

Law on Personal Data Protection

The Law was published in the "Official Gazette of Montenegro, No. 79/2008 and 70/2009 and 44/12 and 22/17.

I. GENERAL PROVISIONS

Article 1

Personal data protection shall be ensured under the conditions and in the manner stipulated by this Law, in compliance with principles and standards involved in established international agreements on human rights and basic freedoms and generally accepted regulations of the international law.

Article 2

The data about a person (hereinafter: personal data) shall be processed in a just and legal manner.

Personal data collected for statistical or scientific purposes in accordance with law may be processed provided that appropriate protection measures are undertaken.

Where personal data is made available for processing for statistical or scientific-research purposes, the data shall be provided for use in the form which does not disclose the person's identity.

Where the personal data controller enables the processing of personal data for statistical or scientific-research purposes, the data shall be provided for use in the form which would not disclose the data subject's identity.

Article 3

Personal data undergoing processing shall be accurate and complete and kept up to date.

Where the terms for processed personal data storage are not prescribed by law, personal data enabling the establishment of data subject's identity may be stored only for the period necessary to fulfil the purpose for which the personal data is being processed.

Article 4

Personal data protection shall be ensured for every data subject regardless of their nationality, place of residence, race, skin colour, sex, language, religion, political and other conviction, ethnic or social background, property, education, social standing or other characteristic.

Article 4a

The purpose and the method of personal data processing shall be laid down by the personal data controller, unless they are prescribed by law.

Personal data controller may be a state body, state administration body, local self-government or local government body, company or other legal person, sole trader or natural person, conducting personal data processing in accordance with this Law.

When conducting personal data processing themselves, or when the data is processed on their behalf, personal data controller shall ensure that the processing is carried out in accordance with Art. 2 and 3 of this Law.

Article 5

This Law shall apply to personal data controllers processing personal data in the territory of Montenegro or outside Montenegro where Montenegrin regulations are applicable in accordance with international law.

This Law shall also apply to a personal data controller which was established outside Montenegro or which does not have residence in Montenegro, if the equipment for personal data processing is located in Montenegro, unless the equipment is used only for personal data transit through the territory of Montenegro.

The personal data controller shall, in a case under Paragraph 2 of this Article, designate a representative or agent with the seat or place of residence in Montenegro, responsible for the application of this Law.

Article 6

Where the purpose of personal data and the manner of its processing are prescribed by law, the personal data controller shall be governed by that law.

Article 7

This law shall apply to the processing of personal data conducted wholly or partly by automatic means or otherwise and is an integral part of a personal data filing system or is intended to form a part of a personal data filing system.

Article 8

This Law, except for the provisions on surveillance, shall not apply to the processing of personal data concerning defence and national security, unless otherwise stipulated by a special law.

This law shall not apply to a natural person conducting the processing of personal data for their own needs.

Paragraph 3 is deleted.

Article 9

Certain terms used in this Law shall have the following meanings:

1) **personal data** means any information relating to an identified or identifiable natural person;

2) **personal data processing** means any operation which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, as well as any other operation performed on personal data;

3) **personal data filing system** means any structured set of personal data which is subject to processing and which may be accessible according to specific criteria, whether centralised, decentralised or classified on a functional or geographical basis;

4) **third party, i.e. personal data user** means any natural or legal person, state body, state administration body, local self-government or local government body and other entities exercising public authorizations, who are entitled to process personal data, but not the person whose personal data is processed, the original personal data controller, personal data processor or a person employed with the personal data controller or the personal data processor;

5) **personal data processor** means a state body state administration body, a local government body, company or other legal person, sole trader or natural person which processes personal data on behalf of the controller;

6) **consent** means a statement given freely in writing or orally by the personal data subject after being informed of the purpose of the processing, whereby the data subject agrees to the processing of their personal data for a specific purpose;

7) **special categories of personal data** means personal data relating to racial or ethnic origin, political opinion, religious or other belief, membership in trade union organizations, as well as data relating to health condition or sexual life;

8) **biometric data** means the data on physical or physiological characteristics owned by any natural person which is specific, unique and constant and according to which it is possible to identify the data subject's identity directly or indirectly;

9) **data subject** means a natural person who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.

II. PROCESSING OF PERSONAL DATA

1. Requirements

Article 10

Processing of personal data may be conducted upon previously obtained consent of the data subject, which may be revoked at any moment.

Processing of personal data shall be conducted without the consent of the data subject provided it is necessary for:

- 1) exercising legally prescribed obligations of the personal data controller;
- 2) the purpose of protecting the life and other vital interests of the data subject which is unable to give their consent personally;
- 3) enforcement of a contract if the data subject is a party to the contract or undertaking the activities upon a request from the data subject prior to conclusion of a contract;
- 4) conducting the affairs of public interest or exercising public authority which is within the competence of or vested in the personal data controller or third party, i.e. personal data user;
- 5) fulfilment of a legal interest of the controller or third party, i.e. personal data user, unless such interests should be restricted for the purpose of achieving and protecting the rights and freedoms of data subjects.

The consent referred to in Paragraph 1 of this Article, for the data subject deprived of business capacity, shall be given by a guardian, and the consent for an underage person shall be given by their parents or foster parents or the guardian, unless the interests of an underage person would be violated by the consent.

