PERSONAL DATA PROTECTION LAW

(Official Gazette of Montenegro 79/08 and 70/09)

I GENERAL PROVISIONS

Article 1

Protection of data relating to individuals shall be provided under the conditions and in the way laid down by this law, in accordance with the principles and standards contained in the ratified international human rights treaties and generally recognised rules of international law.

Article 2

The processing of data relating to individuals (hereinafter referred to as "personal data") may be carried out for a lawful purpose or with the prior consent of the data subject.

Personal data may be processed only to the extent necessary to achieve the purpose of processing and in a way compatible with the aims for which they were collected.

Notwithstanding paragraph 1 of this Article, personal data may be processed for statistical purposes or for the purposes of scientific research, subject to the provision of appropriate safeguards.

Where the personal data filing system controller makes personal data available for processing for statistical purposes or for the purposes of scientific research, such data must be made available in a way that the identity of the individual is not disclosed.

Article 3

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

If the length of time for which processed personal data are to be stored is not laid down by the law, personal data which allow the identity of an individual to be established may be stored only for the time required to achieve the purpose for which personal data are processed.

Article 4

Protection of personal data shall be provided to every individual, regardless of nationality, domicile, race, skin colour, sex, language, religion, political or other belief, ethnicity, social origin, property, education, social position or other personal attributes.

Article 5

This law must be complied with by the state authority, public administration body, local self-government and local administration authority, commercial enterprise and other legal person, entrepreneur and natural person, with the seat or domicile in Montenegro, which carries out processing of personal data or establishes personal data filing systems in the way and for the purpose established by law or its legal act (hereinafter referred to as "personal data filing system controller").

The provisions of this law also apply to a personal data filing system controller whose seat or domicile is outside Montenegro if the equipment for processing of personal data is situated in Montenegro, unless such equipment is used only for purposes of transit through the territory of Montenegro.

In the circumstances referred to in paragraph 2 of this Article, the controller shall designate a representative or an attorney with the seat or domicile in the territory of Montenegro who shall be responsible for the application of this law.

Article 6

Where the purpose of personal data and the way of their processing is laid down by law, the personal data filing system controller shall be determined by such law.

Article 7

This law shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means which forms part of a personal data filing system or is intended to form part of a personal data filing system.

If the processing of personal data is carried out by electronic means, the personal data filing system controller must ensure that the information system automatically records the recipients of personal data, data which were processed, legal grounds for the use of personal data, time of logging on to the system and time of logging out of the system.

Article 8

The provisions of this law, save for the provisions on supervision, shall not apply to the processing of personal data for the purposes of defence, national and public security nor in pre-trial and criminal proceedings, unless otherwise provided by a separate law.

The provisions of this law shall not apply to the processing of personal data by a natural person in the course of a personal activity.

The rights of data subjects provided for by this law may be restricted only when such restriction constitutes a necessary measure to conduct pre-trial and criminal proceedings and only for the duration of such proceedings.

Article 9

Specific terms used in this law shall have the following meaning:

1) 'personal data' shall mean any information relating to an identified or identifiable natural person;
2) 'processing of personal data' shall mean any operation which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, use, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, as well any other operation performed upon personal data;
3) 'personal data filing system' shall mean any structured, whether centralized, decentralized or dispersed on a functional or geographical basis, set of personal data which are undergoing processing and which may be accessible according to the specific criteria;
4) 'recipient of personal data' shall mean a public authority, public administration body, self-government or local administration authority, commercial enterprise or

another legal person, entrepreneur of a natural person, to whom personal data may be made available for use in accordance with the law;

5) 'processor of personal data' shall mean a public authority, public administration body, self-government or local administration authority, commercial enterprise or other legal person, entrepreneur of a natural person, who performs tasks concerning the processing of personal data on behalf of the controller, in accordance with this law;
6) 'consent' shall mean a free statement given in writing or orally on record by which an individual signifies his agreement to personal data relating to him being processed for a specific purpose;
7) 'special categories of data' shall mean personal data concerning racial or ethnic origin, political, religious or other beliefs, social origin, trade-union membership, data concerning health, sex life or sexual orientation, biometric data, as well as data from registers of misdemeanour and criminal convictions;
8) 'biometric data' shall mean data on physical or physiological features intrinsic to every natural persons, which are specific, unique and unchangeable and capable of revealing the identity of an individual either directly or indirectly;
9) 'data subject' shall mean a natural person who is identified or can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

II PROCESSING OF PERSONAL DATA

1. Conditions

Article 10

Personal data may be processed with the prior consent of the data subject.

