Law no. 124/2024

On Personal Data Protection[1]

Pursuant to articles 78 and 83, paragraph 1 of the Constitution, with proposal of the Council of Ministers,

THE ASSEMBLY
OF THE REPUBLIC OF ALBANIA

DECIDED:

PART I
GENERAL PROVISIONS

Article 1

Objective

This law sets out rules about protection of individuals in relation to the processing of their personal data.

Article 2

Purpose

The aim of this law is the protection of fundamental human rights and freedoms, and in particularly the right to personal data protection.

Article 3

Material scope

1. This law applies to the processing of personal data wholly or partly by automated means and to the processing of personal data which form part of a filing system or are intended to form part of a filing system when processing is not automatically performed.

2. This law does not apply to the processing of personal data by natural persons for personal of family purposes.

Article 4

Territorial scope

1. This law applies to the processing of personal data:

a) in the context of the activities of a controller or a processor established in the Republic of Albania, regardless of whether the processing takes place in the Republic of Albania or not.

b) of data subject who are located in the Republic of Albania by a controller who is not

[1] *This law is fully aligned with:*
- 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, Official Journal of the European Union, L series, No. 119/1, dated 4.5.2016.
- Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, CELEX number 32016L0680, Official Journal of the European Union, L series, No. 119, 4.5.2016, p. 89.

established in the Republic of Albania, but the processing processes are related to;

i. the provision of goods or services, irrespective of whether compensation of the data subject is required, to such data subjects in the Republic of Albania;

ii. the monitoring of the data subjects 'behavior as far as their behavior takes place within the Republic of Albania;

c) by a controller or processor who is not established in the Republic of Albania, but in a territory where the Albanian law applies by virtue of public international law.

2. When a controller, for the processing processes as determined in letter "b", paragraph 1 of this article, contracts a processor, which is not established in the Republic of Albania, Chapter IV "International data transfer" applies.

Article 5

Definitions

For the purposes of this Law the following terms shall mean:

1. "Competent authority" is the court, the prosecution office and any public body which mandate is the prevention, investigation, detection, or prosecution of criminal offenses or execution of criminal sentences, including the protection and prevention of public security threats, the protection of national security or any other institution which is vested the right to exercise public functions, tasks or powers by law for one or more of such purposes.
2. "Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;
3. "Personal data" means any information relating to a data subject;
4. "Group of companies" is a group where a mother company and its controlled companies participate;
5. "Standard data protection clauses" are standard contracts approved and published by Commissioner, with a view of ensuring an adequate data protection in their international transfers by agreement between the data sender in the Republic of Albania and data receiver in a foreign country or international organization;
6. "Code of Conduct" is a set of rules issued by the Commissioner and designed by category or branch of controllers, processors, in order to regulate with detailed arrangements implementation of rules of this Law in special sectors;
7. "The Commissioner" is the Right to Information and Personal Data Protection Commissioner, which is an independent authority that monitors and supervises the right for personal data protection and acts in compliance with this law;
8. "The Controller" means any natural or legal person and public authority, which, alone or jointly with others, determines the purposes and means of processing personal data; for the processing of personal data as provided in Part III of this Law, the controller is the competent authority which alone or together with others defines the purposes and means of processing of personal data;
9. "Processing restriction" is the marking of stored personal data with the aim of restricting their processing in the future;
10. "Recipient" means a natural or legal person, and any other public authority, to which the personal data are disclosed or made available, be it a third party or not.
11. "Certification mechanism" is list of criteria about legitimate processing according to this law, approved by the Commissioner and implemented by a certifying body in its certification procedures;
12. "International organization" is an organization and its bodies, which are regulated

according to the international public law, or any other body, which has been established based on agreement between two or more states;

13. "Third party" is any natural personal or legal entity or any public authority, except the data subject, the controller, the processor or persons, who, under the direct authority of the controller or the processors, is authorized to process personal information;
14. "Consent" of the data subject means any freely given, 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 for one or more specific purposes;
15. "Representative" means the natural person with the residence or legal entity with the seat, branch or representative office in the territory of the Republic of Albania, designated by the controller or processor for its representation in issues related to the implementation of this Law;
16. "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
17. "Further processing" is processing of the data for another purpose, different from the initial one, defined at the moment of data collection, including the transfer or making the data available for this new purpose;
18. "Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
19. "Profiling" means 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 analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;
20. "Pseudonymization" means the processing of personal data in such a manner that the 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 organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
21. "Binding corporate rules" means personal data protection policies which are adhered to by a controller or processor established in the territory of the Republic of Albania for transfers or a set of transfers of personal data to a controller or processor located in one or more third countries within a group of companies, or group of entrepreneurs and companies conducting a joint economic activity;
22. "Filing system" means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
23. "Data subject" is any identified or identifiable natural person; a person is identifiable if his identification can be achieved by referring directly or indirectly, to one or several identifying factors, such as name, identification number, location data, an online identifier or one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity;
24. "Biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
25. "Genetic data" means personal data relating to the inherited or acquired genetic characteristics of a 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 person in question;

26. "Data concerning health" are the personal data about physical or mental health of a person, including health care provision information, indicating information on his or her health situation;
27. "Criminal records" are the personal data in relation to criminal sentences, criminal offenses and related precautionary measures;
28. "Sensitive data" are special category of personal data, revealing the racial or ethnic origin, political opinions, religious belief or philosophical views, trade union membership, genetic data, biometric data, health records, or a person's sexual orientation;
29. "Anonymized data" are data that were initially personal data, which have been processed in such a way that it is no longer possible for a natural person or legal entity to attribute such data to an identified or identifiable person;
30. "Entrepreneur and company" is a natural person or legal entity engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
31. "Activities in the field of journalism" are activities aimed at publishing information, the thoughts or the ideas, which contribute to the public interest debate, regardless the form of their delivery.

PART II
PERSONAL DATA PROCESSING

CHAPTER 1
PRINCIPLES RELATED TO LAWFUL PROCESSING OF PERSONAL DATA

Article 6

Principle related to lawful processing of personal data

Personal data shall be in compliance with the following principles:

1. Principle of lawfulness, fairness and transparency, which means that the processing is made in a lawful, fair and transparent way vis-a-vis the data subject.
2. Principle of processing in line with the purpose, which means that the personal data are collected for a specified and legitimate purpose, clearly defined at the moment of their collection and are not further processed for another purpose which is not in line with the initial purpose.
3. Principle of data minimization, which means that the personal data are adequate and necessary to the purpose for which they are processed and limited to the necessary amount for achieving the purpose.
4. Principle of data accuracy, which means that the personal data are accurate and up-to–date when this is necessary and having regard to the purposes for which they are processed, all necessary steps are taken for erasure or rectification of inaccurate or incomplete data.
5. Principle of limitation of storage time, which means that the personal data are kept in a way that allows the identification of the data subject for a period no longer than necessary for archiving the purpose for which they are being processed. Personal data may be stored for longer periods provided that they are processed only for filing purposes to the public interest, research, scientific or historical or statistical purposes, in compliance with the necessary technical and organizational measures to protect the data subjects' rights and freedoms.
6. The principle of integrity and confidentiality, which means that the personal data are processed in a manner that ensures appropriate security of the personal data, including

protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures;

7. Principle of accountability, which means that the controller shall be responsible for, and be able to demonstrate compliance with principles provided for in this article.

Article 7

Legal principles for personal data processing

1. Processing shall be lawful only if and to the extent that at least one of the following criteria is met:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

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

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

ç) processing is necessary in order to protect the vital interests of the data subject or of another person;

d) processing is necessary for the performance of a legal task carried to the public interest by the controller or when the controller is vested with the right to exercise public functions, duties or powers as per the applicable legislation;

dh) processing is necessary for the fulfillment of the legitimate interests of the controller or 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 sub-paragraph shall not apply to processing carried out by public authorities in the performance of their tasks as per sub-paragraph “d” of this paragraph.

2. The processing referred to in sub-paragraph “c” and “d” of paragraph 1 of this article 1 shall be implemented in the law. The law shall provide the purpose of the processing or the processing as per sub-paragraph “d” of paragraph 1 of this Article, the purpose of the processing shall be necessary for the performance of a legal duty of public interest or to exercise public tasks, functions or powers which the controller is vested such right as per the applicable legislation. The law shall fulfil a public interest objective, and be proportionate to the legitimate aim it regulates.

3. The Law, as per paragraph 2 of this article may include specific provisions to adjust the implementation of the provisions of this law:

a) the general conditions governing the lawfulness of processing by the controller;

b) the types of data which are subject to the processing;

c) the data subjects concerned;

ç) the entities to, and the purposes for which, the personal data may be disclosed;

d) the processing purpose limitation in line with principle of processing in accordance with the purpose;

dh) personal data storage time periods;

e) processing operations and processing procedures, including measures to ensure lawful and fair processing for other specific situations as provided in Chapter V of this Part.

4.Where the processing for a purpose other than for which the personal data have been collected is not based on the data subject's consent or on a law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in paragraph 1 of Article 21 of this law, the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose which the personal data were initially collected for, take into account, inter alia:

a) any link between the purposes for which the personal data have been collected and the

purposes of the intended further processing;

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

c) the nature of the personal data, in particular whether sensitive or criminal data are processed;

ç) possible consequences of the intended further processing for data subjects;

d) the existence of appropriate safeguards, which may include encryption or pseudonymization.

Article 8

Consent validity criteria

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of 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 the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Law shall not be binding.

3. The data subject may withdraw his or her consent at any time and be informed on such right before providing his consent. The consent withdrawal shall not affect the lawfulness of processing based on pre- withdrawal provided consent. The withdrawal should be as easy as the consent giving is.

4. The consent is not considered as freely given, when there are elements of coercion, pressure or inability to exercise free will, especially when is a consequence of inequalities in conditions between controller and data subjects.

5. 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 consent to the processing of personal data, which is actually not necessary for the performance of that contract.

6. The consensual- based processing the personal data of minors, within the online delivery of goods or services, is legitimate only if the minor is at least 16 years old. When the minor is under the age of 16, the processing is lawful only when consent is given or authorized by his parents or legal custodian, and so as granted or authorized by him.

Article 9

Lawful processing of sensitive data

1. Processing of sensitive data is prohibited.

2. Processing of sensitive data shall be allowed if adequate measures for the protection of data subjects' fundamental rights and interests are in place, and only in cases where:

a) the data subject has given explicit consent for their processing for one or more specified purposes, except where the applicable legislation provides that the prohibition for processing sensitive data may not be lifted by the data subject consent;

b) the processing is necessary for the purposes of carrying out an obligation or specific right of the controller or of the data subject in the field of employment and social security and social protection, including the rights and obligations deriving from a collective agreement pursuant to applicable law in such areas, provided that fundamental rights and interests of the data subject are guaranteed;

c) is necessary to protect the vital interests of the data subject or of another person where the

data subject is incapable of giving consent due to health situation or his legal aptitude has been removed or limited;

ç) is carried out in the course of legitimate activities of non-for-profit organizations with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to members or to former members of the organization or persons who have regular contact with it in connection with its activity and that the personal data are not disclosed outside that organization without data subjects' consent;

d) relates to personal data which are manifestly made public by the data subject and the processing is necessary for the achievement of a legitimate aim;

dh) is necessary for the submission of a request, or exercise or defense of a legal claim, obligation or interest before the court or public authorities;

e) is necessary for the fulfilment of a substantial public interest, which is proportionate to the aim pursued, and respects the essence of the data protection right;

ë) is necessary for preventive medicine purposes or in the context of occupational health, for the assessment of the working capacity of the employee, for medical diagnosis, for the provision, treatment or management of health or health care services on the basis of the law, or pursuant to a contract with a health professional, and provided that the processing is made by employees subject to professional secrecy or an employee under its responsibility or another person subject to professional secrecy.

f) is necessary for reasons of public interest in the area of public health, protection from serious cross- border threats to health or guaranteeing high standards of quality and security of health care of products or medical appliances, as per the applicable legislation which ensure suitable protection measures, in particular the obligation to keep the professional secrecy of the persons processing personal data protection.

g) is necessary for filing purposes for public interests, for historical, research, scientific or purposes statistical, in compliance with article 45 the this the law.

Article 10

Lawful processing of criminal records

The processing of criminal records is carried out only under the control of the competent authority or when the processing is authorized by law, providing adequate protection for the rights and freedoms of the data subjects. The criminal status register is kept under the control and supervision of the Ministry of Justice, in compliance with the applicable legislation.

Article 11

Processing which does not require identification

1. If the purposes for which a controller processes personal data do not require the identification of a data subject by the controller, or such identification is no longer necessary, 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 as applicable. In such cases, 13-20 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 II
RIGHTS OF THE DATA SUBJECT

Section 1
Transparency with the data subjects

Article 12
Communication with the data subject and modality of exercise of the rights by the data subject

1. The controller shall take appropriate measures to provide any information to the data subject and perform any communication as per articles 13- 20 of this law relating to processing to his data in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a minor. 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 article 13-20 of this law. In the cases referred to in article 11 paragraph 2 of this law, the controller shall not refuse to review the request of the data subject for exercising his or her rights, unless he demonstrates that it is not in a position to identify the data subject.

