LAW NO. 06/L –082

ON PROTECTION OF PERSONAL DATA

Assembly of the Republic of Kosovo,

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

Adopts

LAW ON PROTECTION OF PERSONAL DATA

CHAPTER I
GENERAL PROVISIONS

Article 1
Purpose

1. This law determines the rights, responsibilities, principles and punitive measures with respect to the protection of personal data and privacy of individuals. This Law determines responsibilities of the institution responsible for monitoring the legitimacy of data processing and access to public documents.

2. This Law is in compliance with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Article 2
Scope

1. This law shall be applied to the processing of personal data by public and private bodies. This law shall not be applied 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 be applied to data controllers who are not established in the Republic of Kosovo, which for the purposes of personal data processing make use of automatic or other equipment in the Republic of Kosovo, unless such equipment is used only for purposes of transit through the territory of Kosovo. In these circumstances, controllers must designate a representative registered in Kosovo.

Article 3
Definitions

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

1.1. **Personal Data** - any information related to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified directly or indirectly, particularly by reference to an identifier such as a name, an identification

number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

1.2. **Processing** - any operation or set of operations performed to personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

1.3. **Restriction of Processing**- marking of stored personal data with the aim of limiting their processing in the future;

1.4. **Classification of Personal Data** – marking of personal data to indicate their sensitive nature. Specific conditions should be set for classified data, according to which users shall be able to process them. The classification should be attached to sensitive personal data until their deletion, erasure, destruction or anonymization.

1.5. **Profiling** - any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

1.6. **Pseudoonymization** - processing of personal data in such a manner that personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

1.7. **Filing System Catalogue** - a detailed description of the structure and the content of filing systems;

1.8. **Register of Filing Systems** - a register allowing a detailed overview of existing filing systems;

1.9. **Filing System** - any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

1.10. **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;

1.11. **Data Controller** - any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines purposes and means of personal data processing;

1.12. **Written Consent of the Data subjec**t - consent given from sub-paragraph 1.11 of paragraph 1 of this article, with the addition that the data subject must put his or her signature or sign under his or her written consent to process his or her data.

1.13. **Verbal Consent or Other Appropriate Consent of the Data Subject** - the consent from sub-paragraph 1.11 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;

1.14. **Data Processor** - a natural or legal person, from public or private sector which processes personal data for and on behalf of data controller;

1.15. **Data Recipient** - a natural or legal person from public of private sector, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry, in compliance with the legislation into force, shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

1.16. **Third Party** - a natural or legal person from the public or private sector other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

1.17. **Consent of the Data Subject** - any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

1.18. **Personal Data Breach** - a breach of security measures leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

1.19. **Genetic Data** - personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

1.20. **Biometric Data** - all personal data resulting from specific processing related to physical, physiological or behavioural characteristics of an individual that allows or confirms the unique identification of that natural person as well as visual images or dactyloscopic, psychological and behavioural data of all individuals but which are specific and permanent for each individual, if it can be used for identifying an individual, such as: fingerprints, finger papillary lines, iris, retina, facial features and DNA;

1.21. **Data Concerning Health** - personal data related to physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

1.22. **Cross-Border Processing** - is processing of personal data which takes place in the context of activities of authorities between states;

1.23. **Privacy** – respect for private and family life, inviolability of the home and the secrecy of telephone and other communications correspondence, in compliance with the applicable Law;

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

1.25. **Sensitive Personal Data** – personal data revealing ethnic or racial origin, political or philosophical views, religious affiliation, union membership or any data related to health condition or sexual life, any involvement in or removal from criminal or offence records retained in accordance with the law. Biometric characteristics are also considered sensitive personal data if the latter enable the identification of a data subject in relation with any of the abovementioned circumstances in this sub-paragraph;

1.26. **Information and Privacy Agency (the Agency)** – an independent agency, responsible for supervision of implementation of legislation for personal data protection and access to public documents in order to protect the rights and fundamental freedoms of natural persons in relation to the personal data processing and ensuring the guarantee for access to public documents;

1.27. **Commissioner** – an independent body, appointed within the Agency by the Assembly of the Republic of Kosovo, who is responsible to assure implementation of this law and of the law on access to public documents;

1.28. **Inspection Officer** – inspector of the Agency who carries on inspection duties pursuant to this law, according to the respective law on access to public documents.

Article 4
Principles of personal data processing

1. **Principle of lawfulness, justice and transparency** – personal data are processed in an impartial, lawful and transparent manner, without infringing the dignity of data subjects.

2. **Principle of purpose limitation** – data are collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purpose.

3. **Principle of data minimisation** – personal data shall be adequate, relevant and limited to the purposes for which they are further collected or processed.

4. **Principle of accuracy** – personal data shall be accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. **Principle of storage limitation** - personal data may be stored insofar as necessary to achieve the purpose for which are further collected or processed. After the fulfilment of processing purpose, personal data shall be erased, deleted, destroyed, blocked or anonymised, unless otherwise foreseen in the Law on State Archives or in another relevant law.

6. **Principle of integrity and confidentiality** – personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7. **Principle of accountability** – the controller shall be responsible for, and be able to demonstrate compliance with all principles set forth in this article.

CHAPTER II
LAWFULNESS OF DATA PROCESSING

Article 5
Lawful processing of personal data

1. Personal data processing shall be lawful only if one of the following criteria applies:

1.1. if the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

1.2. if processing is necessary for the performance of a contract to which the data

subject is a contracting party or in order to take steps at the request of the data subject prior to entering into a contract;

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

1.4. if processing is necessary in order to protect the vital interests of the data subject or of another natural person;

1.5. if 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;

1.6. if processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to the processing carried out by public authorities in the performance of their tasks.

2. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on the relevant legislation in force, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

2.1. any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

2.2. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

2.3. the nature of the personal data, in particular if special categories of personal data are processed, pursuant to Article 8 of this Law, or if personal data related to criminal convictions and offences are processed, pursuant to article 9 of this Law;

2.4. possible consequences of the intended further processing for data subjects;

2.5. the existence of appropriate safeguards, which may include encryption or anonymization.

Article 6
Conditions for consent

1. If processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to process his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language.

3. The data subject is entitled to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. The withdrawal shall be done in the same way as the giving of the consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on

the consent to the processing of personal data that is not necessary for the performance of that contract.

Article 7
Conditions applicable to child's consent in relation to information society services

1. Processing of personal data of a child shall be lawful where there is applied Article 5 sub-paragraph 1.1 of this Law with regard to providing the information society services directly to the child, processing of personal data of a child shall be lawful where the child is at least sixteen (16) years old. When the child is under the age of sixteen (16) years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

2. The controller shall make a reasonable effort to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 of this Article does not affect the law in force covering rules on the availability, establishment or effect of a contract in relation with a child.

4. If data processing is made for children aged below sixteen (16) to fourteen (14), data controller makes continuous efforts to verify if in such cases the consent given or authorized by parents or the custodian, taking into consideration the available technology.