Personal data may be processed without the consent of the data subject when processing is necessary:

1) for the performance of legal obligations to which the controller is subject or the exercise of authority vested in the controller;
2) for the protection of life and health of an individual who is not in the position to give his consent personally;
3) in order to take steps prior to entering into a contract and for the performance of a contract in accordance with the law;
4) for the performance of a task carried out in the public interest or in the exercise of public authority falling within the scope of work or competence of the personal data filing system controller or personal data recipient;
5) for the purposes of a legitimate interest pursued by the personal data filing system controller or by the recipient of personal data, except where such interest should be restricted in order to ensure exercise and protection of rights and freedoms of individuals.

The consent referred to in paragraph of this Article shall be given by the guardian on behalf of a person deprived of the capacity to transact business and by the parents or

adoptive parents on behalf of a minor, unless the consent is contrary to the interests of the minor.

The consent to the processing of personal data on behalf a deceased shall be given by his successors determined in accordance with the law governing succession, unless the deceased has forbidden the processing of personal data.

Article 11

The data subject may request the personal data filing system controller to erase personal data which have not been obtained from him directly.

In the case referred to in paragraph 1 of this Article, the personal data filing system controller must erase personal data from the personal data filing system within 30 days from the submission of the request.

Where personal data are processed for statistical purposes or for the purposes of scientific research, the data subject may request the erasure of his personal data only if such data are capable of revealing his identity.

Article 12

Personal data concerning children shall be processed in accordance with the law, in a manner which is in the best interest of the child.

Article 13

The special categories of data may be processed where:

1) the data subject has given his consent to the processing of those data;
2) processing is necessary for the purpose of detecting, preventing or diagnosing of data subject illness or carrying out his medical treatment, as well for the improvement of health services, in so far as the processing is done by a health worker or other person subject to the duties of keeping professional secret;
3) processing is necessary to protect the life, health or interests of the data subject or of another person where the data subject is not in the position to give his consent personally, as well as in other cases provided for by law;
4) the data subject has manifestly made personal data available to the public or the processing is necessary for the establishment or protection of legal interest;
5) processing is carried out in the course of activities of an association or any other non-profit-seeking body with political, religious or other aims, provided that the data relates solely to such association or other organisation and that the data are not disclosed without the consent of the data subjects.

The special categories of data shall be distinctively designated and protected in order to prevent unauthorised access.

The manner of designating of personal data referred to in paragraph 2 of this Article shall be established by the ministry responsible for public administration affairs.

Article 14

The processing of personal data relating to criminal offences, criminal or misdemeanour penalties or security measures may be carried out only by or under the supervision of the competent state authority, provided that measures to safeguard personal data are provided in accordance with the law.

Article 15

The processing of personal data from publicly available sources for the purposes of direct marketing may not be carried out without the consent of the data subject.

Where, in the case referred to in paragraph 1 of this Article, the data subject has given his consent to the processing of his personal data, such consent may be revoked.

The personal data filing system controller may use the data from the filing system which were collected in the exercise of lawful authority or carrying out of an activity for the purposes of direct marketing, without the consent of the data subject.

In the case referred to in paragraph 3 of this Article, the data subject may prohibit the use of his personal data for the purposes of direct marketing.

2. The carrying out of processing by way of a processor

Article 16

The personal data filing system controller may entrust specific activities concerning processing of personal data to a processor of personal data by way of a contract, which must be in writing.

The contract referred to in paragraph 1 of this Article shall stipulate mutual rights and obligations of the personal data filing system controller and the personal data processor.

The activities referred to in paragraph 1 of this Article may be entrusted only to a personal data processor registered for carrying out the processing of personal data and providing guarantees in respect of the technical, personnel and organizational measures for the protection of personal data in accordance with this law.

The personal data processor must destroy or return the personal data to the personal data fling system controller after the processing.

3. Making data available for use

Article 17

The personal data filing system controller must, on request, give to the recipient personal data he requires for the purpose of performing legal obligations and exercising authority within his scope of work or competence.

The request referred to in paragraph 1 of this Article shall include information on the category and purpose of personal data, legal basis for the use of the data and the length of time the data are to be used.

Article 18

Personal data may be used only for the period of time necessary to achieve the purpose of use, unless otherwise provided by a separate law.

After the expiry the period referred to in paragraph 1 of this Article, the recipient of personal data must erase the data, unless otherwise provided by a separate law.

Article 19

The personal data filing system controller shall keep records of the data made available for use, the recipients of personal data, the purpose they have been given for and the legal basis for use of personal data.