The consent for personal data processing for a dead person shall be given by their successors, determined in accordance with the law which stipulates the succession right, provided the dead person did not forbid the processing of personal data.

Article 11

Deleted.

Article 12

Personal data relating to an underage person shall be processed in accordance with the law, in a manner which is in the best interest of an underage person.

Article 13

Special categories of personal data may be processed only:

- 1) with explicit consent of the data subject;
- 2) where the processing of personal data is necessary for employment purposes in accordance with the law regulating labour relations, whereby appropriate protection measures must be stipulated;
- 3) where the processing of personal data is necessary for the detection, prevention and diagnosis of illnesses and treatment of data subjects, as well as for the management of medical services, if the data is processed by a health worker or another person that has to keep the data confidential;

4) where it is necessary for the purpose of protecting the life or other vital interests of the data subject to whom the personal data relates or another person, and they are not able to give consent personally, as well as in other cases prescribed by law;

5) if the data subject manifestly made the personal data available to the public or if the processing is necessary for the exercise or protection of legal interests of the data subject before a court or other authorities;

6) where processing of personal data is carried out within the legal activity of a non-governmental organization, i.e. association or other non-profit organization with political, philosophical, religious or trade union aims, if the data relates only to members of the organization or to persons who have regular contacts with the organization with regard to the organization's activity and if the data is not disclosed without the consent of the data subjects.

Special categories of personal data is specifically designated and protected for the purpose of preventing unauthorized access to this data.

The manner of designating and protecting the personal data referred to in Paragraph 2 of this Article shall be stipulated by the Ministry competent for public administration affairs.

Article 14

The processing of personal data that refers to criminal acts, pronounced criminal and misdemeanour penalties or security measures may be conducted only by or under the supervision of the competent state body and if the measures for personal data protection are provided in accordance with the law.

Article 15

Prior to the processing of personal data for the needs of direct marketing, the data subject shall be provided with the opportunity to object the data processing.

If the data referred to in Article 13 of this Law are used for the needs of direct marketing, it is necessary to obtain the consent from the data subject.

Article 15a

When deciding on the rights, obligations and interests of data subjects, assessment of their personal characteristics and capacities (work performance, reliability, credit rating, behaviour and similar), which are of importance for deciding, may not be based solely on automatic processing of data.

Exceptionally from paragraph 1 of this Article, deciding may be based only on automatic processing of data as follows:

- 1) if during conclusion or implementation of a contract a request of the data subject whose data is being processed was approved or there are appropriate measures to protect their legal interests (opportunity for the data subject to state their opinion and similar);
- 2) if it is stipulated by law, provided that measures for the protection of the data subject's legal interests are prescribed.

2. Assigning personal data processing tasks

Article 16

The personal data controller may entrust certain tasks regarding the processing of personal data within their competences to the personal data processor on the basis of a contract in a written form.

The contract referred to in Paragraph 1 of this Article shall regulate mutual rights and obligations of the personal data controller and personal data processor, and in particular obligation of the processor to act according to the instructions of the personal data controller.

The tasks referred to in Paragraph 1 of this Article may be entrusted only to the personal data processor which fulfils the requirements for implementing technical, personnel and organizational measures for personal data protection, in accordance with this Law.

The personal data processor shall destroy the personal data after processing or return it to the personal data controller.

3. Providing personal data for use to other personal data controllers

Article 17

If the requirements referred to in Articles 10 and 13 of this Law are met, the personal data controller shall provide the third party, i.e. the personal data user, at their request, with the personal data they need.

The request referred to in paragraph 1 of this Article shall include information on the categories of the requested personal data, their purpose, the legal basis for the use and provision of data for use, the time of the use and sufficient information to identify the data subject whose data is requested.

If personal data is requested for use for the needs of national security, defence and pretrial and criminal procedure, the request may also contain the time until the subject whose data is requested may not know that their data is being used.

Exceptionally, a third party, i.e. personal data user may also request personal data for use based on information that are not sufficient for identification of the data subject as provided for in paragraph 2 of this Article, if prescribed so by a special law.

Article 18

Personal data may be used only for the term necessary to fulfil the purpose which is stated in the request for provision of data for use, unless otherwise established by a special law.

Following the expiry of the term referred to in Paragraph 1 of this Article, the personal data user shall erase the personal data, unless otherwise established by a special law.

Article 19

The personal data controller shall keep records on the third parties, i.e. personal data users, personal data provided for use, the purpose of the use, the legal basis for the use and provision of data for use and the time of use.

The records referred to in paragraph 1 of this Article shall be kept for a period of 10 years, and after that period the data shall be deleted from the records.

4. The obligation of informing data subjects about processing, updating and erasure of personal data

Article 20

Unless otherwise prescribed by a special law, the personal data controller shall provide the data subject from whom the data for processing is directly collected with the following information:

- 1) their personal name, or name and address, as well as the personal name, or name and address of their representative or attorney referred to in Article 5 paragraph 3 of this Law;
- 2) the purpose and the legal basis for personal data processing;
- 3) the third party, i.e. personal data user and the legal basis for provision of data for use;
- 4) whether provision of personal data is mandatory or voluntary and on the possible consequences if provision of such data is denied;

5) the right of access to personal data and the right to rectify the personal data concerning the data subject.

The notification referred to in paragraph 1, subparagraphs 1, 2, 4 and 5 of this Article shall be given at the moment when the data is collected, and the notification referred to in subparagraph 3 of this Article shall be given at the moment when personal data is provided for use the latest.