Article 8
Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 of this Article shall not apply if one of the following circumstances exists:

2.1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where the relevant legislation in force provide that the prohibition referred to in paragraph 1 of this Article may not be lifted by the data subject;

2.2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by the relevant legislation in force or a collective agreement providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

2.3. processing is necessary to protect vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

2.4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to their members or data subjects who have regular contact with it in connection with its purposes and that the personal data are not disclosed without the consent of the data subjects;

2.5. if the data subject has made them public without limiting their use in an evidenced or clear manner;

2.6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

2.7. processing is necessary for reasons of substantial public interest, on the basis of relevant legislation;

2.8. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of relevant legislation or pursuant to contracts with a health professional when such data are processed by a professional or under his/her responsibility subject to the obligation of professional secrecy pursuant to respective legislation, established rules by national competent bodies or by another person subjected to professional secrecy;

2.9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of relevant legislation;

2.10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

3. Personal data referred to in paragraph 1 of this Article may be processed for the purposes referred to in sub-paragraph 2 of this Article, when those data are processed in a proportional manner for the required purpose, their processing respects the essence of the right for data protection and is performed in compliance with the specific measures for protection of the rights and fundamental interests of the data subject as foreseen by this Law, including, where necessary, the professional confidentiality.

4. Specific categories of personal data should be protected in a special manner and be classified for the purpose of preventing the unauthorized access and use, except in cases referred to in sub-paragraph 2.5 of paragraph 2 of this Article.

Article 9
Processing of personal data relating to the criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 5 paragraph 1 of this Law shall be carried out only under the control of official authority according to the relevant law. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Article 10
Processing which does not require identification

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this law.

2. Where in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject; the controller shall inform the data subject accordingly, if possible. In such cases, Articles 14 to 19 of this Law shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

CHAPTER III
DATA SUBJECT'S RIGHTS

Article 11
Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in articles 12 and 13 of this Law and any communication under Articles 14 to 21 and 33 of this Law relating to processing of personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 14 to 21 of this Law. In the cases referred to in Article 10, paragraph 2 of this Law, the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 14 to 21 of this Law, unless the controller demonstrates that it is not able to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 14 to 21 of this Law to the data subject without undue delay and in any event within one (1) month of receipt of the request. That period may be extended by two (2) further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one (1) month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not act on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one (1) month of receipt of the request of the reasons for not acting and on the possibility of lodging a complaint with the Agency and seeking a judicial remedy.

5. Information provided under Articles 12 and 13 of this Law and any communication and any actions taken under Articles 14 to 21 and 32 of this Law shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

5.1. charge a reasonable fee considering the administrative costs of providing the information or communication or taking the action requested; or

5.2. refuse to act on the request;

5.3. the controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 10 of this Law, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 14 to 20 of this Law, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 12 and 13 of this Law may be provided in combination with standardised icons (symbols) in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons (symbols) are presented electronically they shall be machine-readable.

CHAPTER IV
INFORMATION AND ACCESS TO PERSONAL DATA

Article 12
Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

1.1. the identity and the contact details of the controller and, where applicable, of the controller's representative;

1.2. contact details of the data protection officer, where applicable;

1.3. purposes of processing for which the personal data are intended as well as the legal basis for the processing;

1.4. where the processing is based on article 5 paragraph 1, sub-paragraph 1.6 of this Law, the legitimate interests pursued by the controller or by a third party;

1.5. the recipients or categories of recipients of the personal data, upon the case;

1.6. where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Agency.

2. In addition to the information referred to in paragraph 1 of this Article, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

2.1. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

2.2. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object the processing as well as the right to data portability;

2.3. wherever the processing is based on Article 5 paragraph 1, sub-paragraph 1.1 of this Law or Article 8 paragraph 2, sub-paragraph 2.1 of this Law, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

2.4. the right to lodge a complaint with the Agency;

2.5. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data;

2.6. the existence of automated decision-making, including profiling, referred to in Article 21 paragraphs 1 and 4 of this Law and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2 of this Article.

4. Paragraphs 1, 2 and 3 of this Article shall not apply where and insofar as the data subject already has the information.

Article 13
Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

1.1. the identity and the contact details of the controller and, where applicable, of the controller's representative;

1.2. the contact details of the data protection officer, where applicable;

1.3. the purpose of the processing for which the personal data are intended as well as the legal basis for the processing;

1.4. the categories of personal data concerned;

1.5. the recipients or categories of recipients of the personal data, if any;

1.6. Where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Agency.

2. In addition to the information referred to in paragraph 1 of this Article, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

2.1. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

2.2. where the processing is based on Article 5 paragraph 1, sub-paragraph 1.6 of this Law, the legitimate interests pursued by the controller or by a third party;

2.3. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

2.4. where processing is based on Article 5 paragraph 1, sub-paragraph 1.1 of this Law or Article 8 paragraph 2, sub-paragraph 2.1 of this Law, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

2.5. the right to lodge a complaint with the Agency;

2.6. from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

2.7. the existence of automated decision-making, including profiling, referred to in Article

21 paragraphs 1 and 4 of this Law and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2 of this Article:

3.1. within a reasonable period after obtaining the personal data, but at the latest within one (1) month, having regard to the specific circumstances in which the personal data are processed;

3.2. if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

3.3. if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2 of this Article.

5. Paragraphs 1 to 4 of this Article shall not apply where and insofar as:

5.1. the data subject already has the information;

5.2. the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 8, paragraph 3 of this Law, or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

5.3. obtaining or disclosure is expressly laid down by the relevant legislation to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

5.4. where the personal data must remain confidential subject to an obligation of professional secrecy regulated by the relevant legislation, including a statutory obligation of secrecy.

Article 14
Right of access by data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

1.1. the purposes of the processing;

1.2. the categories of personal data concerned;

1.3. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

1.4. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

1.5. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

1.6. the right to submit a complaint with the Agency;

1.7. where the personal data are not collected from the data subject, any available information as to their source;

1.8. the existence of automated decision-making, including profiling, referred to in article 21 paragraphs 1 and 4 of this Law and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 of this Article shall not adversely affect the rights and freedoms of others.

CHAPTER V
RECTIFICATION AND ERASURE

Article 15
Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 16
Right to erasure (‘right to be forgotten’)

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

1.1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

1.2. the data subject withdraws consent on which the processing is based according to Article 5 paragraph 1, sub-paragraph 1.1 of this Law or Article 8 paragraph 2, sub-paragraph 2.1 of this Law and where there is no other legal ground for the processing;

1.3. the data subject objects the processing pursuant to Article 20 paragraph 1 of this Law and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to article 20 paragraph 2 of this Law;

1.4. the personal data have been unlawfully processed;

1.5. the personal data have to be erased for compliance with a legal obligation to which the controller is subject;

1.6. the personal data have been collected in relation to the offer of the services of information society referred to in Article 7 paragraph 1 of this Law.

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 of this Article to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 of this Article shall not apply to the extent that processing is necessary:

3.1. for exercising the right of freedom of expression and information;

3.2. for compliance with a legal obligation which requires processing to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

3.3. for reasons of public interest in the area of public health in accordance with Article 8 paragraph 2, sub-paragraphs 2.8, 2.9 and paragraph 3 of this Law;

3.4. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with article 8, paragraph 3 of this Law in so far as the right referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

3.5. for the establishment, exercise or defence of legal claims.

Article 17
Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following criteria applies:

1.1. the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of personal data;

1.2. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

1.3. the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

1.4. The data subject has objected to processing pursuant to Article 20 paragraph 1 of this Law pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. If processing has been restricted under paragraph 1 of this Article, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 of this Article shall be informed by the controller before the restriction of processing is lifted.

