if he continues to process them in contravention of Article 5 of this Law;

1.6 if he discloses to a data recipient personal data in contravention of paragraph 2 of Article 9 or if he does not destroy personal data in accordance with paragraph 3 of Article 9 or does not publish the results of processing in accordance with paragraph 4 of Article 9 of this Law;

1.7 if he does not inform the data subject of the processing of personal data in accordance with Article 10 of this Law;

1.8 if he uses the same connecting code in contravention of Article 11 of this Law;

1.9 if he does not delete, destroy, block or anonymise personal data once the purpose for which they were collected and/or processed has been achieved in accordance with paragraph 5 of Article 3 of this Law;

1.10 if he or she acts in contravention of Article 12 of this Law;

1.11 if he or she fails to ensure that the filing system catalogue contains the information provided for by Article 17 of this Law;

1.12 if he fails to notify the Agency of information regarding the Register of Filing Systems according to Article 18 of this Law

1.13 if he acts in contravention of paragraphs 1 and 2 of Article 22 or the paragraphs 2, 3 or 5 of Article 23 of this Law;

1.14 if he acts in contravention of Article 24 or paragraphs 2 or 5 of Article 25 of this Law;

1.15 if he acts in contravention of paragraph 1 of Article 52 or in contravention of Article 56 concerning the transfer of personal data to other countries or international organizations.

2. A fine for a minor offence between five hundred (500) and two thousand (2.000) Euros shall be imposed on the responsible person of a legal person or independent trader for infringements of sub-paragraph 1.15 of paragraph 1 of this Article.

3. A fine between five hundred (500) and two thousand (2.000) euros shall be imposed for a minor offence on the responsible person of a state body who commits an act from paragraph 1 of this Article.

4. A fine between two hundred (200) and eight hundred (800) euros shall be imposed for a minor offence on an individual who commits an act from paragraph 1 of this Article.

Article 80
Violation of the provisions on contractual processing

1. A fine of between four thousand (4.000) and ten thousand (10.000) euros shall be imposed for a minor offence on a legal person or a person who practices an independent activity, if he oversteps the authorization contained in the contract from paragraph 2 of Article 15 of this Law or does not return personal data in accordance with paragraph 4 of Article 15 of this Law.

2. A fine of between five hundred (500) and two thousand (2.000) shall be imposed on the responsible person of the legal person or on the person who practices an independent activity for violations of paragraph 1 of this Article.

3. A fine of between five hundred (500) and two thousand (2.000) euros shall be imposed for a minor offence on the responsible person of a state body who commits an act from paragraph 1 of this Article.

4. A fine of between two hundred (200) and eight hundred (800) Euros shall be imposed on an individual who commits an act from paragraph 1 of this Article.

Article 81
Violation of the provisions on security of personal data

1. A fine of between four thousand (4.000) and ten thousand (10.000) Euros shall be imposed for a minor offence on a legal person or on the person who practices an independent activity, if he or she fails during the processing of personal to ensure an adequate level of security for the protection of personal data according to Articles 14 and 16 of this Law.

2. A fine of between five hundred (500) and two thousand (2.000) euros shall be imposed for a minor offence on the responsible person of the legal person or on the person who practices an independent activity who commits an act from paragraph 1 of this Article.

3. A fine of between five hundred (500) and two thousand (2.000) euros shall be imposed for a minor offence on the responsible person of a state body who commits an act from paragraph 1 of this Article.

4. A fine of between two hundred (200) and eight hundred (800) euros shall be imposed on an individual who commits an act from the paragraph 1of this Article.

Article 82
Violation of the provisions on direct marketing

1. A fine of between two thousand (2.000) and four thousand (4.000) Euros shall be imposed for a minor offence on a legal person or a person who practices an independent activity, if in accordance with this Law he processes personal data for the purposes of direct marketing and does not act in accordance with Articles 59 or 60 of this Law.

2. A fine of between four hundred (400) and one thousand (1.000) euros shall be imposed for a minor offence on the responsible person of the legal person or on a person practicing an independent activity who commits an act from paragraph 1 of this Article.