Article 21

The personal data controller shall, where the data is not collected directly from the data subject it relates to, inform the data subject no later than immediately prior to initiating the processing of personal data, about:

- 1) their personal name or title, permanent or temporary residence or seat as well as their representative;
- 2) the purpose and the legal basis for the processing of personal data;
- 3) the type of personal data undergoing processing;
- 4) the third party, i.e. the personal data user;
- 5) the right of access to personal data and the right to rectify the data concerning them;

Paragraph 1 shall not apply where the personal data controller is not obliged to inform the data subject in cases where the personal data is provided for use for statistical or scientific-research purposes or the processing of personal data is prescribed by law if the provision of such data is impossible or requires activities which are not appropriate to the aim of informing.

In a case referred to in Paragraph 2 of this Article, the personal data controller shall provide for appropriate protection measures.

Article 22

The personal data controller shall ensure that personal data they are processing are correct and complete, taking into account the purpose they are collected for.

Upon the establishment of incomplete or incorrect personal data, the personal data controller shall amend it.

Article 23

The personal data controller shall, at the request of the data subject, erase personal data if its processing is not in accordance with the law.

While the procedure upon the request referred to in paragraph 1 of this Article, i.e. the procedure whereby it is verified whether the personal data is correct and complete in accordance with Article 22 of this Law, is underway, access to the data being processed shall be suspended.

5. Measures for protection of personal data undergoing processing

Article 24

The personal data controller and personal data processor shall provide technical, personnel and organisational measures to protect personal data against the loss, destruction, unauthorized access, alternation, disclosure and abuse.

The measures for personal data protection referred to in paragraph 1 of this Article shall be adequate to the nature and character of the data undergoing processing, having in mind the highest technology level and the costs of their implementation.

If personal data processing is performed electronically, the personal data controller shall ensure that the information system automatically registers personal data users, data being processed, the legal basis for the use of data, case number, the system check in and check out time and, as appropriate, the date until the data on the user are not available to the data subject.

The personal data controller shall determine the personnel who have access to personal data and which personal data they have access to, as well as the categories of data that may be provided for use and the conditions under which they are provided.

The personal data controller shall allow the access to personal data filing systems and keep the records on personal data users in accordance with their act.

Article 25

Any officials and other entities conducting the processing of personal data within a state body, state administration body, local self-government and local government body, company, other legal person, shall act solely according to the instructions of the head of the entity, i.e. the responsible person within the legal person and they shall maintain the confidentiality of personal data they obtained while performing their duties, unless otherwise prescribed by law.

6. Records and registers of personal data filing systems

Article 26

The personal data controller shall keep the records on personal data filing systems he creates.

The records referred to in Paragraph 1 of this Article shall contain:

- 1) filing system title;
- 2) legal basis for personal data processing;
- 3) name or title of the filing system controller, their seat or permanent or temporary residence and address;
- 4) purpose of personal data processing;
- 5) categories of data subjects;
- 6) types of personal data involved in the filing system;
- 7) time periods for storing and using personal data;
- 8) name or title of the third party, i.e. the user, their seat or permanent or temporary residence and address;
- 9) data on transferring personal data out of Montenegro with the indication of the state the data is being transferred to or international organization or other foreign personal data user, the purpose of this transfer defined by an established international agreement and law or defined by a written consent of the data subject;
- 10) internal rules on processing and protection of the controller's personal data which enable a prior analysis of the adequacy of measures aimed at providing security of processing.

The form and the manner of keeping records referred to in Paragraph 1 of this Article shall be defined by the Ministry competent for public administrations affairs.

Article 27

Prior to establishing of an automatic personal data filing system, the personal data controller shall submit a notification to the supervisory body with the data referred to in Article 26 paragraph 2 of this Law. The personal data controller shall act in the same manner when significant changes occur in processing of personal data.

The obligation referred to in paragraph 1 of this Article shall not relate to public registers and records, established in accordance with law.

After establishing of the automatic personal data filing system, the personal data controller shall appoint the person responsible for the protection of personal data. Personal data controller

having less than 10 officers conducting personal data processing does not have to appoint the person responsible for the protection of personal data.

Article 28

If the personal data controller plans to conduct automatic personal data processing which represents a special risk for personal rights and freedoms, they shall obtain consent from the supervisory body prior to each automatic personal data processing, and particularly if:

- 1) it includes processing of special categories of personal data;
- 2) it includes processing of personal data relating to assessment of personality, capacity or behaviour;
- 2a) video surveillance of public areas introduced,
- 3) it is processing of biometric data.

Provisions of paragraph 1 of this Article shall not apply if personal data processing is conducted in accordance with law, if the data subject has provided consent for personal data processing or the processing is necessary in order to fulfill a contract between the personal data controller and the data subject.

Article 29

The register of records on personal data filing systems referred to in Article 26, paragraph 1 of this Law (hereinafter: Register) shall be maintained by the supervisory body.

The data referred to in Article 26, paragraph 2 of this Law shall be entered into the Register.

Except as provided for in Paragraph 2 of this Article, the data on personal data filing systems shall not be entered into the Register where it is required by the interest of defence, national and public security as well as the protection of life and health of people, upon the obtained opinion of the supervisory body.