Article 18
Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 15, Article 16 paragraph 1 and Article 17 of this Law to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 19
Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

1.1. the processing is based on a consent, pursuant to Article 5 sub-paragraph 1.1 or on a contract pursuant to Article 6 paragraph 1 and 2 or Article 8 sub-paragraph 2.1 of this Law; and

1.2. the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1 of this Article, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to article 16. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 of this Article shall not adversely affect the rights and freedoms of others.

CHAPTER VI
RIGHT TO OBJECT AND AUTOMATED INDIVIDUAL DECISION MAKING

Article 20
Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on Article 5 paragraph 1, sub-paragraph 1.6 or 1.5 of this Law, including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which overrides the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 of this Article shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 21
Automated individual decision making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

2.1. is necessary for entering into, or performance of, a contract between the data subject and a data controller;

2.2. is authorised by a specific law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

2.3. Is based on the data subject's explicit consent.

3. In the cases referred to in paragraph 2 sub-paragraph 2.1 and 2.3 of this Article, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 of this Article shall not be based on special categories of personal data referred to in Article 8 paragraph 1 of this Law, unless sub-paragraph 2.1 or 2.7 of Article 8 of this Law applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Article 22
Restrictions

1. The rights of the data subject provided for in Articles 4, 11 to 21, and Article 33 of this Law, in so far as its provisions correspond to the rights and obligations provided for in Articles 11 to 21 of this Law, may be restricted when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure to safeguard:

1.1. national security;

1.2. defence;

1.3. public security;

1.4. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

1.5. other important objectives of general public interest of the Republic of Kosovo, in particular an important economic or financial interest of the Republic of Kosovo, including monetary, budgetary and taxation matters, public health and social security;

1.6. the protection of judicial independence and judicial proceedings;

1.7. the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

1.8. monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in subparagraphs 1.1 to 1.5 and sub-paragraph 1.7 of this Article;

1.9. the protection of the data subject or the rights and freedoms of others;

1.10. the enforcement of civil law claims.

Measures referred to in paragraph 1 of this Article may be considered to that extent as deemed necessary to achieve a purpose the restriction was applied for.

CHAPTER VII
CONTROLLER AND PROCESSOR
GENERAL OBLIGATIONS

Article 23
Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Law. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

Article 24
Data protection by design and by default

1. Taking into account the state of technology, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of processing itself, implement appropriate technical and organisational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Law and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for

ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism as referred to in Article 43 of this Law may be used as an element to demonstrate compliance with the requirements stipulated in paragraphs 1 and 2 of this Article.

Article 25
Joint controllers

1. If two (2) or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under the law, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 12 and 13 of this Law, by means of an arrangement between them. The arrangement may designate a contact point for data subjects.

2. The measure referred to in paragraph 1 of this Article shall duly reflect the respective roles and relationships of the joint controller's vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1 of this Article, the data subject may exercise his or her rights under this law in respect of and against each of the controller.

Article 26
Representatives of controllers or of processors not seated in Kosovo

1. If paragraph 3 of Article 2 of this Law applies, the controller or the processor shall designate in writing a representative in the Republic of Kosovo.

2. The obligation laid down in paragraph 1 of this Article shall not apply to:

2.1. processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in article 8 paragraph 1 of this Law or processing of personal data relating to criminal convictions and offences referred to in Article 9 of this Law, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

2.2. a public authority or body.

3. The representative shall be authorized by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, the Agency and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this law.

4. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Article 27
Processor

1. If processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Law and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. This contract shall stipulate, in particular, that the processor:

3.1. processes personal data only according to documented instructions from the controller, including with regard to transfers of personal data to a foreign country or an international organisation, unless required to do so by a special law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The processor shall immediately inform the controller if, according to his opinion, a certain rule is in contradiction with this law;

3.2. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

3.3. takes all measures required pursuant to Article 31 of this Law;

3.4. respects the conditions referred to in paragraphs 2 and 4 of this Article for engaging another processor;

3.5. taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights.

3.6. assists the controller in ensuring compliance with the obligations pursuant to Articles 21 to 36 of this Law taking into account the nature of processing and the information available to the processor;

3.7. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Law on Archives requires storage of data;

3.8. makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

4. If a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 of this Article

shall be imposed on that other processor by way of a contract or other legal act under applicable legislation, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this law. If that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 6 and 7 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Article 43.

6. Respect of the approved code of conduct by the processor as referred to in Article 41 of this Law or of the approved mechanism of certification as referred to in Article 43 of this Law, may be used as an element by which sufficient guarantees shall be documented, as referred to in paragraphs 1 and 4 of this Article.

7. The Agency may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article.

8. The contract or the other legal act referred to in paragraphs 3 and 4 of this Article shall be in writing, including in electronic form.

9. Without prejudice to Article 57, 92 of this Law if a processor infringes this Law by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 28
Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by any specific law.

Article 29
Processing activity records

1. Each controller, processor and where applicable, their representatives keep records of processing activities under their responsibility. These records contain all below-listed information:

1.1. name and contact information of the controller and where applicable, of the common controller, the representative of the controller and the data protection officer;

1.2. purpose of processing;

1.3. a description of data subjects' categories and personal data categories;

1.4. categories of recipients to whom personal data were or shall be disclosed, including recipients in third countries or international organizations;

1.5. where applicable, transfer of personal data to third countries or to an international organization, including the identification of that third country or international organization, the authorization according to article 49 paragraph 2 of this Law and in cases of the above transfers, according to article 49 sub-paragraph 1.9 of this Law, documentation of adequate protective measures;

1.6. where possible, the envisaged time limits for erasure of the different categories of data;

1.7. where possible, a general description of technical and organizational security measures mentioned in Article 31 paragraph 1 of this Law.

2. The records referred to in paragraphs 1 of this Article shall be in writing, including in electronic form.

3. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

4. The obligations referred to in paragraph 1 of this Article shall not apply to an enterprise or an organisation employing fewer than two hundred and fifty (250) persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 8 paragraph 1 of this Law or personal data relating to criminal convictions and offences referred to in Article 9 of this Law.

Article 30
Cooperation with the Agency

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the Agency in the performance of their tasks.

CHAPTER VIII
PERSONAL DATA SAFETY

Article 31
Safety of processing

1. Taking into account the technology, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

1.1. the pseudonymization and encryption of personal data;

1.2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

1.3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

1.4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken into account in particular the risks that are presented by processing, particularly from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 41 of this Law or an approved certification as referred to in Article 43 of this Law may be used as an element by

which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by any specific law.

Article 32
Contracted processing

1. Personal data processor may be entrusted to a data processor under a written contract, to conduct such operations pursuant to procedures and security measures.

2. Data processor may act only within the constraints of the authorizations given by data controller and is not entitled to process personal data for other purposes. Mutual rights and obligations should be specified by a written contract, which should also contain a detailed description of procedures and measures in accordance with Article 32 of this Law.

3. Data controllers should oversee implementation of procedures and measures in accordance with Article 32 of this Law. They should also conduct periodical visits to the premises where personal data are processed.

4. In case of a dispute between the data controller and processor, the latter should immediately, upon controller's request, return all the data in possession. The data processor is not allowed to keep copies of and further process them.