4. Obligation to inform data subject about the processing, updating and erasure of personal data

Article 20

The personal data controller or processor of personal data must provide a data subject from whom data relating to himself are collected for the purpose of processing with the following information:

1) his name, domicile or temporary residence, or seat respectively, as well the identity of his representative in the case of personal data filing system controller;
2) the purpose of data processing;
3) the recipients or categories of recipients of the data;
4) the obligation to disclose personal data;
5) possible consequences of the denial to disclose personal data;
6) the existence of the right of access to and the right to rectify the data concerning him.

The information set out in paragraph 1 clauses 3, 4, 5 and 6 shall be given only in so far as such information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing.

Article 21

Where the data have not been obtained from the data subject, the personal data controller must provide the data subject with the following information no later than at the time when the processing begins:

1) his name, domicile or temporary residence, or seat respectively, as well the identity of his representative;
2) the purposes of the data processing;
3) the categories of data o be processed;
4) the recipients of personal data;
5) the existence of the right of access to and the right to rectify the data concerning him.

Notwithstanding paragraph 1 of this Article, the personal data filing system controller shall not be bound to provide the data subject with information when personal data are made available for use for statistical purposes or for the purposes of scientific research, if the provision of such information proves impossible or would involve a disproportionate effort.

In the case referred to in paragraph 2 of this Article, the personal data filing system controller must provide appropriate safeguards.

Article 22

The personal data filing system controller must keep personal data up to date.

When he finds that personal data are incomplete or inaccurate, the personal data filing system controller must supplement or alter them.

Article 23

The personal data filing system controller must, on request of the data subject, erase personal data if their processing does not comply with the law.

The personal data filing system controller must inform the data subject and the recipient of personal data about the alteration or supplementing of personal data referred to in Article 22 paragraph 2 of this law, as well as about the erasure of personal data referred to in paragraph 1 of this Article, no later than 8 days from the day of alteration, supplementing or erasure.

5. Measures to safeguard personal data during processing
6.

Article 24

The personal data filing system controller and the recipient of personal data must implement technical, personnel and organizational safeguards to protect personal data against loss, destruction, unauthorized access, alteration, publicizing and abuse.

The safeguards referred to in paragraph 1 of this Article must be appropriate to the nature and character of the data processed.

Where personal data are stored for longer periods of time for statistical purposes and for the purposes of scientific research, the safeguards referred to in paragraph 1 of this Article shall be provided in accordance with a separate law.

Technical measures and standards, as well as personnel and organisational safeguards shall be established by the personal data filing system controller.

The personal data filing system controller shall allow access to personal data filing systems and keep records of the recipients of personal data in accordance with his internal act.

Article 25

Officers and other employees carrying out the processing of personal data in a state authority, public administration body, local self-government and local administration authority, commercial enterprise, processor of personal data, other legal person, as well as with an entrepreneur and another natural person must keep the secrecy of personal data they become privy to in the course of performance of their tasks.

6. Records and registers of personal data filing systems

Article 26

The personal data filing system controller shall keep records of personal data filing system he establishes.

The records referred to in paragraph 1 of this Article shall include:

1) the name of the personal data filing system;
2) the legal basis for processing of personal data;
3) the name, seat or domicile or residence respectively and the address of filing system controller;
4) the purpose of processing;
5) the categories of data subjects;
6) the categories of data contained in the personal data filing system;
7) the manner of collecting and storing personal data;
8) the time limits for storing and use of personal data;

9) the name of the recipient of personal data, his seat or domicile or residence respectively, and his address;
10) information on transfer of personal data from Montenegro together with the name of the country, international organization or other foreign recipient of personal data to which data are being transferred, the purpose of the transfer as established by a ratified international treaty, law, or by a written agreement;
11) Internal rules of the filing system controller regarding processing and safeguarding personal data, which allow a preliminary assessment to be made of the appropriateness of the measures taken to ensure security of processing.

The template and manner of keeping the records referred to in paragraph 1 of this Article shall be established by the ministry responsible for public administration affairs.

Article 27

The personal data filing system controller must, prior to establishing a personal data filing system obtain the consent of the supervisory authority.

The personal data filing system controller must accompany the request for consent with the information set out in Article 26, paragraph 2 of this law.

If the supervisory authority fails to issue the reply referred to in paragraph 2 of this Article within 30 days from its submission, it shall be considered that the consent has been given.

Article 28

The personal data filing system controller must obtain the consent of the supervisory authority prior to the altering of data referred to in Article 26, paragraph 2 of this Law.

If the supervisory authority fails to issue the reply referred to in paragraph 1 of this Article within 30 days from its submission, it shall be considered that the consent has been given.