3. When the controller has reasonable doubts related with identity of a person, who submits a request under articles 13–20 of this law, the controller shall request additional information, in order to verify the identity, the data subject.

4. The controller shall inform the data subject with regard to the fulfilment of the request or grounds for its rejection as soon as possible and in any case, no later than 30 (thirty days) from the receipt of the request. This period may be extended up to 60 (sixty) days when necessary, taking into account the complexity and number of requests received. The controller shall reasonably inform the data subject of any such extension within 30 (thirty) days of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject. In cases where the controller does not review the request or refuses to fulfil it, the controller shall, no later than 30 (thirty) days from the receipt of the request, inform the data subject on the reasons for not reviewing or refusing to fulfil the request and the possibility of lodging a complaint with the Commissioner and a lawsuit with the court.

5. The response to the request of the data subject, according to articles 13–20 the this the law, shall be provided free of charge. When requests from the data subject are clearly unfounded or excessive, especially due to their repeated character, the controller can:

a) introduce a reasonable fee, taking into account the administrative costs about provision of information or communication, or about undertaking the requested action; or

b) refuse to undertake actions on the request.

6. The controller has the burden of proving the clearly unfounded or excessive nature of the request.

Section 2
Rights of the Data Subjects

Article 13

The right to information

1. Where personal data are collected with the cooperation of the data subject and the data subject does not have the information referred to below, the controller shall provide him with the following information concerning:

a) the identity and contact details of the controller and, where applicable, the contact details of the representative, and of the controller's data protection officer;

b) the purposes for processing for which the personal data are intended, as well as the legal basis for processing;

c) the existence and rationale of the automatic decision-making and profiling, as per paragraph 1 and 3 of art 20 of this Law, and at least, in those cases, the right information in relation to the respective logic, as well as the right and consequences foreseen of this processing for the data subject;

ç) the envisaged time period for storing the personal data, or if that is not possible, the criteria used to determine such period;

d) the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal when processing is made based on consent and lawful interest of the controller or third party, when processing is made on the basis of a lawful interest.

dh) information whether the data subject is obliged to disclose data and whether the disclosure of personal data is an obligation deriving from the applicable legislation, the contractual terms, or requirements necessary to enter into a contract relation, and the possible consequences of failure to provide such data;

e) the recipients or categories of recipients if any;

ë) whether the data will be transferred to foreign countries and, if so, how adequate protection is guaranteed, including information on appropriate protection measures and the manner in which a copy of them can be obtained or the place where they are provided;

f) the exercise of the rights under articles 14–20 of this Law, as well as the right to file a complaint with the Commissioner.

2. Where personal data are not collected with the cooperation of the data subject, in addition to the information as per pg. 1 of this article, the data subject shall also be informed on the categories of personal data that will be processed, their source, and as applicable, whether they have been obtained from publicly available sources. This information shall not be provided in cases where:

a) the provision of the information is impossible or constitutes an unreasonable effort and the controller has taken appropriate measures to protect the rights and legitimate interests of the data subject;

b) obtaining the data from other sources other than the data subject is expressly provided for by law; or

c) the provision of the information is not permitted due to the obligation to maintain professional secrecy under the law.

3. The above information is provided:

a) before the data subject provides the data, as per pg. 1 of this article;

b) in case of collection of information as per pg. 2 of this article;

i. within a reasonable deadline but no later than 30 (thirty) days after obtaining the personal data; or

ii. if the personal data will be used to communicate with the data subject, no later than the moment of the first communication to the data subject; or

iii. if disclosure to another recipient is envisaged, no later than the moment when the personal data are first disclosed.

4. Where the controller intends to further process and the data subject has not been informed in advance, 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 1 and 2 of this article, as applicable.

5. The obligation to inform under the provisions of this article may also be fulfilled by the processor on behalf of the controller, if authorized by him, provided that the information clearly indicates who the controller is and how he can be contacted.

Article 14
The right to access

1. The data subject shall have the right to obtain from the controller, no later than 30 (thirty days) from the submission of the request, a confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, have access to the personal data and the following information:

a) the purpose of processing;

b) the existence and logic of automated decision-making and profiling, as per paragraphs 1 and 3 of article 20 of this law, and at least in those cases, the right information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

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

ç) legal basis for the processing;

d) the categories of personal data concerned, including in cases where the personal data have not been obtained from the data subject, any available information on the source of such data;

dh) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in foreign countries or international organizations, including when the data are transferred to foreign countries and, if so, how appropriate protection is ensured;

e) the existence of rights under articles 15–20 of this law and the right to lodge a complaint with the Commissioner.

2. The controller shall provide free of charge to the subject a copy of the list of categories of processed data, indicating the content of each category related to the data subject and without affecting fundamental rights and freedoms of other persons. 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.

Article 15
The right to rectification or erasure

1.The data subject shall have the right to obtain from the controller as soon as possible, but no later than 30 (thirty) days from the day of receipt of the request, the rectification of inaccurate personal data concerning him or her. In line with 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.

2.The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her as soon as possible no later than 30 (thirty) days, from the day of receiving the request in the following instances:

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

b) the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing;

c) the data subject objects the processing pursuant to paragraph 1, of article 19 of this law, and there are no overriding legitimate grounds for the processing, or the data subject objects the processing, as per paragraph 2 of article 21 of this law;

ç) the personal data have been unlawfully processed;

d) the personal data have to be erased for compliance of the controller with a legal obligation;

dh) personal data are collected in the context of the online provision of goods or services, according to paragraph 6 of article 8 of this law.

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

a) exercising the right of freedom of expression and information;

b) compliance with a legal obligation which requires processing by applicable law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of a public function vested in the controller;

c) for reasons of public interest in the area of public health in accordance with sub-paragraph "ë" and "f" of paragraph 2 of article 9 of this law;

ç) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, and paragraph 4 of article 45 of this law is applicable, as long as the right to erasure under paragraph 1 of this article can render impossible or seriously harm the achievement of the objectives of such processing; or

d) submission of a request or the exercise or defence of a legal claim, obligation or interest before the court or public authorities.

4. Where data are rectified or erased, the controller shall inform all recipients to whom the data have been disclosed. Where requested by the data subject, the controller shall inform him or her of the recipients of the personal data. These obligations shall not apply only where their fulfilment is impossible or constitutes a disproportionate burden for the controller.

Article 16
The right to be forgotten

1. When the controller has published personal data, and as per article 15 of this law he is obliged to erase them, based on the applicable technology and implementation cost, he shall take reasonable measures, including technical ones, to inform the controllers who are processing such personal data, that the data subject has requested the erasure of each link, copy or reproduction of such personal data.

2. At the request of the data subject, operators of online search engines are obliged to delete from the results appearing after the search based on the name of the data subject, the information which is no longer up-to-date, with the elapse of time, but which, when found, has a significant negative impact on the data subject's reputation.

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 applies:

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

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

c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the submission of a request, or exercise or defence of legal claim, obligation or interest before the court or public authorities; or

ç) the data subject has objected to processing pursuant to paragraph 1 of article 19 of this law. The limitation shall be in force for the period necessary for the verification whether the legal grounds of the controller have precedence on those of the data subject.

2. Where processing has been restricted under paragraph 1 of this article, such personal data shall, with the exception of storage, only be processed:

a) after the data subject's consent has been given;

b) for the submission or a request or exercise or defence of a legal claim, obligation or interest before the court or public authorities;

c) for the protection of the rights of another natural or legal person which override the rights of the data subject; or

ç) for an important public interest.

3. The data subject shall be informed by the controller before the restriction of processing is lifted.

4. If the controller rejects the request, the data subject may lodge a complaint with the Commissioner and request a preliminary decision on the restriction of processing. If necessary and proportionate, the Commissioner shall issue a preliminary restriction order, in accordance with article 83 of this law, no later than 14 days from the submission of the request.

5. Where the processing of data is restricted, the controller shall inform all recipients to whom the data in question have been disclosed before the restriction.

Article 18
Right to data portability

1. When the personal data are given to a controller by the data subject, with his approval or for the fulfillment of a contract, and the processing is made through automated means, the data subject shall have the right to receive them from the controller, in a structured, commonly used and machine-readable format, and transmit them to another controller.

2. In exercising his or her right, as per 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 on data portability shall not prejudice the right to their erasure as per art 15 of this law. The right to data portability may not be exercised when the data processing is necessary for the performance of a task carried out in the public interest, or when the controller is vested to exercise public functions, tasks or powers based on applicable legislation.

4. The exercise of the right on data portability shall not adversely affect the rights and freedoms of others.

Article 19
The 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 sub-paragraphs “d” and “dh” of article 7 of this law, including profiling based on them. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, especially when they are related with the submission of a request, or the exercise or defence of legal claim, obligation or interest before the court or public authorities.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time and without the need to explain the reasons, to the processing of his personal data for such purpose, which includes profiling to the extent that it is related to it.

3. Following the exercise of the right as per paragraph 2 of this article, the controller shall be obliged to halt the personal data processing for such purpose.

4. The right to object the processing of the personal data for the purposes referred to in article 44 of this law shall be limited to those processing actions which are not necessary for the performance of a task of public interest.

5. At the latest at the time of the first communication with the data subject, the controller shall inform the data subject on the right to object, as per paragraphs 1 and 2 of this article, explicitly and clearly and separately from any other information.

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

Article 20
The right not to be subject to automated decisions

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

2. Paragraph 2 shall not apply if the decision:

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

b) is authorized by 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

c) is based on the consent of the data subjects whom the data belongs to.

3. The processing of the sensitive data for automatic decisions is made through the expressed clear consent of the data subject or should be based on a legal provision, in line with sub-paragraph “e” of paragraph 2 of article 9 of this law, and provided that suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests are in place.

4. In the cases referred to in paragraph 2 and 3 of this article, the controller shall implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, as well as the right of the data subject to obtain manual intervention on the part of the controller, to express his or her point of view and to contest the decision.

Section 3
Restrictions

Article 21
Restrictions of the data subjects' rights

1. The scope of application of the rights foreseen in article 13-20 of this law and of the obligations deriving for the controller, as well as art 6 of this law, in so far as its provisions correspond to the rights and obligations provided for in articles 13-20 of this law, may be restricted by law. The restriction shall respect the essence of the fundamental rights and freedoms and be a necessary and proportionate in a democratic society to safeguard national security, public security or economic interests of the country for the prevention of turmoil or criminal offenses or the protection of rights and freedoms or third parties.

2. In particular, the law, as per paragraph 1 of this article, shall include specific provisions at least, where relevant, as to:

a) the purposes of the processing or categories of processing;

b) the categories of personal data;

c) the scope of the restrictions;

ç) the safeguards to prevent abuse or unlawful access or transfer;

d) the specification of the controller or categories of controllers;

dh) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

e) the risks to the rights and freedoms of data subjects; and

ë) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

CHAPTER III
OBLIGATIONS OF THE CONTROLLER AND PROCESSOR

Section 1
Responsibility

Article 22
General responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of occurrence and escalation of the risk for the human rights and freedoms, the controller shall implement the appropriate technical and organizational measures to ensure and to be able to demonstrate that the processing is performed in accordance with this law. Those measures shall be reviewed and updated where necessary.

2. Based on paragraph 1 of this article the controller shall take measures for the implementation of data protection by design in its processing processes and data protection by default way in accordance with this article and article 23 of this law. The designation of a data protection officer is taken into account despite the criteria defined in article 33 of this law, especially when the processing processes of the controller, constitute other significant risk factors, other than those referred to in paragraph 1 of article 33 of this law.

3. The implementation of the Code of Conduct, according to article 35 of this law or of the certification mechanism, according to article 37 of this law, may be used as an element through which compliance with the obligations of the controller is demonstrated.

4. Controllers and processors are obliged to cooperate, when requested by the Commissioner, in order to carry out his duties.

Article 23
Data protection by design and by default

1. The controller, both at the moment of the design of processing tools, as well as during the processing shall implement appropriate technical and organizational measures for the implementation of necessary protection measures in its processing actions, such as: pseudonymization of the data designed to implement the principles of personal data protection, as it is the data minimization in an effective way and to integrate the necessary protection measures in processing, so that the requirements of this law are met, as well as to protect the rights of the data subjects. For this purpose, the controller shall take into account technological developments, the costs of implementation, the nature, object, circumstances and purposes of the processing, as well as the likelihood of the risk of infringement of fundamental rights and freedoms, which the processing operations present.

2. The controller shall implement appropriate technical and organizational measures to ensure that, in a predetermined manner, only personal data which are necessary for each specific purpose of the processing are processed. This obligation shall apply to the amount of personal data collected, to the extent of the processing, to the period of storage and to their accessibility. In particular, these measures shall ensure that personal data are not accidentally made accessible without the intervention of the individual to an indeterminate number of persons.

3. In order to prove the implementation of the obligations laid down in paragraph 1 and 2 of this article, the controller may rely on an approved certification mechanism, in accordance with article 37 of this law.