5. In case of discontinuation of data processor's activity, personal data shall immediately be returned to the data controller.

Article 33
Notification of a personal data breach to the Agency

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than seventy-two (72) hours after having become aware of it, notify the personal data breach to the Agency, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Agency is not made within seventy-two (72) hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 of this Law shall at least:

3.1. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

3.2. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

3.3. describe the likely consequences of the personal data breach;

3.4. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Agency to verify compliance with this Article.

Article 34
Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in paragraph 3, sub-paragraphs 3.2, 3.3 and 3.4 of Article 33 of this Law.

3. The communication to the data subject referred to in paragraph 1 of this Article shall not be required if any of the following conditions are met:

3.1. the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

3.2. the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 of this Article is no longer likely to materialise;

3.3. it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the Agency, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 of this Article are met.

CHAPTER IX
DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Article 35
Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risk.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 of this Article shall in particular be required in the case of:

3.1. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

3.2. processing on a large scale of special categories of data referred to in Article 8 paragraph 1 of this Law, or of personal data relating to criminal convictions and offences referred to in Article 9 of this Law; or

3.3. A systematic monitoring of a publicly accessible area on a large scale.

4. The Agency shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1 of this Article.

5. The Agency may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required.

6. The assessment shall contain at least:

6.1. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

6.2. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

6.3. an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1 of this Article; and

6.4. The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Law taking into account the rights and legitimate interests of data subjects and other persons concerned.

7. Compliance with approved codes of conduct referred to in Article 41 of this Law by relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

8. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

9. Where processing pursuant to Article 5 paragraph 1, subparagraph 1.3 or 1.5 of this Law has a legal basis in any specific law to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 6 of this Article shall not apply, unless the Agency considers it necessary to carry out such an assessment prior to processing activities.

10. Where necessary, the controller shall carry out a review to assess if processing is performed

in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Article 36
Prior consultation

1. The controller shall consult the Agency prior to processing if a data protection impact assessment under Article 35 of this Law indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the Agency is of the opinion that the intended processing referred to in paragraph 1 of this Article would infringe this law, particularly if the controller has insufficiently identified or mitigated the risk, the Agency shall, within period of up to eight (8) weeks of receipt of the request for consultation, provide a written advice to the controller and, where applicable to the processor, may use any of its powers referred to in Article 64 of this Law. That period may be extended for six (6) weeks, taking into account the complexity of the intended processing. The Agency shall inform the controller and, where applicable, the processor, of any such extension within one (1) of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the Agency has obtained information it has requested for the purposes of the consultation.

3. When consulting the Agency pursuant to paragraph 1 of this Article, the controller shall provide the Agency with:

3.1. where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

3.2. the purposes and means of the intended processing;

3.3. the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this law;

3.4. where applicable, the contact details of the data protection officer;

3.5. the data protection impact assessment provided for in Article 35 of this Law; and

3.6. any other information requested by the Agency.

4. Notwithstanding paragraph 1 of this Article, the Agency may require controllers to consult with, and obtain prior authorisation in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

CHAPTER X
PERSONAL DATA PROTECTION OFFICER

Article 37
Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

1.1. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

1.2. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

1.3. the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 8 of this Law and personal data relating to criminal convictions and offences referred to in Article 9 of this Law.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1 of this Article, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processor.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39 of this Law.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the Agency.

Article 38
Position of the data protection officer

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 of this Law by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his or her tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this law.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 39
Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

1.1. to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Law and to sub-legal acts on data protection;

1.2. to provide advice, where requested, as regards the data protection impact assessment and monitor its performance pursuant to Article 35 of this Law;

1.3. to cooperate with the Agency;

1.4. to act as the contact point for the Agency on issues relating to processing, including the prior consultation referred to in Article 36 of this Law, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall, in the performance of his or her tasks, have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Article 40
Obligation to issue internal acts

1. Data controllers and processors shall, at all times, ensure that data are protected and processed in the manner specified in this law.

2. Data controllers and processors shall describe in their internal acts the procedures and measures established for the security of personal data and shall, in written form, appoint the competent persons responsible for implementing the rules under this law.

Article 41
Codes of Conduct

1. The Agency shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this law, taking account of the specific features of the various processing sectors.

2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, with regard to:

2.1. fair and transparent processing;

2.2. the legitimate interests pursued by controllers in specific contexts;

2.3. the collection of personal data;

2.4. the pseudonymisation of personal data;

2.5. the information provided to the public and to data subjects;

2.6. the exercise of the rights of data subjects;

2.7. the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

2.8. the measures and procedures referred to in Articles 23 and 24 of this Law and the measures to ensure security of processing referred to in Article 31 of this Law;

2.9. the notification of personal data breaches to Agency and the communication of such personal data breaches to data subjects;

2.10. the transfer of personal data to third countries or international organisations; or

2.11. out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 52 and 54 of this Law.

3. In addition to adherence by controllers or processors subject to this law, codes of conduct approved pursuant to paragraph 5 of this article and having general validity pursuant to paragraph 6 of this Article may also be adhered to by controllers or processors that are not subject to this law pursuant to Article 2 of this Law in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations.

4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the competent authority to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it.

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or supplement an existing code shall submit the draft code, amendment or extension to the Agency. The Agency shall provide an opinion on whether the draft code, amendment or supplementation complies with this law and shall approve that draft code, amendment or supplementation if it finds that it provides sufficient appropriate safeguards.

6. Where the draft code, or amendment or supplementation is approved in accordance with paragraph 5 of this Article, the Agency shall register and publish the code.

Article 42
Monitoring of approved Codes of Conduct

1. Without prejudice to the tasks and powers of the Agency under Articles 57, 64 and 65 of this Law, the monitoring of compliance with a code of conduct may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the Agency.

2. A body as referred to in paragraph 1 of this Article may be accredited to monitor compliance with a code of conduct where that body has:

2.1. demonstrated its independence and expertise in relation to the subject-matter of the code acceptable by the Agency;

2.2. established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

2.3. established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

2.4. demonstrated to the Agency that its tasks and duties do not result in a conflict of interests.

3. The Agency shall submit the criteria for accreditation of a body as referred to in paragraph 1 of this Article.

4. Without prejudice to the tasks and powers of the Agency a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the Agency of such actions and the reasons for taking them.

5. The Agency shall revoke the accreditation of a body as referred to in paragraph 1 of this Article if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this law.

6. This article shall not apply to processing carried out by public authorities and bodies.

Article 43
Certification

1. Controllers, processors as well as legal entities/enterprises which process data under the scope of the present law shall obtain the certification to perform work related to personal data.

2. A certification shall be issued by the Agency on the basis of criteria and procedures foreseen sub-legal act.

3. To obtain the certification, the controllers, processors and legal entities/enterprises shall meet at least the following minimum conditions:

3.1. shall prove that they possess adequate knowledge in the field of personal data protection;

3.2. shall meet where required the necessary the international safety standards;

3.3. in case of legal entities/enterprises, shall engage controllers, processors and other personnel who have obtained the certification;

3.4. shall prove that the exercise of their functions pertaining to the protection of data do not result in a conflict of interest.

4. If a legal person/enterprise possesses a certificate issued by a competent European Institutions or Bodies, that certificate is valid in the Republic of Kosovo as well.