Article 30

The records from the Register shall be available to the public in the manner defined by the regulations on the work of the supervisory body in accordance with the law.

II. SPECIAL FORMS OF PERSONAL DATA PROCESSING

1. Biometric measures

Article 31

Determination and comparison of the data subject's characteristic by the processing of biometric data for the purpose of establishing and proving their identity may be performed in accordance with this Law (hereinafter: biometric measures).

Article 32

A state body, state administration body, local self-government and local government body, company and other legal person and a sole trader exercising public authority (hereinafter: public sector) may apply biometric measures regarding the entry into the business or official premises and the presence of employees at work, provided these measures are prescribed by law.

The measures referred to in Paragraph 1 of this Article may be prescribed if it is necessary for the security of persons or property or for the protection of confidential data or trade secrets, if this could not be achieved otherwise or for the purpose of fulfilling obligations arising from international agreements and establishing the identity of the persons crossing the state border.

2. The records on the entry into and exit from the business or official premises

Article 33

For the purpose of protecting personal and property security of the business or official premises, the public sector, a company, other legal person and a sole trader may request from the person entering the business or official premises to:

- 1) state the reason for entering the business or official premises;
- 2) provide personal data;
- 3) provide an insight into the identification document, where necessary.

The identification document referred to in Paragraph 1, subparagraph 3 of this Article shall be a document on the establishment of identity issued in accordance with the law.

The personal data referred to in Paragraph 1, subparagraph 2 of this Article shall be a personal name, type and number of identification document, permanent or temporary residence, address and employment.

Article 34

The records may be kept on entries into and exits from the business or official premises.

The records referred to in Paragraph 1 of this Article may contain the personal data referred to in Article 33, paragraph 3 of this Law, date, time, a reason for entering the business or official premises or building and leaving them.

The records referred to in Paragraph 1 of this Article shall have the force of a public document, if the data is used for the purpose of protecting an underage person and conducting police and intelligence and security operations.

The personal data from the records referred to in Paragraph 1 of this Article shall be stored for no longer than one year following the day of collection, whereupon they shall be erased, if not otherwise prescribed by law.

3. Video surveillance

Article 35

The public sector, a company, other legal person and a sole trader may conduct video surveillance of the access to the business or official premises for the sake of the security of persons and property, control of the entry into or exit from the business or official premises or in cases where there is a possible risk to the staff due to the nature of work.

The decision on introducing video surveillance referred to in Paragraph 1 of this Article shall be made by the head of a state body, state administration body, local self-government or local government body or a competent person in a company or other legal person or a sole trader, unless the introduction of video surveillance is prescribed by law.

The decision referred to in Paragraph 2 of this Article shall be made in writing and shall contain the reasons for introducing video surveillance.

The video surveillance referred to in Paragraph 1 of this Article shall be conducted so that neither the recordings of the interior of residential buildings which are not connected to the entrance to business or official premises are shown nor the recordings of the entrances to apartments.

The staff employed in the premises under video surveillance referred to in Paragraph 1 of this Article shall be informed in writing about video surveillance.

The access to the recordings of the video surveillance system referred to in Paragraph 1 of this Article shall be forbidden via internal cable television, public cable television, the Internet or other means of electronic communications through which such recordings can be transmitted, whether at the moment of their recording or afterwards.

Article 36

The public sector, a company or other legal person and a sole trader may conduct video surveillance in the official or business premises if required by reasons of protection of the security of persons or property or confidential data and trade secrets and if it cannot be accomplished otherwise.

Video surveillance shall not be allowed in official and business premises outside the work place, particularly in cloakrooms, lifts and sanitary premises and in the area envisaged for clients and visitors.

The decision on introducing video surveillance referred to in Paragraph 1 of this Article, if the introduction of video surveillance is not prescribed by law, shall be made by the head of a state body, local self-government and local government body or a competent person in a company or other legal person or a sole trader.

The persons referred to in Paragraph 3 of this Article shall, prior to reaching a decision on introducing video surveillance, obtain an opinion of the competent trade union or the representative of the staff.

The employed must be informed about the introduction of video surveillance in writing prior to initiating video surveillance.

The provision of Paragraph 4 of this Article shall not apply to official or business premises of state bodies responsible for the affairs concerning defence, national and public security and protection of confidential data.

Article 37

The records shall be kept on the video surveillance referred to in Article 35 Paragraph 1 and Article 36, paragraph 1 of this Law.

The records referred to in Paragraph 1 of this Article may comprise: a recording of a person (image or sound or image and sound), date and time of recording the entry and exit and, as necessary, the personal name of the recorded person, their permanent or temporary residence and address, employment, type and number of the identification document, the reasons for the entry if the entered personal data were collected through the recording of the video surveillance system or otherwise.

The personal data from the records referred to in Paragraph 1 of this Article shall be stored for no longer than six months from the day of recording.

Article 38

Video surveillance of the entry into and exit from the building, as well as of common premises may be conducted in residential buildings.

For the purpose of introducing video surveillance in a residential building, the assembly of condominium owners shall give its consent in a written form.

The consent referred to in Paragraph 2 of this Article shall be deemed to have been given if the members of the assembly of the owners of a residential building or a terraced house with more than 70% ownership endorsed it.

Video surveillance of entrances to apartments shall not be conducted.

Article 39

The public sector, a company or other legal person and a sole trader who conducts video surveillance shall put up a public notice about video surveillance.