Article 24
Joint controllers

1. Joint controllers are two or more controllers who jointly determine the purposes and means of processing. Joint controllers are designated in a transparent manner through a written agreement, the relation established between them and the responsibilities of each controller for the fulfilment of the obligations deriving from this law, and especially as regards the exercise of the rights of the data subject and the respective duties of the controllers in line with Chapter II of this law.

2. The main part of the agreement is made available to data subjects.

3. The agreement may designate a contact point for the data subjects. Irrespective of the terms of the agreement, the data subject may exercise his or her rights under this law against each of the controllers.

Article 25
Representative of the controller or processor

1. With regard to processing processes defined in sub-paragraph “b” of paragraph 1 of article 4 of this law, the controller or processor shall appoint a representative located in the Republic of Albania and shall notify the Commissioner in writing on the identity of the representative.

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

a) processing which is occasional, does not include, on a large scale, processing of sensitive data or criminal records, and is unlikely to result in a risk to the fundamental human rights and freedoms, taking into account the nature, context, scope and purposes of the processing; or

b) a public authority or body.

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

4. The designation of a representative by the controller or processor shall not prevent the complaint that may be brought against the controller or the processor themselves.

Article 26
Processor

1. Where processing is carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing is made in accordance with this law and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without the prior specific or general written authorisation of the controller. In the case of a general written authorisation, the processor shall inform the controller of any changes he intends to make regarding the adding or replacing other processors, giving the controller the opportunity to object to such changes.

3. The processor shall carry out the processing based on a written contract, a law or sub-legal act 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. The contract, the law, or the sub -legal act should define that the processor:

a) processes and especially transfers personal data only based on written instructions from the controller, unless required to do so based on the applicable legislation 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 disclosure on important grounds of public interest;

b) ensures that persons authorized to process the personal data are subject to the obligation to preserve confidentiality as per article 30 of this law and other regulations governing the professional activity: or are under an appropriate statutory obligation of confidentiality;

c) takes all measures required pursuant to article 28;

ç) respects the conditions referred to in paragraphs 2 and 4 of this article for engaging another processor;

d) taking into account the nature of the processing, assists the controller by appropriate technical and organizational 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 laid down in Chapter II of this law;

e) assists the controller in ensuring compliance with the obligations deriving from Chapter III of this law, in particular articles 28 and 29 of this law, taking into account the nature of processing and the information available to the processor;

ë) depending on the instruction 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 the personal data storage is required by law;

f) 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 and immediately inform the controller if, in its opinion, the instruction given by the controller infringes this law.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, he shall be subject to the same data protection obligations as set out in paragraph 3 of this article, my means of a contract, law or sub-legal act which provides sufficient guarantees that the processing is in compliance with the requirements of this law. The initial processor shall remain fully liable to the controller in case the other processor fails to fulfil his data protection obligations.

5. Adherence to the Code of Conduct, as per article 35 of this law, is the mechanisms of certification as per article 36 of this law may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this article.

6. Without prejudice to the right to contractual freedom between the controller and the processor, the contract, the law or sub-legal act may be based, in whole or in part, on standard contractual clauses referred to in paragraph 7 of this article, including when they are part of a certification granted to the controller or processor pursuant to articles 37 and 38 of this law.

7. The Commissioner may lay down and publish standard contractual clauses on aspects referred to in paragraph 3 and 4 of this article.

8. In a processor infringes the provisions of this article, by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 27

Record – keeping duty

1. Each controller and, where applicable, the controller's representative, shall maintain records of his processing activities in order to be able to provide information on the compliance with this law. Such record shall be kept in written and electronic format. The data kept by the controller shall include the following information:

a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

b) the purposes of the processing of the personal data;

c) a description of the categories of data subjects and of the categories of personal data;

ç) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations;

d) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in sub-paragraph "b" of paragraph 1 of article 41 of this law, the documentation of suitable safeguards;

dh) where possible, the envisaged time limits for erasure of the different categories of data

e) where possible, a general description of the technical and organizational security measures applied in the premises of the controller.

2. The processor and, where applicable, his representative shall maintain in manual and electronic format the data of categories of processing activities and carried out on behalf of a controller, containing:

a) the name and contact details of the processor and, where applicable, of the data protection officer;

b) the name and contact details of any controller on whose behalf the processor acts;

c) the names and contact details of officers engaged for specific tasks;

ç) a description of the categories of processing activities carried out on behalf of each controller;

d) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization, as well as the legal basis, in accordance with Articles 40-42 of this Law, for such transfers;

dh) if possible, a general description of the technical and organizational security measures implemented on the premises of the processor.

3. The controller or the processor shall make the data available to the Commissioner on request.

4. The obligations referred to in paragraphs 1 and 2 of this article shall not apply to com panies or organization employing fewer than 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 sensitive data or criminal records.

Section 2
Security of processing

Article 28
Measures to guarantee the security of processing

1. Taking into account the technological developments, the costs of implementation and the nature, scope, context and purposes of processing as well as potential of occurrence and escalation of the risk and rights and freedoms of persons, the controllers and processors shall implement appropriate technical and organizational measures, to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymization and encryption of personal data;

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

c) the ability to restore the availability and access to personal data within a reasonable time in the event of a physical or technical incident;

ç) a process for regularly testing, reviewing and evaluating the rule of efficiency of technical and organizational measures for ensuring the security of the processing.

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

3. Adherence to the Code of Conduct, as per article 35 of this law or of the certification mechanism as referred to in article 37 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 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 under the applicable legislation.

Article 29
Notification of a personal data breach

1. In the case of a personal data breach, the controller shall as soon as possible, but no later than 72 hours, after having become aware of it, notify the notify the Commissioner. Such notification shall not be made where there the data breach is unlikely to endanger the rights and freedoms of data subjects. Where the notification is not made within such deadlines, the controller shall present the Commissioner the reasons for the delay of notification.

2. The processor shall notify the controller immediately after becoming aware of any personal data breach.

3. The controller shall inform the data subject, for the risk arising from the data breach and the infringement of their rights and freedoms are likely to be high as per paragraph 4 of this article. The performance of the notification of the data subject, is not necessary in cases where:

a) the controller has implemented appropriate technical and organizational protective measures, and these measures have been applied to the personal data affected by the security breach, including encryption;

b) the controller has taken additional measures to ensure that the risk of infringement of the fundamental rights and freedoms of data subjects is low;

c) the controller publishes the notice or takes other similar measures by which data subjects are notified in a uniform and effective manner of the personal data breach, where the notification of each personal data subject constitutes a disproportionate burden for the controller.

4. The notification for the Commissioner, as per paragraph 1 of this article should at least:

a) 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;

b) communicate the name and contact details of the data protection officer or other contact point;

c) describe the likely consequences of the personal data breach;

ç) 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.

5. Where all the information specified in paragraph 3 of this article cannot be made available at the same time, it may be made available at a later stage and as soon as possible.

6. The controller shall document any personal data breach, including the facts, its effects and the corrective measures taken in order for the Commissioner to verify compliance with this article.

7. The Commissioner shall respond to the notification in accordance with his/her competences under Part IV of this law. He/she may oblige the controller to also communicate the personal data breach to the data subjects concerned where the breach is likely to result in a high risk to their rights and freedoms and where the controller has not carried out such communication.

Article 30

Data confidentiality

1. Every person, whether a controller, processor or employee of a controller or processor, shall maintain the confidentiality of personal data to which he has access for professional reasons and shall only disclose them to third parties in accordance with the law and, in particular, with paragraph 2 of this article. This obligation shall be provided for in any contract with a processor pursuant to article 26 of this law and in all employment contracts of a controller or processor.

2. Processors engaged by the controller and any person acting under the authority of the controller or processor who has access to personal data shall process those data only on instructions from the controller or the processor engaged by the controller, except where processing is required by specific law. Controllers and processors shall establish written rules concerning the authority to give instructions for processing and shall make them known to all persons concerned.

3. The obligation to keep data confidential in accordance with paragraphs 1 and 2 of this article shall continue beyond the end of the contract between the controller and the processor, as well as beyond the termination of the employment relationship with the controller or the processor.

Section 3
Impact assessment and prior consultation

Article 31
Data protection impact assessment

1. Where a type of processing, in particular processing 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 infringement of the rights and freedoms of the person, the controller shall, prior to the processing stats, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. For similar actions categories posing a similar risk it is sufficient to only perform a single assessment.\

2. When the controller performs certain processing actions, required by law which also defines also the data and processing actions in question, and when an impact assessment has been carried out in the framework of the adoption of the law, a further impact assessment is not required.

3. The impact assessment shall contain at least:

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

b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1 of this article; and

ç) 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.

4. Where a data protection officer has been appointed, the controller shall consult the officer when carrying out the data protection impact assessment.

5. 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.

6. The performance of the personal data protection impact assessment shall be carried out in particular in the case of:

a) a systematic and in-depth evaluation of personal aspects relating to individuals, which is based on automated processing, including profiling, and on which decisions are based which produce legal consequences or similar significant consequences concerning the individual;

b) the processing on a large scale of sensitive data or criminal records; or

c) a systematic monitoring of a publicly accessible area on a large scale.

7. The Commissioner shall draw up lists of types of processing operations for which a data protection impact assessment must be carried out and for which such an assessment must not be carried out, and shall publish them on the official website.

8. In assessing the impact of processing operations carried out by the controller or processor, the implementation of codes of conduct, pursuant to article 45 of this law, shall be taken into account, in particular for the purposes of data protection impact assessment.

9. 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 32

Prior consultation

1. If following the data protection impact assessment is concluded that in absence of risk mitigating or eliminating measures, processing poses a high risk for the infringement of fundamental rights and freedoms, the control shall, before commencing the processing, seek the opinion of the Commissioner.

2. When he considers that the intended processing would infringe this law, and in particular where the controller has not identified or has failed to take the necessary risk mitigating or eliminating measures, the Commissioner shall provide his written opinion to the controller and, may exercise his powers referred to in 83 of this law.

3. The Commissioner shall provide his opinion as soon as possible but no later than 60 days from receiving the request for an opinion. Depending on the complexity of the intended processing, the Commissioner may decide to extend such time period, but by no more than 45 days. The reasoned decision on the extension of the time period shall be notified to the controller, within 30 days from the date of receipt of the request for an opinion. When during the process of advice, the Commissioner has requested information from the controller, the periods shall be suspended until the Commissioner has obtained the information.

4. In the request for an opinion, the controller shall make available to the Commissioner, information especially on:

a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of commercial companies;

b) the purposes and means of the intended processing;

c) the nature and effects of the suspected risks;

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

d) contact details of the data protection officer;

dh) any other information requested by the Commissioner.

5. Notwithstanding paragraph 1 of this article, the controllers shall consult with, and obtain prior authorization from the Commissioner, in relation to processing to be performed by the 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.

Section 4
Data protection officer

Article 33

Obligation to designate a data protection officer

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

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

b) 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

c) the core activities of the controller or the processor lead to processing on a large scale of sensitive data or criminal records.

2. A group of commercial companies, may appoint a single data protection officer, who is easily accessible from each group member.Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several public authorities, taking account of their organizational structure and size.

3. In cases other than those provided for in point 1 of this Article, the controller, the processor, associations or other representative bodies of a category of controllers or processors may or, where provided for by law, must appoint a data protection officer.

Article 34

Tasks and positions of the personal data protection officer

1. The personal data protection officer has the following tasks:

a) gives advice, when required, to steering bodies of the controller or processor in all data protection -related issues;

b) participates in the impact assessment activities pursuant to article 31 of this law;

c) informs and advises the staff of the controller or processor on data protection, including awareness-raising and training of staff involved in processing operations;

ç) monitors compliance with this law, with other applicable provisions on personal data protection, and policies of the controller or processor in relation to the personal data protection, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations and relevant audits;

d) cooperates with and serves as a contact point for the Commissioner;

dh) in the exercise of his duties and based on the nature, object, circumstances and purposes of the processing, pay due attention to the risk of infringement of fundamental rights and freedoms, which may be caused by the processing of personal data.

2. The data protection officer shall be designated on the basis of certified professional qualities and, in particular, good knowledge of data protection law and practices and the ability to fulfil the tasks referred to in paragraph 1 of this article. The data protection officer may be a staff member of the controller or processor, or a person whom a service contract has been entered with. The data protection officer may have other responsibilities and duties, but the controller or processor shall ensure that these responsibilities and duties do not cause a conflict of interest with the duties of the data protection officer.

3. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the Commissioner. The data subjects may contact the data protection officer for all matters related to the processing of their personal data and the exercise of their rights under this law.

4. The controller and the processor shall ensure that the data protection officer is involved, in a timely manner and in all matters relating to the personal data protection, and has the necessary resources to fulfil his or her duties. The data protection officer shall be subject to the obligation of secrecy and confidentiality in relation to the performance of his or her duties.

5. The controller and the processor shall ensure that the data protection officer does not receive instructions in relation to the performance of his or her duties and is not dismissed or penalized by the controller or the processor for the performance of his or her duties under this law. The data protection officer shall report directly to the highest management level of the controller or the processor.