The provisions of paragraph 1 of this Article shall not apply to personal data filing systems where the purpose of personal data or categories of personal data to be processed, categories of data subjects, recipients or categories of recipients of personal data, as well as the length of time the data are to be stored are established by the law.

Article 29

A register of records of personal data filing systems referred to in Article 26 of this law (hereinafter referred to as “the Register”) shall be kept by the supervisory authority.

The information set out in Article 26, paragraph 2 of this law shall be entered into the Register.

Notwithstanding paragraph 1 of this Article, information on personal data filing systems shall not be entered into the Register when so required by the interests of defence, national or public security, in line with an opinion delivered by the supervisory authority.

Article 30

The records from the Register shall available to the public in a way established by the rules on work of the supervisory authority, in accordance with the law.

III SPECIAL CATEGORIES OF PERSONAL DATA PROCESSING

1. Biometric measures

Article 31

The establishment and comparison of personal traits for the purpose of establishing and proving the identity of an individual (hereinafter referred to as "biometric measures") may be performed in accordance with this law.

Article 32

The state authority, public administration body, local self-government and local administration authority, commercial enterprise or other legal person and an entrepreneur exercising public authority (hereinafter referred to as "the public sector") may carry out biometric measures in connection with the entry into business or official premises and presence at work of employees, if such measures are provided for by the law.

The measures referred to in paragraph 1 of this Article may be provided for if so necessary for the protection of individuals and property or for the protection of secrecy of data or business secrets, where these aims cannot be achieved in other way or where this is required in order to discharge of the obligations stemming from international treaties and establish the identity of individuals crossing the state borders.

2. Records on entry and exit from business or official premises

Article 33

In order to protect the safety of individuals and property within business or official areas, the public sector, commercial enterprise, other legal person and entrepreneur may request an individual entering business or official areas to:

1) state the reasons for entering business or official areas;
2) give personal data;
3) present an identity document for inspection, if so required.

The identity document referred to in paragraph 1, clause 3 of this Article shall mean a document on establishment of identity issued in accordance with the law.

The personal data referred to in paragraph 1, clause 2 of this Article shall mean the name, category and number of the identity document, domicile or residence, address and employment.

Article 34

Records may be kept on entries into and exits from business or official areas.

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 and the reason for entering and exiting business or official areas.

The records referred to in paragraph 1 of this Article shall have the force of public documents if the data are used for the purpose of protecting a child and carrying out police, intelligence and security affairs.

Personal data from the records referred to in paragraph 1 of this Article shall be stored no longer that one year from the day when they were collected, whereupon they shall be erased, unless otherwise provided by the law.

3. Video surveillance

Article 35

The public sector, commercial enterprise, another legal person and entrepreneur may perform video surveillance of the access to official or business areas for the purpose of ensuring the safety of persons and property, controlling entries into and exits from official or business areas or if, due to the nature of the business there is a possible risk to the employees.

The decision on the introduction of video surveillance referred to in paragraph 1 of this Article shall be made by the head of a state authority, public administration body, local self-government and local administration authority or the responsible person in the commercial enterprise or in another legal person, or by the entrepreneur if the introduction of video surveillance is not provided for by the law.

The decision referred to in paragraph 1 of this Article shall be in writing and must include the reasons for introduction of video surveillance.

The video surveillance referred to in paragraph 1 of this Article shall be carried out in a way which does not show recordings of the interior of residential buildings not connected with the entrance to official or business areas, or recordings of entrances to apartments.

Employees working within areas under video surveillance referred to in paragraph 1 of this Article must be informed in writing of video surveillance.

Access to recordings made by the video surveillance system referred to in paragraph 1 of this Article via internal cable television, public cable television, the Internet or other means of electronic communication capable of transmitting such recordings either at the time of their making or afterwards shall be prohibited.

Article 36

The public sector, commercial enterprise, other legal person and entrepreneur may perform video surveillance in official or business areas if so required by the reasons of protection of safety of persons or property or secrecy of data and business secrets, provided that this cannot be achieved in another way.

Video surveillance shall not be allowed in official and business areas outside the workplace, particularly in changing rooms, elevators and sanitary premises and the areas for receiving clients and visitors.

Where the introduction of video surveillance is not provided for by the law, the decision on the introduction of video surveillance referred to in paragraph 1 of this Article shall be made the head of a state authority, public administration body, local self-government and local administration authority or the responsible person in a commercial enterprise or in another legal person, or the entrepreneur.

The persons referred to in paragraph 3 of this Article must, before making a decision on the introduction of video surveillance, obtain an opinion of the representative trade union or of the staff representative.