3. A fine of between two hundred (200) and eight hundred (800) Euros shall be imposed for a minor offence on an individual who commits an act from paragraph 1 of this Article.

Article 83
Violation of general provisions on video surveillance

1. A fine of between four thousand (4.000) and ten thousand (10.000) euros shall be imposed for a minor offence on a legal person or on a person practicing an independent activity:

1.1 if he does not publish a notice in the manner set out in paragraph 2 of Article 61 of this Law;

1.2 if the information does not contain the necessary information from paragraph 3 of Article 61 of this Law;

1.3 if he does not protect the video surveillance system and the recordings in contravention of paragraph 5 of Article 61 of this Law.

2. A fine of between eight hundred (800) and one thousand (1.000) Euros shall be imposed for a minor offence from paragraph 1 of this Article on the responsible person of the legal person or on a person who practices an independent activity.

3. A fine of between five hundred (500) and two thousand (2.000) Euros shall be imposed for a minor offence on the responsible person of a state body who commits an act from paragraph 1 of this Article.

4. A fine of between two hundred (200) and eight hundred (800) Euros shall be imposed for a minor offence on an individual who commits an act from paragraph 1 of this Article.

Article 84
Violation of the provisions on video surveillance regarding access to official and business premises

1. A fine of between four thousand (4.000) and ten thousand (10.000) Euros shall be imposed for a minor offence on a legal person or on a person practicing an independent activity:

1.1 if he implements video surveillance systems without the necessary written decision or without any legal grounds from Article 62 of this Law;

1.2 if he implements video surveillance systems which monitor the interior of residential buildings in contravention to paragraph 4 of Article 62;

1.3 if he does not inform employees in writing from paragraph 5 of Article 62;

1.4 if he stores personal data in contravention of paragraph 7 of Article 62 of this Law.

2. A fine of between five hundred (500) and two thousand (2.000) Euros shall be imposed for a minor offence on the responsible person of the legal person or on the person practicing an independent activity who commits an act from paragraph 1 of this Article.

3. A fine of between five hundred (500) and two thousand (2.000) Euros shall be imposed for a minor offence on the responsible person of a state body who commits an act from the paragraph 1 of this Article.

4. A fine of between two hundred (200) and eight hundred (800) Euros shall be imposed for a minor offence on an individual who commits an act from the paragraph 1 of this Article.

Article 85
Violation of the provisions on video surveillance in apartment buildings

1. A fine of between two thousand (2.000) and eight thousand (8.000) Euros shall be imposed for a minor offence on a legal person or on a person practicing an independent activity, who implements video surveillance systems in contravention of Article 63 of this Law.

2. A fine of between four hundred (400) and one thousand (1.000) Euros shall be imposed for a minor offence from paragraph 1 of this Article to responsible person of the legal person or on a person practicing an independent activity.

3. A fine between eight hundred (800) and one thousand (1.000) euros shall be imposed for a minor offence on the responsible person of a state body who commits an act from paragraph 1 of this Article.

4. A fine of between two hundred (200) and four hundred (400) Euros shall be imposed on an individual who commits an act from paragraph 1 of this Article.

Article 86
Violation of the provisions on video surveillance in work areas

1. A fine of between four thousand (4.000) and ten thousand (10.000) Euros shall be imposed on a legal person or on a person practicing an independent activity who implements video surveillance systems in work areas in contravention of Article 64 of this Law.

2. A fine of between one thousand (1.000) and two thousand (2.000) Euros shall be imposed for a minor offence from paragraph 1 of this Article on the responsible person of the legal person or on a person practicing an independent activity.

3. A fine of between one thousand (1.000) and two thousand (2.000) Euros shall be imposed for a minor offence on the responsible person of a state body who commits an act from paragraph 1 of this Article.

4. A fine of between eight hundred (800) and one thousand (1.000) Euros shall be imposed on an individual who commits an act from paragraph 1 of this Article.

Article 87
Violation of the provisions on biometrics in the public sector

1. A fine of between four thousand (4.000) and ten thousand (10.000) Euros shall be imposed on a legal person or on a person practicing an independent activity who implements biometric measures in contravention of Article 66 of this Law.