6. Data protection officers may organize a Network of Data Protection Officers. The “Network” is organized and operates in coordination with the Commissioner. Their training is carried out by the Albanian School of Public Administration, domestic/foreign higher education institutions or international professional organizations with a focus on personal data protection.

Section 5
Codes of conduct and certification

Article 35
Codes of Conduct

1. Associations and other bodies representing categories of controllers or processors may develop codes of conduct, for the purpose of specifying the application of this law, as with regard to:

a) fair and transparent processing;
b) the legitimate interests of the controllers in specific contexts;
c) the collection of personal data;
ç) the pseudonymization of personal data;
d) the information provided to the public and to data subjects;
dh) the exercise of the rights of data subjects;
e) the information provided, the protection of the minor in the manner in which the consent of the minor legal custodian is to be obtained;
ë) the measures and procedures referred to in articles 22 and 25 and the measures to ensure security of processing referred to in article 28 of this law;
f) the notification of the Commissioner and of the data subjects for breaches to personal data;
g) the transfer of personal data to third countries or international organizations; or
gj) extra - judicial dispute settlement between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects to submit a complaint pursuant to Part V of this law.

2. The code of conduct shall contain mechanisms which allows the monitoring body to carry out, without prejudice to the tasks and powers of the Commissioner, the supervision of the processing, the mandatory monitoring of compliance with provisions of the code, by the controllers or processors, who have undertaken to apply it.

3. Associations or other representative bodies shall submit the draft code and any proposal for its amendment to the Commissioner which approves it when finding that the code provides sufficient appropriate safeguards.

4. After the code is approved by the Commissioner, the drafter proposes one of the monitoring bodies, accredited by the Commissioner, according to article 36 of this law, to monitor its implementation. The code shall be implemented after the Commissioner appoints the monitoring body.

5. The Commissioner shall register and publish on the official website the approved codes together with the designated monitoring bodies.

Article 36
Monitoring bodies

1. A private law subject may be accredited by the Commissioner for the monitoring of the compliance with the code of conduct when it:

a) demonstrates its independence and expertise in relation to the subject-matter of the code to the satisfaction of the Commissioner;

b) establishes procedures for assessing the capability of the controllers and processors to apply the code of conduct, the monitoring of compliance of their activity with the provisions of the Code and to periodically review its operation;

c) establishes procedures and responsible 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

ç) demonstrates that the responsibilities and tasks do not result in a conflict of interests.

2. The Commissioner shall define by means of a guideline the criteria to be accredited as a monitoring body;

3. Without prejudice to the tasks and powers of the Commissioner, the monitoring body in accordance with the appropriate safeguards, shall take appropriate action in cases of infringement of the code by a controller or processor, who has committed to comply with the code, including suspension or exclusion of the controller or processor concerned from the code. The monitoring body shall inform the Commissioner on such measures, and on the reasons for taking them. The Commissioner may revoke such measures at any time.

4. The Commissioner shall revoke the accreditation when the monitoring body has not, or no longer meets the conditions for accreditation or where actions taken by it infringe this law.

5. This article shall not apply if the processing is carried out by a public authority.

Article 37
Certification

1. The Commissioner shall define, by a guideline, the general criteria required for the certification and provision of seals and marks of data protection. These instruments prove that the action of processing or all processing actions of a controller or processor have passed the certification process. Data protection seals and marks serve to enable controllers and processors to demonstrate compliance with this law.

2. The application for certification shall be made by the entity itself and the certification shall be granted through a transparent process. The controller or processor, who submits the processing operations for certification, shall provide the certification body referred to in article 38 of this law with all the information and access to the processing activities, which are necessary for carrying out the certification procedure.

3. Without prejudice to the powers of the Commissioner and after he has been informed by the certification body, in order to exercise his powers, the processing operation to be certified shall be checked by the certification body whether it meets all the requirements of the certification mechanism approved by the Commissioner in the framework of the accreditation of the certification body, in accordance with article 38 of this law. Obtaining certification in accordance with this article confirms that the certified processing operation is carried out in accordance with a certification mechanism approved by the Commissioner.

4. Data protection seals and marks may only be used by controllers or processors that have obtained the appropriate certification for the processing operations.

5. Certification shall not exclude or limit the responsibility of the controller or processor for the implementation of this law nor the duties and powers of the Commissioner.

6. The certification issued to a controller or processor shall be valid for no more than three years and may be renewed under the same conditions if the specified criteria are met.
The certification shall be revoked by the responsible certification body when the criteria for certification have not or are no longer met.

7. Certification bodies shall provide the Commissioner with the reasons for granting or revoking a certification.

Article 38
Certification bodies

1. Certification may be provided only by the certification bodies, which have been accredited by the General Directorate of Accreditation, in line with this law, as well as law no. 116/2014 "On accreditation of the bodies for the assessment of conformity in the Republic of Albania". Accreditation shall be granted if the applicant body meets the criteria set out in paragraph 2 of this article, as well as additional criteria, which shall be determined by guideline of the Commissioner. Accreditation shall be issued for a maximum period of 5 (five) years and may be renewed under the same conditions as the initial accreditation.

2. A certifying body shall:

a) have the appropriate level of knowledge regarding the handling of certification, seals or marks, as well as regarding the implementation of data protection for the subject matter, subject to certification;

b) prove independence and engage in the exercise of his responsibilities and duties in a manner that does not cause a conflict of interest;

c) present a certification mechanism, consisting of documenting the criteria and procedures that will be applied for the assessment of processing processes and the issuance, periodic review and revocation of data protection certification, seals and marks;

ç) engage in respecting the certification criteria, determined by the Commissioner's guideline, in accordance with paragraph 1, of article 37 of this law, and the certification mechanism, approved by the Commissioner in the framework of the accreditation of the certification body;

d) establish procedures and structures responsible for examining complaints about violations of the certification procedure or the manner in which certification has been implemented, or is being implemented, by the controller or processor, and to make these procedures and structures transparent to data subjects and the public.

3. The certification bodies shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this law.

4. The General Directorate of Accreditation, based on the proposal of the Commissioner, revokes the accreditation of a certification body when the conditions and criteria for accreditation are not or are no longer met or if the measures taken by the certification body violate this law.

CHAPTER IV

INTERNATIONAL DATA TRANSFER

Article 39
General principles

1. The transfer of personal data which are undergoing processing or are to be processed after transfer to a third country or to an international organization, as well as the further transfer of the personal data, from a third country or an international organization to another third country or to another international organization shall be performed, only if the adequate protection of the data at destination is ensured, or it is specifically ensured for that transfer, in accordance with this chapter. All provisions of this chapter shall be applied in such a way as to ensure that the level of protection of personal data guaranteed by this law is not compromised by the international transfer of data.

2. Court decisions, as well as decisions of administrative bodies of a foreign state, which establish the obligation for a controller or processor to transfer or disclose personal data, may be recognized or enforced only if they are based on an international agreement, such as a treaty on mutual legal assistance in force between the requesting foreign state and the Republic of Albania, without prejudice to the other criteria for transfer provided for in this chapter.

Article 40

Data transfer on the basis of an adequacy decision

1. A transfer of personal data to foreign countries or international organizations shall be allowed where the recipient is in a state, territory, or is part of one or more certain sectors within a foreign state or an international organization, which ensures adequate level of protection of personal data as per paragraph 2 of this article.

2. The level of personal data protection for a given country, territory or sector or international organization shall be determined by a decision of the Commissioner, which shall be published in accordance with paragraph 1 of article 85 of this law.

3. The level of protection of the personal data in a foreign country or international organization shall be defined taking into account:

a) existence and implementation of the legislation in the area of data protection;

b) all circumstances related to the rule of law and respect for human rights and fundamental freedoms;

c) existing legislation and its implementation in the area of national security and public order and including criminal law;

ç) data protection area, especially the existence of an effective system for stipulating and implementation of the data subjects rights, including the existence and effective functioning of one or more independent supervisory authorities in a third country or to which an international organization is subject, vested with responsibility for ensuring and enforcing the data protection rules, including appropriate powers for their enforcement, for assisting and helping the data subjects in exercising their rights and for cooperating with supervisory authorities of other countries, as well as effective administrative and legal remedies; and

d) international commitments of the country or international organization, membership in international instruments and the obligations arising therefrom, as well as participation in multilateral or regional systems, in particular with regard to the protection of personal data.

4. The Commissioner shall monitor developments in those countries or international organizations which have been assessed as having an adequate level of protection of personal data and shall revise his decisions accordingly.

Article 41

Transfer of data in absence of an adequacy decision

1. In the absence of a decision on adequacy, a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. The appropriate safeguards may be provided for, without requiring any specific authorization from a supervisory authority, by:

a) a legally binding and enforceable instrument between public authorities or bodies;

b) binding rules of group of companies adopted by the Commissioner;

c) a data protection standard close, published by the Commissioner;

ç) a code of conduct, adopted by the Commissioner, together with binding and enforceable commitments of the recipient in a country without appropriate safeguards of data or at an international organization, to implement adequate safeguards including as regards data subjects' rights; or

d) a certification mechanism, approved by the Commissioner, together with binding and enforceable commitments of the recipient in a country without adequate data protection or in an international organisation, to implement appropriate safeguards, including the rights of data subjects.

2. Subject to the authorization by the Commissioner, the suitable safeguards may be foreseen also in particular, through:

a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organization; or

b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject's rights.

3. In the absence of an adequacy decision or of appropriate safeguards in accordance with paragraph 1 of this article, including binding company group rules, a transfer or set of transfers of personal data to a third country or an international organisation shall only take place if one of the following conditions apply:

a) the data subject has given his or her informed and explicit consent to the proposed international data transfer, having been clearly informed of the risks of the transfer;

b) the transfer is necessary for the performance of a contract between the data subject and the controller, for the implementation of pre-contractual measures taken at the request of the data subject or the transfer is necessary for the conclusion, or performance, of a contract between the controller and a third party in the interests of the data subject;

c) the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically unable to give consent, or where the right to act has been withdrawn or restricted;

ç) the transfer is necessary for reasons of important public interest;

d) processing is necessary for the establishment, exercise or defence of a right, obligation or legitimate interest before a court or public authority;

dh) the transfer is made from a register which is by law open to consultation and provides information to the general public, provided that the transfer only includes certain information and not entire sections of the register.

4. Where a transfer cannot be based on a provision in article 40 of this law, or paragraph 1 of this article, including the provisions on binding rules of the group of commercial companies, and none of the exceptions for a specific situation referred to in sub-paragraph "a" of paragraph 2 of this article is applicable, a transfer to a third country or an international organization may only be made if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of the legitimate interests pursued by the controller, which do not override the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the transfer of data and, on the basis of that assessment, has provided appropriate safeguards with regard to the protection of personal data. The controller shall inform the Commissioner of the transfer. The controller, in addition to providing the information referred to in articles 13 and 14 of this law, shall inform the data subject of the transfer and of the compelling legitimate interests pursued.

5. Sub-paragraphs "a" and "b", of paragraph 3 and paragraph 4 of this article, shall not apply to activities carried out by public authorities in the exercise of their public functions, duties or powers.

Article 42
Mandatory rules of group of companies

1. The Commissioner may approve binding company rules which provide for rules on personal data processing within the group of companies or group of entrepreneurs and companies conducting joint economic activity, provided that such rules met the following requirements:

a) are binding and apply to each of member of the companies or group of entrepreneurs and companies which conduct joint economic activity, including their employees;

b) expressly confer rights on data subjects with regard to the processing of their personal data; and

c) include provisions as per paragraph 2 of this article.

2. The binding rules for the group of companies shall specify at least:

a) the structure and contact details of the group of companies, or group of entrepreneurs and companies conducing joint economic activity and of each of its members;

b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the country, foreign country or international organizations in question;

c) the binding nature of rules of group of companies, both internally and externally;

ç) the application of the general data protection principles, as specified in article 6 of this law;

d) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions, based solely on automated processing, including profiling, the right to lodge a complaint with the competent supervisory authority and before the competent courts in line with Article 88 of this law, the right to rectification and, where appropriate, compensation for a breach of the internal binding rules;

dh) the acceptance by the controller or processor, established on the territory of Republic of Albania, part of the group of companies, of liability towards data subjects in the Republic of Albania, for any breaches of binding rules of the group of companies by any group member which is not established in the Republic of Albania, unless the Albanian controller or processor proves that the member concerned is not responsible for the event giving rise to the damage;

e) the mechanisms established within the group of companies or the group of entrepreneurs and companies conducting joint economic activities to ensure compliance with the rules, such as the appointment of the data protection officers, training of employees, the performance of audits, the mechanisms for reporting and recording the breaches or rectifying actions;

ë) the mechanisms for reporting and recording changes to the rules and reporting those changes to the Commissioner or supervisory authority;

f) the cooperation mechanism with the supervisory authority, including the mechanisms for reporting any legal criterion applicable to any group member in a foreign country, and which might have a serious negative impact to the safeguards stipulated in the bidding rules of the group of companies.