The employees must be informed in writing of the introduction of video surveillance before video surveillance starts.

The provisions of paragraph 4 of this Article shall not apply to official or business areas belonging to the authorities responsible for the areas of defence, national and public security and protection of secret data.

Article 37

Records shall be kept of 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 contain: the recording of the data subject (image or sound, or image and sound), date and time the recording of entry and exit was made, and where so required, the name of the recorded data subject, his domicile or residence and address, employment, category and number of the identity document, reasons of entry, if personal data entered were collected either in addition to the recording or through the recording made by a video surveillance system.

Personal data from the records referred to in paragraph 1 of this Article shall be stored for no longer than a year from the day they were brought into existence.

Article 38

Video surveillance of entrances and exits as well as of common premises may be performed in apartment buildings.

Video surveillance may be introduced in an apartment building only with the written consent of the assembly of apartment owners.

The consent referred to in paragraph 1 of this Article shall be considered given if members of the assembly of apartment owners who hold over 70% ownership have voted for it.

Video surveillance of entrances to apartments may not be performed.

Article 39

The public sector, commercial enterprise, other legal person and the entrepreneur who performs video surveillance must display a public notification of video surveillance.

The notification referred to in paragraph of this Article must be displayed at a visible place in a way which allows individuals to learn about video surveillance before it begins or at latest at the moment video surveillance begins.

The notification referred to in paragraph 1 of this Article shall contain the following information:

1) the title of the person performing video surveillance;
2) a telephone number to obtain information as to where and for how long the video recordings are to be stored.

The data subject shall be deemed informed of the processing of personal data through video surveillance by the mere fact of the notification referred to in paragraph 1 of this Article being displayed.

Video surveillance system used to perform video surveillance must be protected against access by unauthorised persons.

Article 40

The provisions of Article 35 of this law shall apply where appropriate to video surveillance of public areas, unless otherwise provided by a separate law.

IV TRANSFER OF PERSONAL DATA FROM MONTENEGRO

Article 41

Personal data undergoing processing may be transferred from Montenegro to another country or given to an international organisation, which implements safeguards provided for by this law, with the prior consent of the supervisory authority.

The adequacy of the measures of protection referred to in paragraph 1 of this Article shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to:

1) the nature of the data;
2) the purpose and duration of the proposed processing operation or operations;
3) the country of origin and country of final destination,
4) the rules of law in force in the third country in question and
5) the professional rules and security measures which are complied with in that country.

A transfer of data with the purpose of entrusting specific processing activities within the meaning of Article 16 of this law may take place only with the consent of the supervisory authority, except in the case set out in Article 42 item 6 of this law.

Article 42

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

1) the transfer of personal data is provided for by a separate law or an international treaty binding on Montenegro;
2) the data subject has given his prior consent to the proposed transfer and has been informed of possible consequences of data transfer;
3) the transfer is required for the performance of a contract between a legal or natural person and the personal filing system data controller or the implementation of precontractual obligations;
4) the transfer is required in order to protect the life of the data subject or is in his interest;
5) the transfer is made from a register or records which according to laws or other regulations are available to the public;
6) the data are transferred to the Member States of the European Union and European Economic Area or countries which are included on the European Union list of countries with an adequate level of personal data protection;
7) the transfer is necessary on important public interest grounds, or for the establishment, exercise or defence of legal claims of the data subject;
8) the personal data filing system controller concludes a contract stipulating adequate contractual obligations accepted by the Member States of the European Union, with a personal data processor from the third country, and where
9) the transfer is necessary for the conclusion or performance of a contract between the personal data filing system controller and a legal or natural person concluded in the interest of the data subject.

V RIGHTS OF DATA SUBJECT TO PROTECTION OF PERSONAL DATA

Article 43

The personal data filing system controller must, on written request of the data subject or his legal representative or attorney, if any, notify the data subject no later than 15 days from the day when the request was submitted of the following:

1) whether personal data are undergoing processing;

2) his name, domicile or residence or seat respectively and the processor and recipient of personal data (his name, place of domicile or residence or seat respectively), as well as of the source of data;

3) the purpose and legal grounds for processing of personal data;

4) the right of access to personal data relating to him;

5) the right to rectification of such data;

6) recipient of personal data and

7) the manner of automatic processing of personal data.

The notification referred to in paragraph 1 of this Article may be given in the form of an extract, confirmation or a transcript.