The notice referred to in Paragraph 1 of this Article shall be put up in a visible place in the manner which enables people to become familiar with the video surveillance prior to initiating video surveillance and no later than the moment of initiating video surveillance.

The notice referred to in Paragraph 1 of this Article contains data on:

- 1) the title of the person conducting video surveillance;
- 2) the telephone number which provides information where and how long the video surveillance recordings are stored.

The person shall be deemed to have been informed about the personal data processing through video surveillance by putting up the notice referred to in Paragraph 1 of this Article.

The video surveillance system used for conducting video surveillance shall be protected from the access of unauthorised persons.

Article 40

The provisions of Art. 35 and 37 of this Law shall be accordingly applied to video surveillance of public areas unless otherwise defined by a special law.

Article 40a

If the video surveillance of public areas is done without notice referred to in Article 27, Paragraph 1, and approvals referred to in Article 28, Paragraph 1, Point 2a of this Law, the supervisory authority shall order the removal of means used for video surveillance.

The removal of the means referred to in paragraph 1 of this article is carried out by the entity that manages the public area, that is, the object on which the means used for video surveillance are installed.

III. TRANSFER OF PERSONAL DATA OUT OF MONTENEGRO

Article 41

The personal data undergoing processing may be transferred out of Montenegro to another state or provided for use to an international organization which applies appropriate measures of personal data protection prescribed by this Law, on the basis of previously obtained consent of the supervisory body.

The adequacy of protection measures referred to in Paragraph 1 of this Article shall be assessed according to specific circumstances under which the procedure of personal data transfer or the transfer procedure of a set of this data is carried out, and in doing so, the following is especially taken into account:

- 1) the nature of personal data;
- 2) the purpose and duration of the proposed procedure or the processing procedure;
- 3) the country of origin or the country of final destination;
- 4) legally prescribed regulations which are applicable in the country to which the data is transferred;
- 5) the rules of the profession and security measures which must be observed in that country.

The consent of the supervisory body shall be necessary for the transfer of personal data for the purpose of delegating certain processing tasks in the meaning of Article 16 of this Law, except in the case referred to in Article 42, subparagraph 6 of this Law.

Article 42

The consent referred to in Article 41, paragraph 1 of this Law shall not be necessary where:

- 1) the transfer of personal data is prescribed by a special law or international agreement Montenegro is bound by;
- 2) a prior consent has been obtained from the data subject whose data is being transferred and where the data subject is familiar with possible consequences of the data transfer;
- 3) the transfer of personal data is necessary for carrying out the contract between a legal or natural person and the personal data controller or for fulfilling pre-contractual obligations;
- 4) the transfer of personal data is necessary for saving the lives of data subjects or where it is in their interest;
- 5) the transfer of personal data is carried out from registers or records which are, in accordance with the law or other regulations, available to the public;
- 6) the data is transferred to the EU member states and the countries of the European Economic Community or the EU candidate countries which have an adequate level of personal data protection;

7) the transfer of personal data is necessary for the purpose of achieving the public interest or achieving or protecting legal interests of the data subjects;

8) the personal data controller concludes a contract which contains relevant contractual obligations adopted by the EU member states with the personal data processor from the country which is not a member state of the EU; and

9) the transfer of personal data is necessary for the purpose of concluding or meeting the contract between the personal data controller and a legal or natural person, where the contract is in the interest of the data subject whose data is being processed.

V. RIGHTS OF DATA SUBJECTS TO PERSONAL DATA PROTECTION

Article 43

The personal data controller shall, upon a written request from the data subject, or their legal representative or attorney, upon establishing of the identity of the data subject, not later than 15 days from the day of submitting the request, submit the notification as to whether the personal data relating to them are being processed.

If the data on the subject are being processed, the notification of the personal data controller referred to in paragraph 1 of this Article, shall include additional information on:

- 1) the personal name, i.e. official name and address of the personal data controller;
- 2) the name, i.e. official name and address of the personal data processor when that is explicitly required;
- 3) the content of the data being processed;
- 4) the purpose and the legal basis for personal data processing;
- 5) on the data source according to the information available;
- 6) the third party, i.e. the user; and
- 7) the manner of automatic personal data processing in the case referred to in Article 15a of this Law.

The notification referred to in paragraph 1 of this Article shall be given in written form and shall be comprehensible.

Article 44

Upon a written request from the data subject or their legal representative or attorney, within 15 days from the day of submitting the request, the personal data controller shall:

- 1) supplement incomplete data or amend or erase incorrect personal data;
- 2) erase personal data if its processing is not in accordance with the law;
- 3) deleted;
- 4) deleted.

The personal data controller shall, within 8 days, inform the data subject or their legal representative or attorney, as well as the third party, i.e. the user of personal data, about the implemented amendment, erasure or suspension of the personal data use referred to in Paragraph 1 of this Article, unless this proved to be impossible.

If the personal data controller fails to act in accordance with par. 1 and 2 of this Article or denies a request referred to in paragraph 1 of this Article, the data subject shall be entitled to file a complaint to the personal data controller in accordance with a special law, or to request protection of their rights from the supervisory body.