CHAPTER V
DATA PROCESSING FOR SPECIFIC PURPOSES

Article 43
Personal data processing and freedom of expression

1. In order to harmonize the right to the protection of personal data with freedom of expression and information, including processing of personal data for journalistic and academic, artistic and literary purposes, to the extent necessary and proportionately, exception by provisions of this the law, may be applied, provided that:

a) the controller has the purpose to publish journalistic, academic, literary or artistic materials,

for which preparation personal data are needed;

b) the controller does not process personal data for any purpose other than those provided for in sub-paragraph "a" of this paragraph;

c) publication the material in a specific case shall be in the public interest;

ç) the implementation of the provisions of this law may make it impossible or seriously jeopardize the achievement of the controller's objective;

d) no to violate the essence of the rights and the freedoms of the data subjects.

2. When the controller applies to the exception under paragraph 1 of this article, he shall store the personal data only for the time needed to publish journalistic, academic, literary or artistic materials and shall disseminate them only:

a) in the form of published journalistic, academic, literary or artistic material;

b) to recipients, who help him in the preparation of journalistic, academic, literary or artistic material which he intends to publish;

c) to recipients, who are potential publishers of this material; or

ç) when required for the submission of a legal claim, obligation or interest to the court of public authorities.

3. When publishing a journalistic, academic, literary or artistic material, which is prepared based on the exceptions under paragraph 1 of this article, the controller must not publish information on the basis of which, directly or indirectly, the following may be identified:

a) a minor, except for when:

i. the consent of the parent or the legal guardian of the minor has been obtained; or

ii. it is so permitted by the court;

b) the victim or person, who claims to have been damaged by the commission of criminal offenses, except in cases where:

i. the consent of the victim or the person, who claims to have been damaged by commission of the criminal offense has been obtained;

ii. it is so permitted by the court; or

iii. the victim is a public figure and the action which makes him a victim is related to his public function.

4. Derogations from provisions that are related to the requirements for processing of data of minors, provisions of articles 6 of 21 of this law, and provisions of Part V of this law are not allowed.

Article 44
Data processing and access to information in the public sector

1. The right to personal data protection shall be exercised in harmony with the right to access official documents and right to information, as provided for in Law no. 45/2022, “On the ratification of the Council of Europe Convention on Access to Official Documents”, Law no. 119/2014, "On the Right to Information", as amended, and Law no. 33/2022, "On Open Data and Reuse of Public Sector Information".

2. Public access to public information, as determined in Law no. 119/2014, "On the Right to Information", as amended, and public access to information regarding the performing of official functions and duties, shall not be prevented by the right to personal data protection of natural persons, who are considered public authorities or exercise state functions, unless other fundamental rights, such as their right to life and right to physical and mental integrity require the protection of their data in a case of certain category of cases.

Article 45

Personal data processing for filing for public interest, historical or research, scientific or statistical purposes

1. The processing of personal data, including sensitive data and criminal records, for filing purposes in the public interest, historical or research, scientific or statistical purposes, constitute a legitimate interest of the controller, unless the data subject interest and fundamental rights and freedoms prevail, which require protection of their personal data protection. For this purpose, paragraph 43 of this article shall apply.

2. Personal data, including sensitive data and criminal records, collected for any purpose, can be further processed for filing purposes for public interest, for historical, research, scientific or statistical purposes, according to specific criteria defined in paragraph 3 of this article.

3. The processing pursuant to paragraph 1 of this article, as well as further processing pursuant to paragraph 2 of this article, shall be carried out where appropriate safeguards are implemented for the rights and freedoms of the data subject. Such protection measures include, but are not limited to, as per below:

a) technical and organizational measures taken by controller in compliance with this law and in particular respecting the principle of data minimization or pseudonymization in such a way as to fulfill the purpose of the processing. When the purposes under this article can be fulfilled keeping the information anonymized or at least pseudonymized, the purpose shall be fulfilled in this way;

b) pseudonymization of the data and, if the fulfilling of goal of further processing is not affected, their anonymization before the data transfer for further processing purposes;

c) specific protection measures, in order that the data collected for processing or further processing, according to paragraph 1 or 2 of this article, are not processed regarding the taking of measures or decisions towards the data subjects, unless the data subject has explicitly consented.

4. The exceptions from the exercise of one or more rights of the data subjects in relation to data processing operations for the purposes referred to in paragraph 1 and 2 this article, shall apply in those cases where their exercise may cause a serious damage or make impossible the fulfillment of a specific purposes and are necessary for their fulfilment. The burden of proof to prove the degree of the difficulty of the barriers, in achieving the purpose of the processing process that would be caused by exercising the rights of a data subject belongs to the controller.

Article 46

Data processing for the purpose of direct marketing

1. The personal data processing may be conducted within direct marketing, as a form of communication with directly identifiable persons, for the purpose of promoting goods or services, including advertising membership in organization, search of donations, and direct marketing activities, which include any preparatory action by the advertiser or a third party to enable this communication.

2. The processing for direct marketing purposes which is followed by the controller or third parties may be based in the legitimate interest, in the meaning of sub-paragraph "dh", of article 7 of this law, as far as interests for the protection of data subjects are not affected. This paragraph shall also apply for data taken from resources accessible by the public for direct marketing purposes.

3. The processing of sensitive data for direct marketing purposes shall be carried on express consent of the data subject.

4. When personal data are processed for direct marketing purposes, the data subject shall be entitled to object such processing at any time, in accordance with the special provisions of paragraph 2, of article 19 the this the law.

PART III
PROCESSING OF PERSONAL DATA BY COMPETENT AUTHORITIES FOR PUBLIC OR NATIONAL SECURITY AND FOR THE PREVENTION AND PROSECUTION OF CRIMINAL OFFENCES

CHAPTER I

Article 47
Scope of application

The provisions of this section shall apply to the processing of personal data referred to in paragraph 1, of article 3 of this law, by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, including the protection and prevention of threat to public security, defense and national security.

CHAPTER II
PERSONAL DATA PROCESSING

Article 48

Principle in relation to personal data protection

1. Processing of the personal data according to this part shall be conducted by competent authorities, in accordance with the principles set out in articles 6 and 51 of this law, regarding further processing for other purposes.
2. Each law on prevention, investigation, recovery or prosecution of acts criminal or execution of criminal sentences, including protection and prevention of threats to public safety, defense and national security, must provide for adequate time periods about the deletion of personal data or a periodicals review of the need to store personal data, including procedural measures which ensure compliance with time restrictions.

Article 49
Data distinction and quality

1. As far as possible, the controller shall make a clear distinction between personal data of different categories of the data subjects in criminal cases as follows:

a) a person, to whom a criminal offence is attributed, the person under investigation, arrested, detained person, defendant and a person for which, there are reasonable grounds and based on evidence, that he will commit a criminal offence;

b) a person convicted by a final criminal court decision of the Albanian courts or convicted by a court decision of foreign courts, a decision which has been recognized under the applicable legislation and the sentence has been converted by a final decision of the Albanian courts;

c) victims of a criminal offence, accusing victim, the civil plaintiff in a criminal proceeding, or a person for whom there is a reasonable doubt based on evidence, that he could be a victim of a criminal offence; and

ç) the referring party, the victim presenting the complaint, a person who might disclose useful circumstances for the purpose of investigation, a person who is suspected to receiving or transmitting communications from the suspect for committing the criminal offence or participates in transactions with him, the person whose observation may lead to the discovery of the whereabouts of the persons referred to in sub- paragraphs “a” and “b” of this paragraph,

the person indicted as a defendant in a related proceeding, the witness, related persons and collaborators of the persons referred to in sub-paragraph "a" and "b" of this paragraph.

2. Personal data based on facts, shall be distanced from the personal data based on personal evaluations. For personal data based on personal evaluations, a specific register shall be kept, where the reasons and circumstances having dictated such evaluation shall be recorded.

3. The competent authorities shall take the right technical and organizational measures to ensure that the incorrect or incomplete personal data, or data that are not updated or to be deleted, are not transferred or made available, in particular for automatic storage purposes by archiving systems. Before their transmission or disclosure, the competent authority shall verify, to the extent possible the quality of the data. The personal data held ready for automatic recovery shall be kept complete and updated at any time.

4. To the extent possible, together with each transmission of personal data, additional information shall be provided, that enable the receiver to evaluate the up-to-dateness, accuracy, completeness and reliability of the transmitted personal data.

5. If it turns out that personal data have been transmitted that do not comply with the requirements of paragraph 3 of this article, the competent authority for the transmission or the competent authority that keeps the archiving system shall notify the recipient without delays. The recipient shall immediately delete the data that have been transmitted unlawfully, correct the inaccurate data, complete the incomplete data or immediately restrict processing.

6. If the receiving competent authority has reason to believe that the transmitted personal data are inaccurate, not updated, or shall be deleted, or which processing should be restricted, it shall immediately notify the transmitting competent authority. The latter shall immediately take the necessary measures.

Article 50
Legitimate processing of personal data

The processing of the personal data as per this part shall be legitimate, only if and to the extend which:

a) it is foreseen by law; and

b) it is necessary and proportionate for fulfilling a task by the competent authority for the purposes under article 47 of this law.

Article 51
Processing for other purposes

1. Further processing of the personal data by the same competent authority, or another competent authority for purposes as per article 47 of this law, shall be allowed when the competent authority is authorized by the law to achieve the other purpose and for as much as it is necessary and proportionate with the new purpose.
2. The further processing for other purposes, except those determined in article 49 of this law, can the conducted only when this authorized expressly by the law. For the processing according to these purposes the provisions of Part II of this law shall apply.
3. The further processing for filing purposes for public interest, for research, historical, scientific or statistical purposes, shall be permitted subject to appropriate safeguards for the rights and freedoms of the data subjects, in compliance with paragraph 3 of article 45 of this law.

Article 52
Legitimate processing of sensitive data

1. Processing of sensitive data by competent authorities shall be allowed only where such processing is absolutely necessary, subject to appropriate safeguards for the rights and

freedoms of the data subject, and only if:

a) is specifically authorized by law, unless it is absolutely necessary to protect vital interest of the data subject or another person;

b) is related to data which are manifestly made public by the data subject or serve a purpose for which the controller is competent under the law.

2. Special restrictions provided by paragraph 2, of article 53 the this the law, must the held into consideration.

Article 53

Automated individual decision-making

1. Decision-making based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, shall be prohibited, unless superficially provided by law, which provides appropriate safeguards for the rights and freedoms of the data subject, and the right to obtain manual intervention on the part of the controller.

2. Decisions referred to in paragraph 1 of this Article shall not be based on sensitive data, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

3. Profiling that results in discrimination against persons due to sensitive data shall be prohibited.

CHAPTER III

RIGHTS OF THE DATA SUBJECT

Article 54

Communication and modalities for exercising the rights of the data subject

1. The controller shall take the right steps to provide any information and communication referred to articles 55 - 57 of this law, relating to processing to the data subject in a concise, intelligible and easily accessible form, using clear and plain language. The information shall be provided by any appropriate means, including by electronic means. As a general rule, the controller shall provide the information in the same form as the request.

2. The controller shall facilitate the exercise of the rights of the data subject under articles 55 - 57 of this law.

3. The controller shall provide inform to the data subject in writing about the follow up to his or her request without undue delay.

4. The information provided and any other communication made or action taken pursuant to articles 55 -57 and 67 of this law shall be made 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:

a) charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested; or

b) refuse to act on the request.

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

6. Where the controller has reasonable doubts concerning the identity of the natural person making a request referred to in article 57 or 58 of this law, may request the provision of

additional information necessary to confirm the identity of the data subject.

7. When restrictions about answers their requests, according to articles 57 and 58 of this law, are applied, the data subject may request the Commissioner to verify the legitimacy of all responses. The controller shall inform the data subject about this the right.

8. When the right provided for in paragraph 2 of this article is exercised, the Commissioner shall inform the data subject on the performance of all needed verifications and reviews by the Commissioner and his right to make a complaint to the competent administrative court.

9. In the cases referred to in articles 54, paragraph 1, 56, paragrah 3, and 57, paragrah 6, of this law, the rights of the data subject may also be exercised through the Commissioner.

10. The controller shall inform the data subject of the possibility of exercising his or her rights through the Commissioner, pursuant to paragraph 9 of this article.

11. When exercising the right referred to in paragrpah 9 of this article, the Commissioner shall inform the data subject at least that all necessary verifications or a review by the Commissioner have been carried out. The Commissioner shall also inform the data subject of his or her right to seek a legal remedy.

Article 55

The right to information

1. The controller shall make available to the data subject at least the following information:

a) the identity and contact data of the controller and where applicable the contact data of the data protection officer

b) the processing purposes for which the personal data are obtained;

c) the legal basis for processing;

ç) the existence of the rights for access, rectification, erasure and restriction of data processing and the right to lodge a complaint with the Commissioner, including contact details of the Commissioner;

2. In addition to the information provided for in paragraph 1 of this article, with the aim of enabling the exercise of his or her rights, the controller shall, in specific cases, provided the data subject with the additional information as following:

a) the storage time period of the personal data, or if possible, the criteria used for the determination of such time period;

b) as applicable, the categories of recipients the personal data, including those in foreign countries or international organizations;

c) other additional information, when necessary, and, in particularity, when personal data have been collected without the knowledge of the data subject. For the provision of information on the source of data collection, special attention shall be paid to the fundamental rights and legitimate interests of persons who have supplied such data.