5. The controller, the processor or the legal entity/enterprise which submits its processing to obtain the certification shall provide the Agency with all information and access to its processing activities which are necessary to conduct the certification procedure.

6. Certification shall be issued for a maximum period of three (3) years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the Agency where the requirements for the certification are not or are no longer met.

7. In addition to adherence by controllers or processors subject to this law, the Agency may establish data protection certification mechanisms for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this law pursuant to Article 2 of this Law within the framework of personal data transfers to third countries or international organisations. Such controllers or processors shall make binding and enforceable commitments, via contractual instruments, to apply those appropriate safeguards,

including with regard to the rights of data subjects.

8. A certification pursuant to this article does not reduce the responsibility of the controller or the processor for compliance with this law and is without prejudice to the tasks and powers of the Agency.

CHAPTER XI
TRANSFER OF PERSONAL DATA TO OTHER COUNTRIES AND INTERNATIONAL ORGANIZATIONS

Article 44
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 45
Procedure for determining the 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 46
List of countries and international organizations with an adequate level of data protection

1. The Agency shall maintain a list of countries and international organization or one or more sectors specified within them, for which it finds that they ensure an adequate level of data protection in the meaning of this law.

2. In order to draft a list anticipated in paragraph 1 of this Article, the Agency may apply decisions taken by a competent body of the EU if such countries and international organizations provide an adequate level of data protection.

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

Article 47
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 by taking into account the following elements:

1.1. the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectorial, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which apply within that country or international organisation, case-law, as well as effective and enforceable data subject

rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

1.2. the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities;

1.3. the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

1.4. the type of personal data to be processed;

1.5. the purpose and duration of the proposed processing;

1.6. the legal arrangement in the country of origin and the recipient country, including legal arrangement for protection of personal data of foreign citizens;

1.7. the 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 to be transferred will be or are used solely for the purpose for which they are 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 will be have been used, to whom they are were supplied and the possibility of correcting or erasing inaccurate or out-dated 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 further 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 effective legal protection is ensured for data subjects whose personal data were or are to be transferred.

3. The Agency shall carry out a periodic review of the list, at least every four (4) years, which shall take into account all relevant developments in the third country or international organization that could affect the permanence in the list.

4. The Agency shall, where available information reveals that a third country, one or more specified sectors within a third country, or an international organisation no longer ensures an

adequate level of protection within the meaning of paragraph 1 and 2 of this Article, to the extent necessary, amend or suspend the decision of inclusion in the list by means of implementing acts without retro-active effect.

Article 48
Criteria for decision making

The Agency shall, by sub-legal act, define 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 49
Authorizations for data transfer to a country or international organization that does not provide adequate level of data protection

1. Irrespective of article 45 of this Law, the Agency may authorize the transfer or the disclosure of personal data to a country or international organization not ensuring an adequate level of data protection, if one or more of the following conditions are met:

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. In this case, the transfer shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients;

1.9. 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 adduced 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 before the competent court.

Article 50
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 1.5 of paragraph 1 of Article 29 of this Law.

Article 51
Recognition and implementation of third party claims for transfer

Judgements and any decision of a third country administrative authorities requiring transfer or disclosure of personal data by controllers or processors, can only be recognized or implemented based on the international agreement between the third country submitting the request and the Republic of Kosovo, without prejudice to the reasons for transfer under this Law.

CHAPTER XII
MEANS OF COMPLAINT, LIABILITY AND PENALTIES

Article 52
The right to file a complaint at the Agency

1. Without prejudice to other administrative or judicial remedies of protection, any data subject has the right to file a complaint before the Agency, if the data subject claims that the processing of his or her personal data violates this law.

2. The Agency shall notify the complainant of the progress and outcome of the complaint, including the possibility of a judicial remedy in accordance with Article 54 of this Law.

Article 53
Right to an effective judicial remedy against the Agency

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of the Agency concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the Agency, based on its powers does not address a complaint or fails to notify the data subject within three (3) months on the progress or outcome of the complaint lodged pursuant to Article 52 of this Law.

3. The unsatisfied party has the right to initiate an administrative dispute before the competent court against Commissioner’s final decision.

Article 54
Right to an effective judicial remedy against a controller or processor

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 53 of this Law, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this law have been infringed as a result of the processing of his or her personal data in non-compliance with this law.

Article 55
Representation of the data subject

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law in force, as statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 53, 54 and 55 of this Law on his or her behalf, and to exercise the right to receive compensation referred to in Article 56 of this Law on his or her behalf.

2. The authorization for the representative must be given in writing and certified by the competent body.

Article 56
The right to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this law shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this law. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Law specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 of this Article if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3 of this Article, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5. Where a controller or processor has, in accordance with paragraph 4 of this Article, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

6. For the compensation of the damage, the party is entitled to file a lawsuit before the competent court.

CHAPTER XIII
INSTITUTIONAL PROTECTION OF PERSONAL DATA INFORMATION AND PRIVACY AGENCY

Article 57
The Status of the Agency

1. The Agency is an independent authority in charge of supervising the implementation of this law and other regulations for protection of personal data and access to public documents and information.

2. The Agency acts in full independency in fulfilling its duties and exercising its competences in

accordance with this law. The Agency shall report to the Assembly of Kosovo.

3. The Agency shall, in fulfilling its duties and exercising its powers, act free of external influence, whether direct or indirect, and shall not solicit or receive instructions from anyone.

4. Human, financial, and technical resources, along with the premises and required infrastructure for effectively fulfilling its duties and discharging competencies shall be made available to the Agency.

Article 58
Organization of the Agency

1. The Agency shall be led by the Commissioner;

2. The Commissioner represents the Agency, organizes and coordinates its work.

3. The Agency has its Director General who carries out all duties of the Chief Administrative Officer in accordance with the relevant legislation.

4. The organizational structure of the Agency consists of two (2) special professional scopes for access to public documents and the protection of personal data.

5. Special professional scopes defined in paragraph 4 of this Article are managed and composed by civil servants in accordance with this law and the respective legislation.

6. Agency officials refrain themselves from any action that is inconsistent with their duties and do not engage themselves in occupations which are in conflict with their duties be with or without payment during their mandate.

7. Pursuant to the applicable law in force, the Commissioner issues a sub-legal act on the organization and internal functioning of the Agency.

8. Agency officials, in accordance with this law are subjects of the duty of professional secrecy, both during their mandate and after its termination, in relation to any confidential information they may face when performing their duties or exercising their powers.

Article 59
Criteria for selecting the commissioner

1. Candidates for the Commissioner must meet the following criteria:

1.1. to be citizens of the Republic of Kosovo;

1.2. to have a university degree in one of the following fields: law, public administration or international relations;

1.3. should have at least eight (8) years of professional experience, of which at least five (5) years of experience in managing positions;

1.4. should not have been convicted by a final decision for a criminal offense or should have no indictment for the last five (5) years;

1.5. must have high moral and professional integrity;

1.6. should have experience and distinguished knowledge in the area of human rights protection;

1.7. should not have been dismissed from work or civil service due to a disciplinary measure;

1.8. should not have exercise any function in any political party during past five (5) years. Should not be a member of the Assembly of the Legislature of the Assembly of the Republic of Kosovo who elects him or her, or a member of the Government Cabinet in the last mandate.