Article 45

The rights of data subjects referred to in Articles 43 and 44 of this Law may be restricted if deemed necessary for the reasons of defence, national and public security, to prevent criminal offences, for the detection and prosecution of criminal offenders, protection of the economic or financial interest, as well as for the protection of data subjects or rights and freedoms of others, within the scope necessary for the fulfilment of the purpose for which the restriction has been determined, in accordance with a special law.

Article 46

Costs of the procedure referred to in Articles 43 and 44 of this Law shall be borne by the personal data controller, unless otherwise prescribed by law.

Article 47

A person who considers that any of their rights guaranteed by this Law have been violated may submit a request for the protection of rights to the supervisory body.

The supervisory body shall issue a decision regarding the request, within 60 days from the day of submitting the request.

The procedure and decision-making upon the request referred to in Paragraph 1 of this Article are carried out in accordance with provisions of Articles 66 to 73 of this Law.

Upon a written request of a person asking for the protection of their rights, the supervisory body may issue a temporary decision prohibiting further processing of personal data until the decision referred to in Paragraph 2 of this Article is passed, if the violation of rights defined by this Law has been committed or if there is reasonable doubt that it has been committed.

The administrative proceedings can be initiated against the decision referred to in Paragraph 2 of this Article.

Article 48

The personal data controller shall be responsible for the damage suffered by the data subject as a result of the violation of rights prescribed by this Law, in accordance with general regulations regarding the compensation of damages.

VI. PERSONAL DATA PROTECTION AGENCY

Article 49

The Agency for personal data protection (hereinafter: Agency) shall be established for the purposes of performing the activities of the supervisory body defined by this Law

The Agency shall be independent in performing the activities within its competences.

The Agency shall be a legal person.

Article 50

The Agency shall:

- 1) supervise the implementation of personal data protection in accordance with this Law;
- 2) resolve requests for the protection of rights;
- 3) pass an opinion regarding the application of this Law;
- 4) give consent regarding the establishment of personal data filings system;
- 5) pass an opinion where there is doubt whether a particular set of personal data is considered a filing system in the meaning of this Law ;
- 6) monitor the application of organizational and technical measures for personal data protection and propose improvements of these measures;
- 7) give proposals and recommendations for the improvement of personal data protection;
- 8) express an opinion as to whether a particular method of personal data processing threatens the rights and freedoms of data subjects;
- 9) cooperate with the bodies competent for supervision of personal data protection in other countries;
- 10) cooperate with competent state bodies in preparing draft regulations regarding personal data protection;
- 11) give a proposal for the assessment of constitutionality of the laws or constitutionality and legality of other regulations and general acts which regulate personal data processing issues;

12) perform other tasks in accordance with the law regulating free access to information and this Law.

Article 51

The bodies of the Agency are the Council and Director.

Article 52

The Council of the Agency has the president and two members.

The President and the members of the Agency's Council shall be appointed by the Parliament of Montenegro (hereinafter: Parliament), upon a proposal by a competent working body.

The President and the members of the Agency's Council shall be appointed for a period of five years and they cannot be appointed to these functions more than twice.

The President and the members of the Agency's Council shall be accountable to the Parliament for their work.

Refer to: Article 1 of the Law - 70/2009-1.

Article 53

The President or a member of the Agency's Council may be appointed if they fulfil the following requirements:

- 1) to be a citizen of Montenegro;
- 2) to have a university degree;
- 3) to have five years of work experience in performing tasks in the area of human rights and freedoms.

Article 54

The President or a member of the Agency's Council may not be a person who:

- 1) is a member of the Parliament;
- 2) is a member of the Government;
- 3) has been appointed by the Government of Montenegro;
- 4) is an official of a political party (the President of a party, a member of the Presidency, their deputy, a member of the Executive and General Committee and other party official);
- 5) is convicted for a criminal offence prosecuted ex officio, regardless of the pronounced sanction or is convicted for other criminal offence to a prison sentence longer than six months in the period during which legal consequences of conviction are still present;
- 6) is a spouse of the person referred to in Articles 1, 2 and 3 of this Paragraph or is a member of their nucleus family, first cousin once removed and a relative-in-law.

The applicant for a member of the Agency's Council shall submit a written statement to the competent working body referred to in Article 52, paragraph 2 of this Law that there are no obstacles to the appointment defined by this Law.

Article 55

The President or a member of the Agency's Council may be recalled before the expiration of the office term.:

- 1) at a personal request;
- 2) due to permanent loss of working ability to perform the function;
- 3) in case of occurrences referred to in Article 54 of this Law;
- 4) If they violate the obligation of storing personal data.

Article 56

The Agency's Council shall:

- 1) adopt the regulations of the Agency;

- 2) adopt the Statute and the Act on Systematization, with the consent of the working body referred to in Article 52, Paragraph 2 of this Law, as well as other acts of the Agency;
- 3) prepare an annual and special report on the state of personal data protection;
- 4) establish an annual work plan and an annual report on the work of the Agency;
- 5) outline a proposal of the financial plan and annual balance sheet;
- 6) issue decisions upon complaints referred to in Article 68 paragraph 3 of this Law;
- 6a) decide in accordance with the law regulating free access to information;
- 7) perform other activities defined by the law and the Agency's Statute.

Regulations referred to in Paragraph 1, subparagraph 1 of this Article shall be published in the "Official Gazette of Montenegro".

Article 57

The Agency's Council shall decide by a majority of votes of the overall number of the Council's members.