Article 44

The personal data filing system controller must, on written request of the data subject or his legal representative or attorney, if any, and no later than 15 days from the day when the request was submitted:

1) supplement incomplete or alter or erase inaccurate personal data;

2) erase personal data the processing of which does not comply with the law;

3) block the use of inaccurate or incomplete personal data; and

4) block the use of personal data the use of which does not comply with the law,

The personal data filing system controller must notify the data subject or his legal representative or attorney, if any, as well as the recipient of personal data of any supplementing or alteration, erasure or blocking referred to in paragraph 1 of this Article within eight days, unless this proves impossible.

Article 45

The rights of data subjects set out in Articles 43 and 44 of this law may be restricted when such a restriction is required for the purpose of defence, national and public security, detection and prosecution of criminal offenders, safeguarding economic or financial interest or cultural assets of importance for the state, as well for protection of the data subject or of human right and freedoms, to the extent necessary to achieve the purpose for which the restriction was established, in accordance with a separate law.

Article 46

The costs of proceedings referred to in Articles 43 and 44 of this law shall be borne by the personal data filing system controller, unless otherwise provided by the law.

Article 47

Any person who alleges a breach of his rights set forth in this Law may submit a request for protection of rights to the supervisory authority.

The supervisory authority must decide on the request within 60 days from the day of submission of the request.

The procedure and making of a decision with regards to the request referred to in paragraph 1 of this shall be carried out in accordance with the provisions of Articles 66 through 73 of this law.

Until the decision referred to in paragraph 2 of this law is made, the supervisory authority may, at the written request of the person who submitted a request for protection of rights, temporarily ban further processing of personal data, if a breach of the rights established by this law exists or is established as likely.

Administrative dispute proceedings may be initiated against the decision referred to in paragraph 2 of this Article.

Article 48

The data subject shall be entitled to receive compensation from the personal data filing system controller for the damage suffered as result of a breach of rights set forth in this law in accordance with general rules on compensation of damage.

VI AGENCY FOR PERSONAL DATA PROTECTION

Article 49

An Agency for Personal Data Protection (hereinafter referred to as "the Agency") is hereby set up to perform the tasks of the supervisory authority as laid down by this law.

The Agency shall be autonomous and independent in the performance of the tasks falling within its competence.

The Agency shall have legal personality.

Article 50

The Agency shall:

1) perform supervision over the protection of personal data in accordance with this law;
2) decide on requests for protection of rights;
3) deliver opinions with regards to the application of this law;
4) give consent with regards to the establishment of personal data filing systems;
5) deliver an opinion in the case of doubt whether a set of personal data is considered a filing system within the meaning of this law;
6) monitor the application of organisational and technical measures for the protection of personal data and propose improvement of such measures;
7) put forward proposals and offer recommendations for the improvement in the protection of personal data;
8) deliver an opinion as to whether a specific way of personal data processing puts rights and freedoms of individuals at risk;
9) cooperate with authorities responsible for supervising the protection of personal data in other countries;
10) cooperate with competent state authorities in the process of development of regulations relating to protection of personal data;
11) put forward proposals for assessment of constitutionality of laws and constitutionality and lawfulness of other regulations and general acts which govern the issues of personal data processing and
12) perform other tasks in accordance with this law.

Article 51

The Agency shall have a Council of the Agency and a Director.

Article 52

The Council of the Agency shall have a Chairman and two members.

The Chairman and members of the Council of the Agency shall be appointed by the Parliament of Montenegro (hereinafter referred to as "the Parliament"), at a proposal of the competent working body.

The Chairman and members of the Council of the Agency shall be appointed for the period of five years and are eligible for one reappointment.

The Chairman and members of the Council of the Agency shall be accountable to the Parliament.

Article 53

The Chairman and members of the Council of the Agency must meet the following requirements:

1) must be Montenegrin nationals,
2) must have a university degree and
3) must have five years of work experience in the area of human rights and freedoms.

Article 54

The following persons may not be appointed as Chairman and members of the Council of the Agency:

1) a Member of Parliament or a Local Assembly;
2) person appointed by the Government of Montenegro;
3) political party official (president of a party, member of presiding body, their deputy, member of executive or main board and other party officials);
4) persons who have been convicted by a final decision of a criminal offence prosecuted *ex officio*, regardless of the sentence imposed, as well as persons who have been convicted of another criminal offence by a final decision and sentenced to an imprisonment in excess of six months, during the period in which legal consequences of conviction are in force;
5) spouse of the persons referred to in clauses 1, 2 and 3 of this Article or relatives of these persons in the direct line, in the collateral line within the second degree and relatives by affinity.

A candidate for member of the Council of the Agency must submit a written statement to the competent working body referred to in Article 52 paragraph 2 of this law to the effect that there are no impediments for appointment established by this law.