3. In special cases, the disclosure of information about sensitive data, in compliance with paragraph 2 of this article, may be delayed, limited or rejected for as long as it is necessary or proportionate, considering the basic rights and legitimate interests of the data subject, in order to:

a) avoid obstacles or prejudice to the prevention, detection, investigation or prosecution of criminal offenses or execution of criminal sentences, in particularly preventing searches, investigations, procedures carried out by competent authorities or the judicial process;

b) protect public security, national security or protect the rights and freedoms of others.

Article 56

Right for access

1. The data subject shall be entitled to ask and 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 as per article 14 of this law. For providing information on the

data collection source, in case the personal data have not been obtained from the data subject a special attention shall be paid to the fundamental rights and legitimate interests of the persons who have supplied such data.

2. The restriction of the right to access wholly or partly, shall be allowed to the extent and as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, only when and to the amount its application would affect one of the purposes provided for in paragraph 3 of article 55 of this law.

3. The controller shall inform the data subject without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may be omitted where the provision thereof would undermine a purpose under paragraph 3 of article 55 of this law. In any response to a request for access the controller shall inform the data subject of the possibility of lodging a complaint with the Commissioner or competent authority for the review of the response.

4. The controller shall document the facts and legal reasons of the refusal of access as per paragraph 2 of this article and makes this information available to the Commissioner.

Article 57

Right to rectification or erasure of personal data and restriction of processing

1. The data subject shall be entitled towards the controller for the rectification of inaccurate personal data as soon as possible. Taking into account the purposes of the processing, the data subject shall be entitled to have his or her incomplete personal data completed, including by means of providing a supplementary statement.

2. The data subject shall be entitled that his or personal data are erased as soon as possible, in any case he is informed that his personal data are being unlawfully processed, in particular due to the violation of articles 6, or 49 – 52 of this law, or where personal data must be erased in order to comply with a legal obligation to which the controller is subject. The controller shall erase the data immediately as per the specifications of this paragraph.

3. The controller shall not erase but only restricts the data processing in cases where:

a) the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or

b) the personal data must be maintained for the purposes of evidence for performing of a tasks vested on the controller by law.

4. In case of a restriction pursuant to paragraph (a) of paragraph 3 of this article, the controller shall inform the data subject before lifting the restriction.

5. The controller shall inform the data subject in writing of any refusal of rectification or erasure of personal data or restriction of processing. The restriction, wholly or partly, of the rights foreseen in this article shall be allowed to the extent that and as long as such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned only in order to and to the amount that their application would affect one of the purposes provided in paragraph 3 of article 55 of this law. The controller shall inform the data subject of the possibility of lodging a complaint with the Commissioner for the review of the response of the controller.

6. The controller shall communicate the rectification of inaccurate personal data to the competent authority from which the inaccurate personal data originate.

7. Where personal data has been rectified or erased or processing has been restricted pursuant to this article, the controller shall notify all recipients of personal data who in turn shall rectify or erase the personal data or restrict processing of the personal data under their responsibility.

CHAPTER IV
OBLIGATIONS OF THE CONTROLLER AND PROCESSOR

Section 1
Liability

Article 58
Obligations of the controller

For the implementation of the provisions of this part, the controller shall apply paragraphs 1, 2 and 4, of article 22 and paragraph 1 and 2, of article 23 of this law.

Article 59
Joint controllers

Where two or more controllers jointly determine the purposes and means of processing, paragraph 1 and 3 of article 24 of this law shall apply, provided that references about the rights of data subjects and respective duties of the controller are in accordance with the rights and duties set out in this part the law.

Article 60
Processor

1. Where processing is carried out on the behalf of one controller, paragraphs 1–4, and paragraph 8 of article 26 of this law shall apply with reference to applicable provisions provided for under this Part.

2. The processor and any person that acts under authority of controller or the processors, that has access to the personal data, shall only process those data according to instructions of the controller, except where the law provides to act otherwise.

Article 61
Record keeping duty

Every controller and processor shall keep record documentation of processing activities in accordance with article 27 of this law, in accordance with the relevant circumstances, provided that references to the provisions of Part II of this law are in compliance with provisions of this part. Documentation kept by the controller contains also information about use of profiling, where applicable.

Article 62
Record-keeping

1. Processing operations, in particular consultations and disclosures, including transmissions, modifications, rectifications and erasures, shall be recorded adequately, by ensuring that lawfulness of processing can be monitored and verified. In automatic processing systems, recording includes any act of collection or combination. Recording data, in particular, in related with consultation and dissemination, enable the determination of the reason, date and time of these actions and, to the extent possible, the identification of the person who consulted or disclosed the personal data and identity of any recipient of such personal data.

2. The records are used only to verify the lawfulness of data processing, including self-

monitoring, to ensure the integrity and security of personal data processing, as well as for criminal prosecution or to ensure national security. The records shall be kept for as long as needed for the purpose they are collected for.

3. The controller and processor shall make available to the Commissioner the records upon the latter's request.

Article 63
Cooperation with the Commissioner

Upon request of the Commissioner, the controller and processor shall collaborate with it and provide any information necessary for the performance of these tasks, in accordance with the applicable legislation. In case they have received a recommendation or order from the Commissioner, the controller or processor must inform the Commissioner about compliance level immediately after deadline specified in it.

Article 64
Data protection impact assessment

Prior to commencing a new processing activity, the controller shall make a data protection impact assessment in accordance with paragraphs 1–5, 8 and 9 of article 31 of this law.

Article 65
Prior Consultation

1. In line with article 32 of this law, the controller shall consult with the Commissioner before processing the personal data that will be included in a new filing system to be created, when from the impact assessment it is concluded that the processing present a high risk about the fact that risk mitigating measures have not been undertaken or are not easily applicable, or the type of processing and, in particular, processing that uses new technologies, mechanisms or procedures, represent a high risk to the fundamental rights and freedoms of the data subjects. The controller shall make available to the Commissioner the impact assessment report, and as requested by the latter, information pursuant to paragraph 4 of article 32 of this law, and any other information that allows the supervisory authority to make an assessment of processing compliance, and in particular of the risks of data protection of the data subject and of the related protective measures. The controller may authorize the processor to conduct consultation with the Commissioner.

2.The Commissioner shall act according to paragraphs 2 and 3 of article 32 of this the law.

3.When processing operations of personal data for the purposes determined in article 49 of this law are regulated by law or sub-legal act, the opinion of the Commissioner shall be obtained on the risks that processing can present.

4. The Commissioner may the publish by a decision the processing operations as per article 47 of this law about which preliminary consultation is needed.

Section 2
Security of personal data

Article 66
Security of processing

1. Taking into account the technological developments, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk of occurrence and escalation of the risk to the rights and freedoms of persons, the controller and processor shall implement appropriate technical and organizational measures, to ensure an adequate level of security towards risk, in particular as regards the processing of sensitive data referred to in article 52 of this law.

2. In respect of automated processing, and where applicable, in relation to the non -automatic processing in the filing system, the controller and processor, following an evaluation of the risks, shall implement measures designed to:

a) access control to equipment, not to allow unauthorized persons to have access to equipment used for processing;

b) control of data media, to prevent the unauthorized reading, copying, modification or removal of data media;

c) storage control, to prevent unauthorized input of personal data and the unauthorized inspection, modification or deletion of stored personal data;

ç) user control, to prevent the use of automated processing systems by unauthorized persons using data communication equipment;

d) data access control, to ensure that persons authorized to use an automated processing system have access only to the personal data covered by their access authorization;

dh) communication control, to ensure that it is possible to verify and establish the authorities to where personal data have been or may be transmitted or made available using data communication equipment;

e) data input control, to ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input;

ë) transport control, to prevent the unauthorized reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media;

f) recovery, to ensure that installed systems may, in the case of interruption, be restored at working conditions;

g) reliability and integrity, to ensure that the functions of the system perform, that the appearance of faults in the functions is reported and that stored personal data cannot be corrupted by means of a malfunctioning of the system;

3. The controller shall record the technical and organizational measures adopted and implemented to ensure the protection of personal data, in accordance with the law and the implementing sub-legal acts.

4. The Commissioner, shall, by means of a guideline, define detailed rules for data security and shall regulate the procedures for the administration of data recording, data disposal, processing and disclosure.

Article 67
Notification of a personal data breach

1. The controller shall notify the Commissioner on the personal data breach, in line with article 29 of this law.

2. In cases where the personal data breach may represent a significant risk to the rights and

freedoms of persons, the controller shall immediately communicate the personal data breach to the data subject. This communication shall describe in a clear and plain language the nature of the personal data breach and include at least the information and measures referred to in sub-paragraph "b" to "ç" of paragraph 4 of article 29 of this law.

3. The communication with the data subject referred to in paragraph 2 of this article, is not needed if one of the following conditions is in place:

a) the controller has implemented adequate technical and organizational protection measures and such measures are implemented for personal data affected by the personal data breach, in particular those measures which make personal data unintelligible to any unauthorized person about to access those, including encryption;

b) the controller has taken additional measures, which ensure that the violation of the fundamental rights and freedoms of data subjects is no longer possible to happen; or

c) the controller publishes the notice or takes other similar measures, through which the data subjects are notified at an equal and effective way, on the personal data breach, when notifying any personal data subject would constitute an unreasonable effort for the controller.

4. If the controller fails to provide notification, the Commissioner shall require the controller to provide it when he/she assesses that the risk of infringement of fundamental rights and freedoms is high or decides on the fulfilment of one of the conditions set out in point 3 of this article.

5. Communication with the data subject, referred to in point 2 of this article, may be delayed, restricted or refused depending on the conditions and reasons, according to paragraph 3 of article 55 of this law.

Section 3
Special instruments that support compliance

Article 68
Data protection officer

Competent authorities, except for the courts when acting within their judicial activity shall appoint a data protection officer in line with articles 33 and 34 of this law.

Article 69
Confidential reporting mechanisms

Competent authorities shall establish effective mechanisms to promote confidential reporting of violation the provisions of this part.

CHAPTER V
INTERNATIONAL DATA TRANSFER

Article 70
General principles on international data transfer between competent authorities

1. In line with other provisions of this part, which regulate the lawful processing of personal data, the transfer by a competent authority of personal data which are undergoing processing or are intended for processing after transfer to a third country, or to an international organization including for onward transfers from this country or international organization to another country or another international organization, may take place, only if:

a) the recipient is another competent authority;

b) the transfer is necessary for one or more of the purposes set out in article 47 of this law; and

c) conditions foreseen in paragraphs 2-4 of this article, as well as in articles 71, 72 and 73 of this law are met.

2. All provisions if this chapter shall be applied in a way that does not affect the level of protection of the persons as per this part.

3. In all transfer cases as per paragraph 1 of this article any further transfer to a third country or international organization shall only by allowed based on a preliminary authorization by the competent authority that has made the initial transfer. Authorizations for onward transfers shall take into account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data were initially transferred and the level of protection of personal data in the country or other international organization to which the personal data are onward transferred.

4. Transfers under articles 72 or 73 of this Law shall be specifically documented and the documentation shall be made available to the Commissioner upon request, including the date and time of the transfer, information regarding the receiving competent authority, the justification for the transfer and the personal data transferred.

Article 71

International data transfer between competent authorities on the basis of an adequacy decision

1. International data transfer in line with sub-paragraphs “a” and “b” of paragraph 1 of article 70 of this law, may take place if the country, territory or one or more specified sectors within it, that or the international organization, where personal data are to be transferred, ensures an adequate level of data protection. Such a transfer shall not require any specific authorization.

2. The level of protection of a country, territory or specified sector, or of an international organization shall be determined by decision of the Commissioner, which shall be made public as per paragraph 1 of article 85 of this law.

3. While evaluating the adequacy of the protection level, the Commissioner shall take account in particular the following elements:

a) the rule of law, respect for fundamental human rights and freedoms, the relevant legislation, both general and sectoral, including public security, defense, 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 transfer of personal data to another third country or international organization, which are complied with in that country or international organization, 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 transferred;

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

c) the international commitments the third country or international organization 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.

4. The Commissioner shall monitor developments in those countries or international organizations which have been considered to have an adequate protection level, with regard to the protection of personal data and shall revise its decisions accordingly.

Article 72
International transfers in absence of an adequacy decision

1. International data transfers to a competent authority of a country or international organization in absence of an adequacy decision may take place where:

a) appropriate safeguards with regard to the protection of personal data are provided for in a law or binding sub-legal acts;

b) the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with regard to the protection of personal data.

2. The controller shall inform the Commissioner about categories of transfers under sub-paragraph "b" of paragraph 1 of this article. The Commissioner shall be provided additional data upon request.