Article 60
Selection procedure for the commissioner

1. The Commissioner shall be elected by the Assembly of the Republic of Kosovo with a majority of votes of the total number of parliament members for a five (5) years mandate with the right to be re-elected for another mandate.

2. The election procedure commences by announcing the job vacancy for the Commissioner's position, which shall be published in mass media, both written and electronic.

3. The job vacancy announcement sets out the criteria for the selection of the commissioner as provided by this law. The deadline for the vacancy to remain public cannot be shorter than fifteen (15) and longer than twenty (20) days.

4. After the expiration date predetermined in the paragraph 3 of this Article, the selection panel appointed by the parliamentary committee for security of the Assembly of the Republic of Kosovo within fifteen (15) days evaluates if the candidates meet the criteria to be elected a commissioner.

5. The selection panel conducts an interview with each candidate that meets the conditions to be elected a commissioner and according to the submitted data and the interview results, it prepares a shortlist of candidates qualified to be voted by the Assembly of the Republic of Kosovo.

6. The shortlist is composed of three (3) candidates, except in the case when within number three (3) there are more candidates with equal points. The selection panel hands over the short list to the committee, which proposes the same to the Assembly of the Republic of Kosovo. The proposal given by the committee contains the justification why the panel has given priority some of the candidates compared to other candidates.

7. In case of mandate expiration, the commissioner exercises his function until a new commissioner is elected.

Article 61
Termination of commissioner's mandate

1. The Commissioner's mandate shall be terminated in cases when:

1.1. the regular mandate ends;

1.2. resignation;

1.3. his/her death;

1.4. reaches the age of retirement;

1.5. permanent loss of ability to act, ascertained by the competent court;

1.6. becomes incapable due to health reasons which make it impossible to practice the function for more than three (3) months;

1.7. is sentenced by a final court decision for criminal offence which is punishable with more than six (6) months of imprisonment;

1.8. is dismissed.

2. Assembly of Kosovo may, upon the proposal of the functional Committee on security matters, with the majority of all deputies, dismiss the Commissioner due to the following reasons:

2.1. for violation of the provisions of this Law;

2.2. in cases of performing the duties in non-compliance with his/her function.

Article 62
Financing of the Agency

1. Agency shall be financed from the Budget of the Republic of Kosovo, and it shall have its own budgetary line which guarantees its independence.

2. Agency shall prepare the annual proposal-budget in compliance with the Law on Public Financial Management and Accountability.

3. The budget of the Agency shall be subject to the audit in compliance with the legislation into force.

Article 63
Commissioner's salary

1. The level of Commissioner's salary shall be determined in compliance with the relevant Law on Salaries in Public Sector.

2. Until the entry into force of the relevant Law on Salaries in Public Sector, the Commissioner's salary shall be equivalent to the salary of the deputy of the Assembly of Kosovo.

Article 64
Tasks and competencies of the Agency

1. Without harming other duties defined in accordance with this law, the Agency performs the following duties:

1.1. supervises the implementation of this law;

1.2. provides advice to public and private bodies on issues related to data protection;

1.3. informs the public on issues and developments in the area of data protection;

1.4. promotes and supports fundamental rights on personal data protection;

1.5. decides about complaints submitted by data subjects;

1.6. provides advice to the Assembly, the Government, other internal institutions and bodies on legislative and administrative measures in relation to protection of fundamental rights and freedoms of natural persons in terms of data processing;

1.7. carries out inspections regarding the implementation of this law;

1.8. as appropriate, carries out periodical review of issued certifications in accordance

with Article 43 of the Law and may withdraw certification in case certification criteria are no longer met;

1.9. on its own initiative or upon request it provides opinions for public institutions and other bodies, as well as publishes on any issue related to personal data protection.

Article 65
Cooperation with other bodies

1. The Agency shall cooperate with governmental and international institutions, other EU bodies, regarding issues considered important for access to public documents and personal data protection;

2. In particular, the Agency shall apply measures for effective cooperation with supervisory authorities of other countries and international organizations and provides relevant information and mutual assistance in accordance with the applicable law. Mutual assistance covers, in particular, requests for information and supervisory measures, such as requests for carrying out authorizations and consultations, prior inspections and investigations.

3. The Agency, without any delay and not later than one (1) month after the receipt of the request shall take all necessary measures required to respond the request of another supervisory authority. Such measures may include, in particular, transmitting relevant information for conducting investigations.

4. Requests for assistance contain all necessary information, including the purpose and reasons of the request. The exchanged information shall be used only for the purpose for which it has been requested.

5. The Agency shall not reject completion of the request, unless:

5.1. it is not competent for the object of the request or for the measures required to execute; or

5.2. the action upon request would violate this law or other applicable laws.

6. The Agency informs the requesting supervisory authority about the results or when appropriate, on the progress of measures taken to respond the request. The Agency provides reasons for rejecting the request in accordance with paragraph 4 of this Article.

7. The Agency, as a rule, shall provide the information requested by other supervisory authorities by electronic means by using a standardized format.

8. The Agency shall not require any payment for actions taken based on mutual assistance requests in terms of reciprocity.

9. The Agency shall carry out joint operations, when appropriate and in compliance with the law in force, including joint investigations and measures of enforcement where members or the staff of other countries' or international organizations supervisory authorities is included.

Article 66
Annual work report

1. The Agency shall submit an annual activity report on its work the Assembly of the Republic of Kosovo and shall 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 the relevant assessments and recommendations.

Article 67
Publicity concerning work

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

1.1. an internal journal and professional literature;

1.2. any decision of general jurisdiction courts concerning the access to public documents and data protection. In such cases, personal data concerning parties, damaged parties, witnesses or experts involved are not published;

1.3. opinions on the compliance of codes of professional ethics, general terms of business or draft-regulations in the area of personal data protection;

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

1.5. any instruction and recommendation regarding the protection of personal data in individual fields;

1.6. public statements on inspections undertaken in individual cases;

1.7. any other important announcement.

CHAPTER XIV
INSPECTIONS AND AUDITS

Article 68
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 personal 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:

1.3.1. recording of the activities of processing, according to Article 29 of this Law;

1.3.2. notification on the violation of data, according to Articles 33 and 34 of this Law;

1.3.3. impact assessment of data protection, according to Articles 35 and 36 of this Law;

1.3.4. official for data protection, according to Articles 37 to 39 of this Law;

1.3.5. codes of conduct, according to Articles 41 and 42 of this Law;

1.3.6. certification mechanisms, according to Article 43 of this Law; and

1.3.7. recordings of disclosure of the recipient.

Article 69
Direct performance of inspections

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

2. Inspection officers when carrying out inspections and audits shall identify themselves with an official identity card containing photography, his or her personal name, professional title and other necessary information.

3. With Commissioner's proposal, the Government of Kosovo issues a sub-legal act which defines in detail the shape and contents of the card.

Article 70
Responsibilities of inspection officers

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

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 71
Inspection measures

1. If an inspection officer 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:

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 disclose in contravention of legal provisions or international agreements;

1.5. order the controller or the processor meet the requirements of data subjects to exercise his/her rights in accordance with this law;

1.6. impose fines for the violations of this law.

1.7. in minor cases of violations, 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 inspection officer to ensure lawful data processing.