Article 58

The Agency's Council shall appoint the Director of the Agency on the basis of a public job announcement for a period of four years.

The person who does not fulfil the requirements for a member of the Agency's Council according to this Law may not be appointed as the Agency's Director.

Article 59

The Director of the Agency shall:

- 1) represent the Agency;
- 2) organize and run the Agency;
- 3) execute decisions of the Agency's Council;
- 4) propose the work plans, reports on the state of personal data protection to the Agency's Council, opinions regarding application of this Law, opinions when there is doubt whether a specific set of personal data is considered a data filing system as stipulated in this Law, opinions whether a specific manner of personal data processing compromises rights and freedoms of data subject, proposals and recommendations for improvement of personal data protection, submission of proposals for the assessment of the constitutionality of the law, i.e. constitutionality and legality of other regulations and general acts regulating personal data processing;
- 5) perform other activities defined by this Law and the Statute of the Agency.

Article 59 a

The salary of the President and the members of the Agency's Council, as well as of the Director of the Agency shall be defined by the Statute of the Agency.

+ **Refer to : Article 2 of the Law - 70/2009-1.**

Article 60

The Agency shall have a professional service.

General labour regulations shall apply to the rights, obligations and responsibilities of the employees of the Agency's professional service.

Article 61

The Agency shall have the Statute.

The Statute of the Agency shall contain:

- 1) seat and activity of the Agency;
- 2) internal organization of the Agency;
- 3) method of work, decision-making and competences of the Agency's bodies.

Article 62

The Agency shall submit an annual report on the state of personal data protection to the Parliament until 31st March of the current year for the previous year.

The Agency shall submit a special report on the state of personal data protection to the Parliament:

- 1) at the request of the Parliament,
- 2) if the Agency estimates that there are special reasons for that .

The report referred to in Paragraph 1 of this Article shall include an analysis of the state in the area of personal data protection, procedures initiated on the basis of this Law and proposed measures as well as the data on the level of respecting the rights of data subjects during personal data processing.

Reports referred to in Paragraph 1 and 2 of this Article shall be made available to the public.

Article 63

The funds for the operations of the Agency shall be provided from the budget of Montenegro or from other sources in accordance with the law.

Article 64

The President and a member of the Council, the Director of the Agency and the employees of the Agency shall ensure the confidentiality of all the data they come across while performing their duties, in accordance with the regulations which stipulate the data confidentiality.

The obligation referred to in Paragraph 1 of this Article shall continue to apply even after the termination of the term of office of the Agency's Director, or the termination of employment in the Agency.

VII. SUPERVISION

Article 65

The Agency shall perform supervision in accordance with this Law through the persons employed in that body who are competent for performing supervisory activities, in accordance with the Act on Systematization (hereinafter: Supervisor).

The Supervisor may be a person who, apart from general requirements prescribed by law, fulfils the following requirements:

- 1) has a university degree;
- 2) has five years of work experience;
- 3) has passed a state examination for the work in state bodies;
- 4) has not been convicted for a criminal offence which makes them unsuitable for the employment in a state body;
- 5) criminal proceedings is not being conducted against them.

The procedure of supervision referred to in Paragraph 1 of this Article shall be initiated and conducted ex officio.

Any person may submit an initiative for initiating the supervisory procedure.

Article 66

The Supervisor shall have the right of access to personal data contained in personal data filing systems regardless of whether the records on the filing systems are kept in the Register as well as the right of access to files and other documentation regarding personal data processing and to the means of electronic data processing.

The Supervisor shall have the right of access to the personal data referred to in Paragraph 1 of this Article in performing tasks within their competences, regardless of the level of confidentiality.

Article 67

The personal data controller, user or personal data processor shall enable the access to filing systems, files and other documentation, as well as to the means of electronic data processing and shall submit the requested files and other documentation at the Supervisor's request.

Article 68

The record shall be made on the performed supervision referred to in Article 65 of this Law, within 15 days from the day of the performed supervision and it shall be submitted to the personal data controller.

Where the supervision is performed upon the request for the protection of rights referred to in Article 47 of this Law, the Supervisor shall conduct the procedure and draw up a record immediately, no later than 8 days from the day of submitting the request. The record shall be submitted to the person who submitted the request for the protection of rights and to the personal data controller.

The personal data controller as well as the person who submitted the request for the protection of rights may, within eight days from the day of the receipt of the record, file an appeal to the Agency against the record referred to in Paragraphs 1 and 2 of this Article.

Article 69

If the Agency establishes that the appeal of the personal data controller against the record in which irregularities in the personal data processing have been detected, is unfounded, it shall impose measures referred to in Article 71 of this Law.

In the case referred to in Paragraph 1 of this Article, the Agency shall submit a request for initiating the criminal proceedings.

Article 70

If the Agency, according to the record on performed supervision, establishes that there are no irregularities in the personal data processing which have been stated in the request for the protection of rights or in the appeal against the record, it shall reject the request by a decision.

Where the Agency, acting upon the appeal against the record of the person who submitted the request for the protection of rights, which stated that there were no irregularities in personal data processing related to them, establishes that the appeal is founded, it shall impose measures referred to in Article 71 of this Law on the personal data controller.