Article 73
Derogations for specific situations

1. International data transfer to a competent authority of a country or international organization, which has an inadequate level of data protection or in absence of the adequate protection measures, as per sub-sub-paragraph "a" of paragraph 1 of article 72, shall only be permitted when the transfer is necessary:

a) in order to protect the vital interests of the data subject or another person;

b) to safeguard legitimate interests of the data subject, where this is provided by law;

c)for the prevention of an immediate and serious threat to the public security of the Republic of Albania, or of a third country;

ç) in individual cases for the purposes set out in article 49 of this law, and adequate protection measures, are not possible to be applied at the right time; or

d) at an individual case for the submission of a request or exercise or defense of a legal claim relating obligation or interest, before the court or public authorities, relating to the purposes set out in article 49 of this law.

2. Personal data shall not be transferred if the transferring competent authority determines that fundamental rights and freedoms of the data subject concerned override the public interest in relation to the transfer set out in sub-paragraphs "ç" and "d" of paragraph 1.

Article 74
International data transfers to recipients who are not competent authorities

1. Except for the cases provided for in sub-paragraph "a" of paragraph 1 of article 74 of this law and without prejudice to any international agreement in force between the Republic of Albania and other countries in the area of judicial cooperation for criminal matters and police cooperation the competent authorities which are the public authorities in individual and specific cases, may transfer personal data directly to foreign recipients, who are not the competent authorities, if acted in compliance with this part and all of the following conditions are fulfilled:

a) the transfer is necessary for the performance of a task, vested by law to the competent authority for the transfer, within the purposes defined in article 47 of this law;

b) the transferring competent authority shall determine that no fundamental rights and freedoms of the data subject override the public interest necessitating the transfer in the case at hand;

c) the transferring competent authority considers that the transfer to a competent authority of another country as per paragraph 1 of article 48 of this law, is ineffective or inappropriate,

in particular because the transfer cannot be achieved in good time;

ç) the authority that is competent in the other country, for the purposes referred to in Article 47 of this law, shall be immediately informed, unless the immediate notification is ineffective or inappropriate; and

d) the transferring competent authority, informs the recipient of the specified purpose or purposes for which the personal data are only to be processed by the latter provided that such processing is necessary, and in particular that any further transfer shall be subject to prior authorization by the transferring competent authority.

2. The transferring competent authority shall inform the Commissioner of transfers pursuant to paragraph 1 of this article. Such transfers shall be documented in a specific manner and the documentation shall be made available to the Commissioner upon request, including the date and time of the transfer, information concerning the receiving competent authority, the justification for the transfer and the personal data transferred.

PART IV
COMMISSIONER FOR THE RIGHT TO INFORMATION AND PERSONAL DATA PROTECTION

Section 1
Independent status

Article 75
The Commissioner

1. The Commissioner for the Right to Information and Personal Data Protection is a public legal person and an independent supervisory authority responsible for monitoring and supervising the implementation of this law, with the aim of protecting the fundamental rights and freedoms of natural persons with regard to the processing of personal data.

2. The salary of the Commissioner consists of:

a) the amount for the job position determined by the ratio with the salary of the President of the Republic according to the legislation in force on salaries, remunerations and structures of independent constitutional institutions and other independent institutions established by law;

b) allowance for working conditions (special nature of work) at the rate of 55% of the salary amount for the job position

Article 76
Independence and incompatibility of functions

1. The Commissioner shall operate in complete independence in performing its tasks and exercising its powers in accordance with this law and shall not be influenced either directly or indirectly and shall not seek or receive any guidance.
2. During his term of office, the Commissioner shall not engage in any incompatible activity with his role, and shall not exercise any incompatible occupation, whether gainful or not.
3. The Commissioner has his own budget, which is part of the state budget approved by the Assembly and manages it independently. He proposes the budget in accordance with the legislation in force. The Commissioner is subject to financial control, insofar as it does not affect his independence.
4. The Commissioner enjoys the same protocol treatment as the chairman of the standing committee in the Assembly.

Article 77
Office of the Commissioner, human and financial resources

1. The Commissioner shall be assisted by the Office of the Commissioner, which is provided with the human, technical, financial resources, as well as facilities and infrastructure necessary for the effective performance of his duties and the exercise of his powers.
2. The staff is subject to the exclusive direction of the Commissioner and reports regularly to him. The Commissioner, in order to achieve the mission and objectives of the institution, in order to receive appropriate advice on specific issues, has the right to have external advisors. Their remuneration is determined by the Commissioner with reference to the legislation in force.
3. The Commissioner approves the structure and organigram of the Office of the Commissioner. Employees of the Office of the Commissioner benefit from an allowance for working conditions (special work nature), which is determined by decision of the Council of Ministers.
4. Confidential information of which the Commissioner and his staff become aware due to the exercise of their duties and powers and, in particular, information obtained from the submission of complaints by natural persons for violations of this law, constitutes a professional secret. The Commissioner and the staff of his Office are exempt from the obligation to maintain professional secrecy when the information is related to a criminal offense, according to the Criminal Code of the Republic of Albania, and the Commissioner refers it to the competent criminal prosecution authority.
5. The employment relations of the employees of the Commissioner's Office are regulated by the law on civil servants. The employment relations of administrative employees and cabinet functionaries are regulated by the Labor Code.

Section 2
Appointment and end of term of office

Article 78
Appointment and end of term of office

1. The Commissioner shall be appointed by a majority of all members of the Assembly, upon the proposal of the Council of Ministers, for a 7-year term, with the right to re-election.
2. The procedure for appointing a candidate shall begin with the publication of a call for expressions of interest to be selected as a Commissioner 90 (ninety) days before the end of the term or no later than 7 (seven) days in the event of dismissal or resignation.
3. Before taking office, the Commissioner shall take an oath before the Assembly with the following oath: *"I swear that during the performance of my duties I will always protect the constitutional rights to information and personal data protection, as fundamental human rights and freedoms."*

Article 79
Selection criteria

The candidate for Commissioner must meet the following criteria:

a) be an Albanian citizen;

b) have completed integrated studies in law or a second-cycle university study program in law, equivalent to them, or have completed university studies in law abroad, and have obtained an equivalent diploma, unified according to the rules on unification of diplomas provided for by the legislation in force;

c) have no less than 15 (fifteen) years of active full-time professional experience after completing studies in law according to sub-paragraph “b” of this article;

ç) have knowledge, as well as have carried out prominent activities in the field of human rights, other areas of law and, in particular, in the field of personal data protection and the right to information;

d) have not been convicted by a final decision for committing a criminal offense during the last 10 (ten) years;

dh) not have held the role of member of the Council of Ministers or Member of Parliament during the last 4 (four) years.

Article 80

End of term of office

1. The Commissioner ‘s term of office shall end when:

a) the 7-year term of office expires;

b) he resigns;

c) he is dismissed.

2. The Commissioner shall be dismissed only upon a motivated request from the Council of Ministers, which is supported by no less than one third of all members of the Assembly. The Assembly shall decide on the dismissal of the Commissioner by three-fifths of all its members, due to:

a) serious violations, which seriously damage the public reputation or the functioning of the Office; or

b) his inability to further fulfill the function of the Commissioner.

3. In the event of dismissal or resignation, the Council of Ministers shall propose to the Assembly a new candidacy, within 1 (one) month. When the term of office ends according to sub-paragraph “a” and “b”, of paragraph 1 of this article, the Commissioner shall remain in office until the election of a new Commissioner.

4. At the end of the mandate, the Commissioner, who before the appointment was working full-time in the public sector, shall return to his previous role or, if impossible, to an equivalent one.

Section 3

Powers and Duties

Article 81

Powers in the Field of Personal Data Protection

The Commissioner is responsible for performing the tasks assigned to him and exercising the powers granted to him in the field of data protection in accordance with this law.

Article 82

Tasks and relevant powers for their achievement

1. Without prejudice to other tasks set out under this Law, the Commissioner shall be responsible for:

a) monitoring and supervising the implementation of this law and sub-legal acts issued for its implementation, and preparing an annual report for this issue;

b) promoting the awareness of the public, controllers and processors, and the understanding of the risks, rules, safeguards and rights in relation to personal data processing also through

publications and training programs/modules with special attention to activities that focus on minors and data protection officers;

c) provide opinions to the Assembly, Council of Ministers and other central institutions on legislative and administrative measures relating to the protection of fundamental rights and freedoms of natural persons with regard to personal data processing;

ç) monitoring relevant developments to the extent that they have an impact on personal data protection, as well as providing recommendations for the implementation of the requirements of the personal data protection law and their publication;

d) the adoption and publication of guidelines on processing of personal data, which include, among others, the legal duration of the storage of personal data or security measures in education, health, video surveillance system, and direct marketing sectors, as well as for the competent authorities as defined in this law;

dh) the approval and publication of various guidelines on obligations arising from this law;

e) the authorization pursuant to paragraph 3 of article 41 of this law, the adoption and publication of standard contractual clauses for contracts between controllers and processors pursuant to paragraph 7 of article 26 of this law, and binding company rules pursuant to article 42 of this law;

ë) advising controllers within prior consultation pursuant to article 32 of this Law, and authorizing the processing pursuant to paragraph 5 of article 32 of this law, as well as the publication of lists in relation to the criteria for data protection impact assessment pursuant to paragraph 7 of article 31 and paragraph 4 of article 65 of this law;

f) promoting the development of codes of conduct pursuant to Article 35 of this Law, and publishing the criteria for the accreditation of a body for monitoring codes of conduct pursuant to Article 36 of this Law, the adoption of codes of conduct and the accreditation of a monitoring body, when and for as long as the requirements are met;

g) promoting the implementation of certification, data protection seals and marks, with the aim of facilitating compliance with this law, drafting and publishing criteria for certification, in accordance with Article 37 of this law, and for the accreditation of certification bodies in accordance with Article 38 of this law, as well as the accreditation of certification bodies, including the approval of their certification mechanisms, when and for as long as the requirements are met;

gj) supervising, regulating and authorizing the international transfer of personal data in accordance with Chapter IV, Part II and Chapter V, Part III of this Law, including, in particular, adequacy decisions and standard data protection clauses;

h) conducting investigations into the compliance of personal data processing operations with this Law, either on its own initiative or on the basis of a complaint;

i) guaranteeing the exercise of the rights of data subjects, as provided for in Chapter II, Part II and in Chapter III, Part III of this law, including informing and advising data subjects in this regard;

j) handle complaints lodged to the Commissioner by natural persons or entities, organizations or NGOs, representing the natural person, in accordance with article 89 of this law, in case of violation of this law;

k) reviewing the responses given by the competent authorities to the requests of data subjects regarding the exercise of their rights of access or rectification or erasure, pursuant to article 90 of this law;

l) imposing administrative sanctions and other penalties, pursuant to chapter II, part V of this law, and supervising their implementation;

ll) take appropriate steps in relation to foreign states and international organizations to:

i. develop international cooperation mechanisms to facilitate the effective execution of legislation on the protection of personal data;
ii. provide international mutual assistance in the enforcement of legislation on the

protection of personal data, including through notification, complaint referral, assistance in investigations and exchange of information, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

iii. engage relevant stakeholders in discussions and activities aimed at further international cooperation in the implementation of personal data protection legislation;

iv. promote the exchange and documentation of personal data protection legislation and practice, including jurisdictional conflicts with foreign countries.

m) representing the Office of the Commissioner in activities carried out at national and international level;

n) maintaining an internal register of violations of this law and of measures taken under paragraph 2, article 83 of this law.

2. The Commissioner shall draft an annual report, which he shall send to the Assembly and report before it whenever requested, as well as requesting it to be heard on issues he considers important.

Article 83
Subsidiary powers

1. In order to fulfil his duties, according to article 82 of this law, the Commissioner shall have the following investigative powers:

a) notifies the controllers or processors of alleged violations of this Law and request their position regarding these allegations;

b) orders the controllers and processors to provide any information requested by the Commissioner for the performance of his duties, including access to documentation;

c) has access to any premises of the controller and processor, including data processing equipment and tools;

ç) conducts administrative investigations in the form of data protection audits;

d) reviews certifications issued by certification bodies, in accordance with articles 37 and 38 of this law;

dh) reviews the lawfulness of processing within the framework of restrictions on the data subjects' rights, according to chapter III, part III of this law.

2. In order to fulfil the tasks under article 82 of this law, the Commissioner shall have the following remedial powers:

a) warns the controllers or processors that intended processing operations may result in a breach of the provisions of this law and give them recommendations regarding compliance with the law;

b) gives notice to controllers or processors where processing operations have breached the provisions of this law;

c) orders controllers or processors to comply with the data subject's requests for the exercise of his or her rights in accordance with this law;

ç) orders controllers or processors to carry out processing operations in accordance with the provisions of this law and, where possible, in a specific manner and within a specified time limit;

d) orders controllers to communicate the personal data breach to data subjects;

dh) imposes a temporary or permanent restriction of processing, including the processing bans;

e) orders the rectification, erasure or erasure of personal data, as well as the restriction of processing, in accordance with articles 15, 16 and 17 of this law, and the notification of recipients on such actions, as provided for in articles 15 and 17 of this law;

ë) revokes the certification or orders the certification body to revoke a certification issued in

accordance with articles 37 and 38 of this law, or orders the certification body not to issue certifications if the criteria for certification have not been met or are no longer met;

f) orders the suspension of the data transfer to a recipient in a third country or to an international organization;

g) imposes administrative sanctions in accordance with articles 93 and 94 of this law, which may be added to or replace the measures referred to in letters "a"-"i" of this point, depending on the circumstances of each individual case.