2. A fine of between one thousand (1.000) and two thousand (2.000) Euros shall be imposed from paragraph 1 of this Article on the responsible person of the legal person or on a person practicing an independent activity.

3. A fine of between one thousand (1.000) and two thousand (2.000) Euros shall be imposed on the responsible person of the state body who commits an act from paragraph 1 of this Article.

Article 88
Violation of the provisions on biometrics in the private sector

1. A fine of between four thousand (4.000) and ten thousand (10.000) Euros shall be imposed for a minor offence on a legal person or an independent trader who implements biometric measures in contravention of Article 68 of this Law.

2. A fine of between one thousand (1.000) and two thousand (2.000) Euros shall be imposed on the responsible person of the legal person or on a person practicing an independent activity who commits an act from paragraph 1 of this Article.

Article 89
Violation of the provisions on records of entry and exit

1. On a legal person or a person who practices an independent activity a fine of between two thousand (2.000) and four thousand (4.000) Euros:

1.1 shall be imposed for a minor offence if he or she uses entry and exit records as official records in contravention of paragraph 3 of Article 69 of this Law;

1.2 who acts in contravention of paragraph 4 of Article 69 of this Law.

2. A fine of between two hundred (200) and eight hundred (800) Euros shall be imposed for a minor offence on the responsible person of the legal person or on a person practicing an independent activity who commits a minor offence from paragraph 1 of this Article.
3. A fine of between two hundred (200) and eight hundred (800) Euros shall be imposed for a minor offence on the responsible person of the state body who commits a minor offence from paragraph 1 of this Article.

4. A fine of between two hundred (200) and eight hundred (800) Euros shall be imposed for a minor offence on an individual who commits a minor offence from paragraph 1 of this Article.

Article 90
Violation of the provisions on linking filing systems

1. A fine of between eight hundred (800) and two thousand (2.000) Euros shall be imposed for a minor offence on the responsible person of a state body, who links filing systems in contravention of Article 71 of this Law.

2. A fine of between eight hundred (800) and two thousand (2.000) Euros shall be imposed for a minor offence on the responsible person of a state body who links filing systems from criminal records or minor offence records with other filing systems, or links filing systems from criminal records with filing systems from records on minor offences according to Article 72 of this Law.

Article 91
Violation of the provisions on supervision from the expert

1. A fine of between four thousand (4.000) and ten thousand (10.000) Euros shall be imposed for a minor offence on a legal person:

1.1 i if he or she carries out controls in contravention of paragraph 2 of Article 78 of this Law;

1.2 if he or she makes an official annotation in contravention of Article 78 of this Law.

2. A fine of between eight hundred (800) and one thousand (1.000) Euros shall be imposed for a minor offence from paragraph 1 of this Article on the responsible person of the legal person.

3. A fine of between one thousand (1.000) and two thousand (2.000) Euros shall be imposed for a minor offence on the responsible person of a state body who commits an act from paragraph 1 of this Article.

4. A fine of between two hundred (200) and eight hundred (800) Euros shall be imposed for minor offences on an individual who commits an act from paragraph 1 of this Article.

CHAPTER VIII
TRANSITIONAL AND FINAL PROVISIONS

Article 92
Other responsibilities

The pronouncement of penal provisions according to this Law, does not exclude other responsibilities according to legal provisions in force in particular the liability of data controllers and data processors for damages arising from unlawful processing.

Article 93
Fees

The fees for notifications and authorizations according to this Law will be regulated by sub-legal act adopted by the Agency.

Article 94
Sub-legal acts

The Agency can issue also other sub-legal acts to implement this Law.

Article 95
Abrogation

This law abrogates part seven of the Law no. 02/L-23 on Information Association Services.

Article 96
Entry into Force

This law enters into force fifteen (15) days after its publication in the Official Gazette of Republic of Kosovo.

Law No. 03/L-172
29 April 2010

Promulgated by the Decree No. DL-020-2010, dated 13.05.2010, of the President of Republic of Kosovo, Dr. Fatmir Sejdiu.