Article 55

The Chairman and members of the Council of the Agency may be dismissed before the expiry of their terms of office in the following cases:

1) on personal request,
2) due to the permanent loss of the working ability to perform the office,
3) if the circumstances referred to in Article 54 of this law arise,
4) if they violate the duty of protecting personal data.

Article 56

The Council of the Agency shall:

1) adopt the rules of the Agency;

2) adopt a Statute and an internal act on working posts, 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) draw up annual and special reports on the situation regarding the protection of personal data;

4) establish an annual workplan and annual report on the work of the Agency;

5) establish a proposal of the financial plan and balance sheet;

6) make decisions on requests for protection of rights and in other cases following supervision;

7) perform other tasks established by the law and the Statute of the Agency.

The rules referred to in paragraph 1 clause 1 of this Article shall be published in the Official Gazette of Montenegro.

Article 57

The Council of the Agency shall decide by the vote of an absolute majority of its members.

Article 58

The Director of the Agency shall be appointed by the Council of the Agency on the basis of a public vacancy notice for the period of 4 years.

A person who does not meet the requirements for member of the Council of the Agency under this law may not be appointed as Director of the Agency.

Article 59

The Director of the Agency shall:

1) act on behalf of and represent the Agency;
2) organise and lead the Agency;
3) execute decisions of the Council of the Agency,
4) propose to the Council of the Agency workplans, reports on the on the situation regarding the protection of personal data,
5) perform other tasks laid down by this law and the Statute of the Agency.

Article 59 a

Remuneration of the Chairman and members of the Council of the Agency shall be determined by the Statute of the Agency.

Article 60

The Agency shall have a technical service.

General labour regulations shall apply to the rights, obligations and responsibilities of the technical service staff.

Article 61

The Agency shall have a statute.

The Statute of the Agency shall include at least the provisions on:

1) the seat and the activities of the Agency,
2) internal organisation of the Agency,
3) the manner of work, decision making and competences of the bodies of the Agency.

Article 62

The Agency shall submit an annual report on the situation regarding the protection of personal data to the Parliament no later than 31st March of the current year for the previous year. The Agency shall submit to the Parliament a special report on the situation regarding the protection of personal data in the following cases:

1) at the request of the Parliament,
2) if the Agency finds there are special reasons to do so.

The report referred to in paragraph 1 of this Article shall include an analysis of the situation regarding the protection of personal data, proceedings brought under this law and measures which have been ordered, as well as information on the level of protection of the rights of data subjects with regard to the processing of personal data.

The reports referred to in paragraphs 1 and 2 of this Article must be made available to the public.

Article 63

The work of the Agency shall be financed from the Budget of Montenegro and other sources, in accordance with the law.

Article 64

The Chairman and members of the Council, Director of the Agency and Agency staff must keep secrecy of all data they become privy to in the performance of their duties, in accordance with the laws governing secrecy of data.

The duty referred to in paragraph 1 of this Article shall continue even after the tenure of the Director and employment of staff of the Agency has ended.

VII SUPERVISION

Article 65

The Agency shall perform supervision in accordance with this law through its staff who are authorised to perform the tasks of supervision in accordance with the act on working posts (hereinafter referred to as "the controller").

In order to become a controller, a person must, in addition to the general requirements established by the law, meet the following requirements:

1) must have a university degree;
2) must have five years of work experience;
3) must have passed the civil service exam;
4) must not have a conviction for a criminal offence which makes him unsuitable for employment in a state authority and
5) must not be subject to criminal proceedings.

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

Any person may request initiating of the procedure of supervision.

Article 66

The controller shall have the right of access to personal data contained in personal data filing systems, regardless of whether the records of such filing systems are kept in the Register, as well as the right of access to files and other documents relating to the processing of personal data and to electronic means of personal data processing.

The controller shall have the right of access to the personal data referred to paragraph 1 regardless of the level of data secrecy.

Article 67

The personal data filing system controller or the processor of personal data must provide access to the filing systems, files and other documents, as well as to the means of electronic processing and must supply, on the request of the controller the required files and documents.

Article 68

Minutes of the supervision performed under Article 65 of this law shall be prepared within 15 days from the day when the supervision was performed and issued to the personal data filing system controller.

When supervision is performed on the basis of a request for protection of rights referred to in Article 47 of this Law, the controller must conduct the procedure and prepare minutes immediately or within eight days from day when the request was submitted at latest. The minutes shall be issued to the claimant and the personal data filing system controller.

The personal data filing system controller and the claimant may make an objection to the minutes referred to in paragraphs 1 and 2 of this Article with the Agency within eight days of the receipt of the minutes.