3. When a violation may constitute a criminal offense, according to the Criminal Code of the Republic of Albania, the Commissioner shall act according to paragraph 4, of article 77 of this law.

Article 84
Duty to cooperate

Public institutions and private entities shall cooperate with the Commissioner, providing him with all the information he requires to fulfill his duties, and notifying him of the implementation of the recommendations given immediately after the deadlines provided for their implementation have expired.

Article 85
Publication

1. The instructions, decisions and other sub-legal acts of the Commissioner, of a general nature, shall be published in the Official Gazette.

2. The annual report and special reports shall be published on the official website of the Commissioner.

3. Decisions, authorizations, recommendations or other administrative acts, relating to individual cases, shall be published after pseudonymization on the official website of the Commissioner.

PART V
LEGAL REMEDIES, LIABILITY AND PENALTIES

CHAPTER I

REMEDIES AND LIABILITY

Article 86
The right to lodge a complaint

1. Without prejudice to other legal administrative or judicial remedies available, every data subject who claims that the processing of his personal data is taking place in violation of this law, shall be entitled to lodge a complaint with the Commissioner, who shall review it in line with the provisions of the Administrative Procedures Code, and this law.

2. After being informed by the Commissioner of the complaint lodged, the controller or processor, when requested by the Commissioner, shall not make substantial changes to the processing of the personal data in question without the Commissioner's approval, until the review of the complaint is completed.

3. The Commissioner shall inform the complainant of the progress of the review of the complaint, the decision taken, as well as the right to appeal to a court, including the court where the complaint may be filed, the means of appeal, the deadline and the method of calculating it for filing the complaint.

4. The Commissioner shall facilitate the submission of complaints through their submission forms, which may also be completed electronically, without excluding other means of communication.

5. The performance of the Commissioner's duties under this Article shall be carried out without compensation.

6. Where complaints are manifestly unfounded or excessive, in particular because of their repetitive character, the Commissioner may refuse to take action in relation to the complaint. The Commissioner shall bear the burden of proof regarding the unfoundedness and excessive nature of the complaint.

Article 87

Appeal against the decision of the Commissioner

1. Without prejudice to other administrative or extra -judicial settlement remedies, each natural or legal person, who claims that a legal claim or interest has been breached, as a result of an action or omission, administrative or sub-legal normative act issued by the Commissioner, shall have the right to lodge an appeal before the competent administrative court, as per the applicable legislation on adjudication of administrative disputes.

2. Without prejudice to other administrative or extra -judicial settlement remedies, any data subject that lodges a complaint pursuant to article 86 of this law, or a request pursuant to article 90 of this law, shall be entitled to lodge a lawsuit to the competent administrative court where the Commissioner does not review his complaint or request or does not inform the data subject within 90 (ninety) days about the progress of reviewing the complaint or request.

Article 88

Right to compensation and liability

1. Without prejudice to any available administrative or extra- judicial remedy, including the right to lodge a complaint with the Commissioner, aby data subject is entitled to an effective legal remedy, when he or she considers that his or her rights under this law have been violated as a result of the processing of his or her personal data in violation of this law. Whomever has suffered a financial or non-financial damage as a result of an infringement of this law shall have the right to receive compensation from the controller, processor or any competent authority for the damage suffered as per the Civil Code.

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 he proves that it is not responsible for the action 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 of this article and applicable legislation.

Article 89

Representation of data subjects

The data subject has the right to authorize an entity, organization or non-profit association, established under the law, which, according to its statute, has as part of its scope activity of public interest and is active in the field of protection of the rights and freedoms of data subjects with regard to the protection of their personal data, to lodge a complaint on his behalf, as well as to exercise the rights referred to in articles 86–88, 90 and 91 of this law on his behalf.

Article 90

Right to review the response of a competent authority

1. The recipient of a response from a competent authority following a request by him for the exercise of the rights under articles 55–57 of this law may request the Commissioner to review the lawfulness of the response and, if possible, the lawfulness of the processing operations underlying the response.

2. The Commissioner shall examine the request of the recipient, following the procedure provided for in article 86 of this law and shall ultimately reply to the recipient in accordance with paragraph 3 of article 55 of this Law.

Article 91

Request for a preliminary restriction order

During the appeal procedure, pursuant to article 86 of this Law, the complainant may ask the Commissioner, in accordance with article 17 of this law, to issue a preliminary restriction order in relation to specific processing operations by the other party, due to the serious and irreparable risk that threatens the rights of the complainant under this law. The Commissioner shall take a decision as soon as possible, but, in any case, no later than 14 (fourteen) days from the date of submission of the request, if the immediate blocking is necessary and proportionate. The order may be revoked at any time by the Commissioner based on the findings of the administrative investigation, otherwise it shall be binding on the other party until the conclusion of the examination of the case.

CHAPTER II

PENALTIES

Article 92

Administrative penalties

Violations of this law by controllers or processors of personal data shall be punishable by administrative penalties in accordance with the following articles of this chapter.

Article 93

General conditions for imposing administrative penalties

1. The Commissioner shall impose administrative penalties in accordance with this article for violations of this law, pursuant to paragraphs 1, 2 and 3 of article 94 of this law, as well as

in accordance with the legislation in force on administrative offences, in such a way that they are effective, proportionate and deterring.

2. Depending on the circumstances of each individual case, administrative penalties are accompanied by or replaced by corrective measures, pursuant to sub-paragraphs "a"–"f", of paragraph 2, of article 83 of this law. In deciding whether or not to impose an administrative penalty, as well as its amount in each case, the following shall be taken into account:

a) the nature, seriousness and duration of the breach, taking into account the nature, object or purpose of the processing in question, as well as the number of data subjects involved and the level of damage caused to them;

b) whether the breach was committed intentionally or negligently;

c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

ç) the level of responsibility of the controller or processor, taking into account the technical and organizational measures implemented by them, in accordance with Articles 23 and 28 of this law;

d) any previous similar breaches committed by the controller or processor;

dh) the level of cooperation with the Commissioner in rectifying the breach and mitigating its possible adverse effects;

e) the categories of personal data affected by the infringement;

ë) the manner in which the Commissioner was made aware of the breach, in particular whether the controller or processor notified the breach, and, if so, to what extent they did so;

f) the application of corrective measures, where such measures were taken against the controller or processor in relation to the same matter prior to the breach;

g) compliance with the codes of conduct adopted in accordance with article 35 of this law, or the certification mechanisms adopted in accordance with article 38 of this law; and

gj) any other aggravating or mitigating circumstances, relevant to the circumstances of the case, such as financial benefits or losses avoided, directly or indirectly from the breach.

3. Where a controller or processor, intentionally or through negligence, infringes several provisions of this law in respect of the same processing operations or operations connected thereto, the total amount of the administrative penalty shall not exceed the amount provided for the most serious breach.

Article 94

Amount of penalty

1. Based also on the circumstances specified in paragraph 2 of article 93 of this law, the following violations of the obligations, shall constitute administrative contraventions and are punishable by a fine of up to 1 000 000 000 (one billion) Albanian Lek, or in the case of a commercial company up to 2% of the total annual global turnover for the previous financial year, whichever is higher:

a) of the controller and processor, according to articles 8, paragraph 6, and 11, of chapter III, of part II of this law, with the exception of article 22 of this law;

b) the certification body in accordance with articles 37 and 38 of this law;

c) the monitoring body, according to paragraph 3, of article 36 of this law.

2. Based also on the circumstances specified in paragraph 2 of article 93, the following violations constitute administrative contraventions and are punishable by a fine of up to 2 000 000 000 (two billion) Albanian Lek, or in the case of a commercial company, up to 4% of the total annual global turnover for the preceding financial year, whichever is higher:

a) failure to apply the basic principles of processing, including the conditions for granting consent, according to articles 6, 7, 8 and 9, of this law;

b) violations of the rights of data subjects according to Articles 12–20 of this Law;

c) transfers of personal data to a recipient in a third country or an international organization, in violation of articles 39–42 of this Law;

ç) violation of obligations, according to articles 43–46 of this law.

3. Violation of the obligation to cooperate or of any act of the Commissioner, according to paragraph 1 of article 83 of this law, non-compliance with an order or temporary or final restriction of processing or suspension of data exchange, issued by the Commissioner, according to sub-paragraph "b" of paragraph 2, of article 83 of this law, also based on the circumstances specified in point 2 of article 93 of this law, constitutes an administrative contravention and is punishable by a fine of up to 2 000 000 000 (two billion) Albanian Lek, or in the case of a commercial company, up to 4% of the total annual global turnover for the previous financial year, whichever is higher.

4. Without prejudice to his subsidiary powers in article 83, paragraph 2, the Commissioner shall lay down by means of a guideline the rules on whether and to what extent the administrative penalties provided for in paragraphs 1, 2 and 3 of this article may be imposed. This guideline shall be based on the guidelines adopted by the European Data Protection Board.

Article 95

Appeal against the decision on the fine and its execution

1. Against the decision to impose a fine, the controller or processor has the right to file an appeal with the competent court in accordance with the applicable legislation.

2. The execution of fines in application of this law shall be carried out in accordance with the applicable legislation on administrative offenses.

3. Fines shall be collected in the state budget.

PART VI
FINAL AND TRANSITORY PROVISIONS

Article 96
Transitory Provisions

1. Requests, complaints and contraventions, which on the date of entry into force of this law are in the process of being reviewed by the Commissioner or by the court, shall be treated according to the provisions of the law in force at the time of their submission and at the time of the commission of the violation.

2. The term of the Commissioner in office shall end in accordance with the provisions of paragraph 1 of article 80 of this law.

3. Each public authority, within a period of 3 years from the date of adoption of this law, shall assess the compliance of existing laws, regulations and by-laws with this law.

4. Where there are inconsistencies or gaps compared to this law, in particular articles 7, paragraph 2 and 3, 20, paragraph 2, sub-paragraph "b", 21, paragraph 2, and 48, paragraph 2, of this law, identified during the assessment, the relevant public authority must immediately amend or propose amendments to the relevant legislation and sub-legal acts to bring them into line with this law.

Article 97

Sub-legal acts

1. The Council of Ministers shall be responsible to issue, within 3 months from the entry into force of this law, the sub-legal acts pursuant to paragraph 3 of article 77 of this law.

2. The Commissioner for the Right to Information and Personal Data Protection shall be responsible to adopt, within 3 months from the entry into force of this law, the sub-legal acts pursuant to Articles 31, paragraph 7; 36, paragraph 2; 37, paragraph 1; 38, paragraph 1; 40, paragraph 2; 43, paragraph 2; 65, paragraph 4; 66, paragraph 4; 82, paragraph 1, sub- paragraph "d", and 94, paragraph 4, of this law.

Article 98

References to applicable legislation

Upon the entry into force of this law, any reference that legal and sub-legal provisions make to Law No. 9887, dated 10.3.2008, "On Personal Data Protection", as amended, or its specific provisions, shall be deemed to be made to this law, to the extent possible.

Article 99

Repeals

1. Law No. 9887, dated 10.3.2008, "On Personal Data Protection", as amended, shall be repealed upon the entry into force of this law.

2. The sub-legal acts issued for the implementation of Law No. 9887, dated 10.3.2008, "On Personal Data Protection", as amended, shall remain in force until the adoption of new by-laws, as long as they do not contradict the provisions of this law.

3. Decisions and authorizations issued before the date of entry into force of this law remain in force as long as they do not contradict the provisions of this law.

4. International agreements, which include the transfer of personal data to third countries or international organizations, concluded before the entry into force of this law and which are in accordance with Law No. 9887, dated 10.3.2008, "On Personal Data Protection", as amended, shall remain in force until their amendment, replacement or denunciation.

Article 100

Repeals on the date of accession of the Republic of Albania to the European Union

1. On the date of accession of the Republic of Albania to the European Union, all provisions of this law shall be repealed, with the exception of the provisions of part III and part IV of this Law.

2. The provisions of this law referred to in the provisions of part III shall remain in force and shall apply only to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding and prevention of threats to public security, defense and national security.

Article 101

Entry into force

1. This law shall enter into force 15 days after its publication in the Official Gazette.
2. Exceptionally, articles 29, paragraphs 3, 31, 32, 35, 36, 64, 65 and 67, paragraphs 2, 3 and 5, of this law shall enter into force 2 (two) years after its publication in the Official Gazette.

Approved on 19.12.2024.

Promulgated by decree no. 5, dated 15.1.2025, of the President of the Republic of Albania, Bajram Begaj