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

Article 72
Obligation to ensure support

1. Public and private bodies shall be obliged to assist inspectors in performing their duties via:

1.1. providing information as a response to the question of the Agency and allowing the inspection of documents and data files, in particular data stored and programs for processing data related to the processing of personal data; and

1.2. allowing access to their facilities at any time.

CHAPTER XV
DIRECT MARKETING

Article 73
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 using 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 the provisions 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 74
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.

CHAPTER XVI
VIDEO SURVEILLANCE

Article 75
General provisions

1. The provisions of this chapter 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. Public bodies shall take appropriate measure to identify the controller. 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. Data collected from video surveillance may be processed or used, if necessary, to achieve the purposes even if there are no indication of the violation of legitimate interests of data subject. These data may be processed or used for other purposes only if necessary to prevent threats against the state and public security or prosecute crimes.

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

Article 76
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 system

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, and 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 one (1) month unless otherwise required for legitimate purposes.

Article 77
Monitoring of apartment buildings

1. For the installation of video surveillance systems in apartment buildings at least seventy percent (70%) of the owners must 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 devices, whether at the same time or later, 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 78
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 and in the working places with the potential of infringing the privacy of the employees.

4. Prior to the installation of video surveillance systems the employer must inform the data subjects in writing about their rights and the reasons for the surveillance. The areas monitored must 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, state security activities of investigation in places where the secret data are protected.

Article 79
Video surveillance by drones

1. Personal data obtained by drones shall be processed in accordance with this law, except for cases when it is stipulated otherwise by respective legislation that determines issues related to the operation of drones.

2. The Agency, together with the Civil Aviation Authority shall issue a sub-legal act on the manner of data processing obtained by use of drones.

CHAPTER XVII
USE OF BIOMETRIC FEATURES

Article 80
Processing of biometric features

Determination and use of a data subject's biometric features and their comparison to allow his or her identification shall be governed by the provisions of this law.

Article 81
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 agreements or for the identification of persons crossing state border.

Article 82
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 84 of this Law shall be applied accordingly (mutatis mutandis).

Article 83
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 must be informed in writing prior to the use of their biometric characteristics, about the intended measures and their rights.

2. If not otherwise provided 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 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. No appeal against the decision from paragraph 3 of this Article is allowed, but an administrative dispute may be initiated in the competent court.

CHAPTER XVIII
RECORDS OF ENTRY TO AND EXIT FROM PREMISES

Article 84
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 shall then be deleted or destroyed, unless otherwise provided by law.

CHAPTER XIX
PUBLIC BOOKS AND PROTECTION OF PERSONAL DATA

Article 85
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.

CHAPTER XX
LINKING FILING SYSTEMS

Article 86
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 (2) 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 87
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 88
Separation of official documents and public books

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

Article 89
Personal data from previous institutions

1. If, prior to 12 June 1999, personal data have been stored from previous institutions mainly for self-assigned administrative tasks to be performed by authorities, institutions and other public state bodies, from the socialist republics, communities, associations of local authorities, or other public bodies, whereby the right to such data shall be bared by the carriers of public administration for administrative duties.

2. Previous institutions, as defined in paragraph 1 of this Article, are former state bodies or economically active bodies, collective combines, operations or commercial objects, as well as social organizations of the former Social Federative Republic of Yugoslavia.

Article 90
Processing personal data from previous institutions

1. The bodies mentioned in Article 89, paragraph 1 of this Law, shall be allowed to process personal data from previous institutions, if:

1.1. the recognition of these data is necessary for legal fulfilment of any task within the scope of responsibilities of these bodies;

1.2. the re-collection of such data requires non-proportional efforts;

1.3. the data subject has not objected processing; and

1.4. competencies and responsibilities of bodies for data processing have been clearly determined;

1.5. personal data which may be processed according to sub-paragraph 1.1 of this Article shall be considered to have been stored in advance for the purpose determined in compliance with Article 89,paragraph 1 of this Law.

CHAPTER XXI
PUNITIVE PROVISIONS

Article 91
General conditions for imposing administrative fines

1. Agency, shall impose a fine for minor offence directly to the data controllers and processors who breach the provisions of this Law when processing data, taking into account the following criteria:

1.1. the nature, gravity and duration of the infringement considering the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

1.2. the intentional or negligent character of the infringement;

1.3. any action taken by the controller or processor to mitigate the damage suffered by data subjects;

1.4. the degree of responsibility of the controller or processor considering technical and organisational measures implemented by them pursuant to Articles 24, 25 and 32 and 33 of this Law;

1.5. any relevant previous infringements by the controller or processor;

1.6. the degree of cooperation with the Agency, to remedy the infringement and mitigate the possible adverse effects of the infringement;

1.7. the categories of personal data affected by the infringement;

1.8. the way the infringement became known to the Agency, particularly, whether, and if so to what extent, the controller or processor notified the infringement;

1.9. if the measures referred to in competencies of the Agency have been previously ordered against the controller or processor concerned regarding the same subject-matter, compliance with those measures;

1.10. adherence to the code of conduct and other internal acts;

1.11. any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

2. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this law, the unified minor offence sanction may not exceed the maximum amount of twice of the highest punishment of a fine determined by this law.

Article 92
General violations of the provisions of this Law

1. The legal person or the person discharging such independent activity shall be punished for a minor offence of twenty thousand (20,000) to forty thousand (40,000) €, if:

1.1. he or she processes personal data without any legal basis or the consent of the data subject according to this law;

1.2. 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 32 of this law;

1.3. he/she processes specific sensitive personal data in contradiction with Article 6, 8 of this Law, or fails to protect them in accordance with Article 7 of this Law; paragraph 4 of Article 8 of this Law.

1.4. if he processes personal data in contradiction to Articles 10 and 12 of this Law;

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

1.6. provides the recipient with personal data contrary to paragraph 3 of Article 8 of this Law;

1.7. he fails to inform the data subject of the processing of personal data in accordance with Articles 10 and 12 of this Law;

1.8. he uses the same connecting code in contradiction with paragraph 3 of Articles 86 of this Law;

1.9. 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 4 of this Law;

1.10. he or she fails to ensure that the filing system catalogue contains the information provided for by Article 29 of this Law;

1.11. he fails to notify the Agency of information regarding the registry of filing systems, according to Article 30 of this Law;

1.12. he acts in contravention with Article 14 of this Law;

1.13. he acts in contravention of Article 46, 49 of this Law transfers of personal data to other countries or international organizations.

2. A fine of two thousand (2, 000) to four thousand (4,000) € shall be imposed on the responsible persons of the legal person or the person discharging independent activities, for violations under sub-paragraph 1.13, paragraph 1 of this Article.

3. A fine between one thousand (1,000) and two thousand (2,000) € shall be imposed for a minor offence on the responsible person of a state body for violation from paragraph 1 of this Article.

4. A fine of four hundred (400) to one thousand (1,000) € shall be imposed for a minor offence on an individual for violation from paragraph 1 of this Article.

Article 93
Violation of the provisions on contractual processing

1. A fine of between twenty thousand (20,000) to forty thousand (40,000) € 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 32 of this Law or does not return personal data in accordance with paragraph 4 of Article 32 of this Law.

2. A fine of one thousand (1,000) to four thousand (4,000) € shall be imposed on the responsible person of the legal person or on the person who practices an independent activity for violations from paragraph 1 of this Article.