Article 71

In performing supervision, the Agency shall be authorized to issue a decision:

- 1) ordering that irregularities in personal data processing be eliminated within a certain time period;
- 2) temporarily prohibiting the processing of personal data processed contrary to this Law;
- 3) ordering erasure of personal data collected without a legal basis;
- 4) prohibiting the transfer of personal data out of Montenegro or providing personal data to personal data users contrary of this Law;
- 5) prohibiting the assignment of personal data processing tasks where the personal data processor does not fulfil the requirements regarding personal data protection or where the assignment of these tasks has been carried out contrary to this Law.

Article 72

The administrative proceedings may be initiated against the decision of the Agency.

Article 73

The regulations which govern the supervision and administrative procedure shall be accordingly applied to the procedure and method of supervision, obligations and competences

of the Supervisor and other issues of importance for the supervision, unless otherwise prescribed by this Law.

Article 73a

Trading associations and other bodies representing special categories of personal data controllers shall submit their rules of work and conduct to the Agency, as well as acts based on which they conduct personal data processing.

The Agency shall provide consent and assess compliance of the rules with this Law.

VIII. CRIMINAL PROVISIONS

Article 74

A legal person shall be charged for an offence with a fine from EUR 500 to EUR 20,000 if:

- 1) they process personal data contrary to Article 10 of this Law;
- 2) they process special categories of personal data contrary to Article 13 of this Law;
- 3) they process personal data regarding criminal and misdemeanour proceedings contrary to Article 14 of this Law;
- 4) they do not keep records on third parties i.e. personal data users (Article 19 paragraph 1);
- 5) they assign the tasks of personal data processing within their competences to the personal data processor which is not registered for performing the tasks of personal data processing or which does not fulfil the requirements for implementing technical, personnel and organizational measures for personal data protection (Article 16 paragraph 3);
- 6) the data belonging to one of the special categories are used for direct marketing purposes without the consent from the data subject (Article 15 paragraph 2).
- 7) they do not erase personal data if their processing is not in accordance with Article 23 paragraph 1 of this Law;
- 8) they do not provide technical, personnel and organizational measures for personal data protection for the purposes of protection from the loss, destruction, unauthorised access, alternation, disclosure and abuse (Article 24 paragraph 1);
- 9) they do not submit notification to the supervisory body prior to establishing automatic personal data filing system (Article 27 paragraph 1);
- 10) they conduct video surveillance so that recordings of the interior of residential buildings which are not connected to the entrance to residential and official premises are shown or they record entrances to apartments (Article 35);
- 11) they do not inform the employed in the premises under video surveillance in a written form about conducting video surveillance and do not pass a decision (Article 35 paragraph 5);
- 12) they conduct video surveillance in official or business premises outside the workplace (Article 36 paragraph 2);
- 13) they do not inform the employees in a written form about the introduction of video surveillance prior to initiating video surveillance (Article 36 paragraph 5);
- 14) they record entrances to apartments of data subjects through the video surveillance system (Article 38 paragraph 4);
- 15) they do not put up a public notice about video surveillance in a visible place (Article 39 paragraphs 1 and 2);
- 16) the public notice about video surveillance does not include the prescribed information (Article 39 paragraph 3);
- 17) they do not protect the video surveillance system from the access of unauthorized persons (Article 39 paragraph 5);
- 18) they do not provide the data subject with a notice within 15 days from the day of submitting the request (Article 43);
- 19) they do not amend, erase or suspend the use of personal data within 15 days from the day of submitting the request (Article 44 paragraph 1);

20) they do not inform the data subject, or their legal representative or attorney, as well as the personal data user about the implemented amendment, erasure and suspension of the personal data use within eight days (Article 44 paragraph 2);

21) the user or processor fails to act upon the order or prohibition of the Agency (Article 71).

A responsible person in a legal person in a state body, state administration body, local government body, local self-government body and a natural person shall be charged for the offence referred to in paragraph 1 of this Article with a fine from EUR 150 to EUR 2,000.

A sole trader shall be charged for the offence referred to in paragraph 1 of this Article with a fine from EUR 150 to EUR 6,000.

IX. TRANSITIONAL AND FINAL PROVISIONS

Article 75

The President and the members of the Agency's Council shall be appointed in accordance with this Law within 6 months from the day of entry into force of this Law.

The Director of the Agency shall be appointed within 3 months from the day of the appointment of the Agency's Council.

Article 75a

The Agency for Personal Data Protection established in accordance with the Law on Personal Data Protection ("Official Gazette of Montenegro" no. 79/08) shall continue its work under the following name: the Agency for Personal Data Protection and Free Access to Information.

Article 76

Bylaws for the implementation this Law shall be adopted within 3 months from the day of the appointment of the Agency's Council.

Article 77

The personal data filing systems established until the entry into force of this Law shall be harmonized with this Law, within 9 months from the day of entry into force of this Law.

The personal data filing systems controllers shall establish the records referred to in Article 26 of this Law and submit them to the Agency within 15 months from the day of entry into force of this Law.

The public sector, company, other legal person and sole trader shall harmonize the records on the entry into and exit from the premises and video surveillance with this Law within 18 months from the day of entry into force of this Law.

Article 78

The Law on Personal Data Protection (Official Gazette SRY, No. 24/98) shall cease to be applied as of the day of the entry into force of this Law.

Article 79

This Law shall enter into force on the eight day following its publication in the "Official Gazette of Montenegro" and shall be applied upon the expiration of a six-month term following the day of its entering into force.