3. A fine between five hundred (500) € to two thousand (2,000) € 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) € shall be imposed on an individual who commits an act from paragraph 1 of this Article.

Article 94
Violation of the provisions on security of personal data

1. A fine of eight thousand (8,000) to forty thousand (40,000) € 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 data to ensure an adequate level of security for the protection of personal data according to article 31 of this law.

2. A fine of one thousand (1,000) to four thousand (4,000) € 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 one thousand (1,000) to eight thousand (8,000) € 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 one thousand (1,000) to two thousand (2,000) € shall be imposed on an individual who commits an act from the paragraph 1 of this Article.

Article 95
Violation of the provisions on direct marketing

1. A fine of four thousand (4,000) up to ten thousand (10,000) € 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 73 or 74 of this law.

2. A fine of eight hundred (800) to two thousand (2,000) € 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 four hundred (400) to one thousand (1,000) € shall be imposed for a minor offence on an individual who commits an act from paragraph 1 of this article.

Article 96
Violation of general provisions on video surveillance

1. A fine of four thousand (4,000) to ten thousand (10,000) € 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 75 of this law;

1.2. if the information does not contain the necessary information from paragraph 3 of Article 75 of this Law;

1.3. If he does not protect the video surveillance system and the recordings in contradiction with paragraph 4 of Article 76 of this Law.

2. A fine of eight hundred (800) to two thousand (2,000) € 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 five hundred (500) to two thousand (2,000) € 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 two hundred (200) to eight hundred (800) € shall be imposed for a minor offence on an individual who commits an act from paragraph 1 of this article.

Article 97
Violation of the provisions on video surveillance regarding access to official and business premises

1. A fine of four thousand (4,000) to ten thousand (10,000) € 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 76 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 76 of this law;

1.3. if he does not inform employees in writing from paragraph 5 of article 76 of this law;

1.4. If he stores personal data in contravention of paragraph 7 of article 76 of this law.

2. A fine of five hundred (500) to two thousand (2,000) € 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 five hundred (500) to two thousand (2,000) € 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 two hundred (200) to eight hundred (800) € shall be imposed for a minor offence on an individual who commits an act from the paragraph 1 of this article.

Article 98
Violation of the provisions on video surveillance in apartment buildings

1. A fine of four thousand (4,000) to twelve thousand (12,000) € 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 77 of this law.

2. A fine of four hundred (400) to two thousand (2,000) € 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 of eight hundred (800) to two thousand (2,000) € 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 two hundred (200) to four hundred (400) € shall be imposed on an individual who commits an act from paragraph 1 of this article.

Article 99
Violation of the provisions on video surveillance in work areas

1. A fine of eight thousand (8,000) to forty thousand (40,000) € shall be imposed on a legal person or on a person practicing an independent activity who implements video surveillance systems in work areas in contradiction of article 78 of this law.

2. A fine of two thousand (2,000) to four thousand (4,000) € 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 one thousand (1,000) to two thousand (2,000) € 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 eight hundred (800) to one thousand (1,000) € shall be imposed on an individual who commits an act from paragraph 1 of this article.

Article 100
Violation of the provisions on biometrics in the public sector

1. A fine of eight thousand (8,000) to forty thousand (40,000) € shall be imposed for a minor offence on a legal person or on a person practicing an independent activity who implements biometric measures in contravention of article 81 of this law.

2. A fine of two thousand (2.000) to four thousand (4,000) € for a minor offence from paragraph 1 of this article shall be imposed 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) € shall be imposed on the responsible person of the state body who commits an act from paragraph 1 of this article.

Article 101
Violation of the provisions on biometrics in the private sector

1. A fine of eight thousand (8,000) to forty thousand (40,000) € shall be imposed for a minor offence on a legal person or an independent person who implements biometric measures in contravention of article 83 of this law.

2. A fine of two thousand (2,000) to four thousand (4,000) € 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 102
Violation of the provisions on records of entry and exit

1. A fine of four thousand (4,000) to eight thousand (8,000) € shall be imposed against a legal person or a person who practices an independent activity, if:

1.1. he or she uses entry and exit records as official records in contravention of paragraph 3 of article 85 of this law;

1.2. acts in contravention of paragraph 4 of article 84 of this law;

2. A fine of two hundred (200) to eight hundred (800) € 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 two hundred (200) to eight hundred (800) € 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 two hundred (200) to eight hundred (800) € shall be imposed for a minor offence on an individual who commits a minor offence from paragraph 1 of this article.

Article 103
Violation of the provisions on linking filing systems

1. A fine of one thousand (1,000) to five thousand (5,000) € shall be imposed for a minor offence on the responsible person of a state body, who links filing systems in contravention of article 87 of this law.

2. A fine of eight hundred (800) to two thousand (2,000) € 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 87 of this law.

Article 104
Violation of the provisions on supervision from the responsible person for protection of personal data

1. A fine of eight thousand (8,000) to forty thousand (40,000) € shall be imposed for a minor offence on a legal person:

1.1. if he or she carries out controls in contravention of article 39 of this law;

1.2. If he or she makes an official annotation in contravention of article 39 of this law.

2. A fine of one thousand (1,000) to two thousand (2,000) € 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 one thousand (1,000) to two thousand (2,000) € 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 five hundred (500) to one thousand (1,000) € shall be imposed for minor offences on an individual who commits an act from paragraph 1 of this article.

Article 105
Serious and great violations of legal provisions

If the Agency find there is a serious and great violation of personal data, it may impose a fine from twenty thousand (20,000) € to fourty thousand (40,000) € or in the case of a company or an enterprise it may impose a fine amounting two percent (2%) to four percent (4%) of the general turn over of the previous fiscal year in compliance with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data.

Article 106
Other responsibilities

The imposition 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 and criminal liability as defined in the Criminal Code of the Republic of Kosovo.

Article 107
Fees

The fees for notifications and authorizations according to this law shall be regulated by sublegal act adopted by the Agency.

CHAPTER XXII
TRANSITIONAL AND FINAL PROVISIONS

Article 108
Transfer of assets, rights and obligations, budget and personnel

1. Upon entry into force of this Law, all physical assets, the rights and obligations that derive from the concluded contracts, and budgetary allocations of the State Agency for Protection of Personal Data shall be transferred to the Information and Privacy Agency.

2. Upon entry into force of this Law, the personnel of the State Agency for Protection of Personal Data shall be transferred to the Information and Privacy Agency, together with their positions held, upon acts of appointments, decisions and employment contracts.

3. Information and Privacy Agency shall, within three (3) months from the entry into force of this Law, make official the contracting obligations with the transferred personnel, by issuing new acts of appointments, according to this Law and relevant legislation.

Article 109
Sub-legal acts

1. Sub-legal acts foreseen by this Law shall be issued within six (6) months from the entry into force of this Law.

2. Sub-legal acts that are into force shall continue to be applied until the issuance of new sub-legal acts, provided that they are not in contradiction with this Law.

Article 110
Abrogation

After the entry into force of this Law, the Law No. 03\L-172 on Protection of Personal Data and shall be abrogated.

Article 111
Entry into Force

This Law shall enter into force fifteen (15) days after its publication in the Official Gazette of Republic of Kosovo.

Law No.06/L - 082
30 January 2019

Promulgated by Decree No.DL-59-2019, dated 14.02.2019 President of the Republic of Kosovo Hashim Thaçi.