Article 69

Where the Agency establishes that an objection made by the personal data filing system controller to the minutes which make a note of unlawful activities and irregularities in the processing of personal data is unfounded, it shall impose the measures set out in Article 71 of this Law.

In the case referred to in paragraph 1 of this Article, the Agency shall submit a request for bringing of misdemeanour proceedings.

Article 70

Where on the basis of minutes on supervision performed the Agency establishes there are no unlawful activities or irregularities in the processing of personal data as alleged in a request for protection of rights or in an objection to the minutes, it shall reject the request by way of a decision.

When the Agency, acting on an objection of a claimant to the minutes which note there are no unlawful activities or irregularities in the processing of personal data relating to him, establishes that the objection is founded, it shall impose the measures referred to in Article 71 of this law on the personal data filing system controller.

Article 71

In the performance of supervision the Agency shall have the authority to:

1) order that irregularities in the processing of personal data be eliminated;
2) impose a temporary ban on unlawful processing of personal data;
3) order the erasure of personal data collected without legal grounds;
4) impose a ban on transfer of personal data from Montenegro or disclosure of data to recipients of personal data in contravention to this law;
5) impose a ban on entrusting of personal data processing where the processor of personal data does not meet the requirements with regards to the protection of personal data or where entrusting of such tasks was carried out in contravention to this law.

Article 72

Administrative dispute proceedings may be brought against the decision of the Agency.

Article 73

The regulations governing the inspection supervision shall apply to the procedure and manner of performance of supervision, duties and authority of the controller and other issues of importance for performance of supervision, unless otherwise provided by this law.

VIII PENAL PROVISIONS

Article 74

A fine ranging from tenfold to three hundred fold amount of the minimum wage in Montenegro shall be imposed on an authority, legal person or an entrepreneur who:

1) carries out processing of personal data without a prior consent of the data subject (Article 10 paragraph 1);
2) fails to erase personal data from a personal data filing system within 30 days from the day the request was made (Article 11 paragraph 2);
3) processes special categories of personal data in contravention to the provision of Article 13 of this law;
4) processes personal data relating to criminal and misdemeanour proceedings in contravention to Article 14 of this law;
5) processes personal data for commercial purposes and by resorting to other forms of publicizing without the consent of the data subject (Article 15);
6) entrusts the tasks of personal data processing falling within his scope of work to a processor of personal data who is not registered for carrying out the processing of personal data or does not meet the requirements for implementation of technical, personnel and organisational measures for protection of personal data (Article 16 paragraph 3);
7) does not keep records of personal data which have been made available to recipients of personal data, the purpose for which they have been made available for use and legal grounds for the use of personal data (Article 19);
8) fails to erase personal data the processing of which in not in compliance with Article 23, paragraph 1 of this law;

9) does not provide technical, personnel and organisation measures of protection of personal data for the purpose of protection from loss, destruction, unauthorised access, alteration, publicizing and abuse (Article 24 paragraph 1);
10) establishes a personal data filing system prior to obtaining the consent from the Agency or prior to the expiry of the 30-day time limit from the day of the submission of the request (Article 27 paragraph 1);
11) does not keep records on personal data filing systems or fails to update such records (Article 25);
12) performs supervision in a way which shows recordings of interiors of apartment buildings which have no bearing on entrances to residential and business areas or records entrances to apartments (Article 35);
13) fails to inform in writing the employees working within areas under video surveillance on the performance of video surveillance (Article 35 paragraph 5); ?
14) performs video surveillance in business or official areas outside the working post (Article 36 paragraph 2);
15) fails to inform the employees in writing of the introduction of video surveillance before the performance of video surveillance begins (Article 36 paragraph 5);
16) records entrances to apartments via a video surveillance system (Article 38 paragraph 4);
17) fails to display a public notification of video surveillance at a visible place (Article 39 paragraphs 1 and 2);
18) fails to include all the required information in the public notification of video surveillance (Article 39 paragraph 3);
19) fails to protect the video surveillance system used to perform video surveillance from access by unauthorised persons (Article 39 paragraph 5);
20) fails to submit a notification to the data subject within 15 days from the day when the request was submitted (Article 43);
21) fails to supplement, alter, erase or block the use of personal data within 15 from the day when the request was submitted (Article 44 paragraph 1),
22) fails to inform the data subject, or his legal representative or attorney, if any, as well as the recipient of personal data of the supplementing, alteration, erasure or blocking of the use of personal data (Article 44 paragraph 2),
23) as a recipient or processor fails to act on an order of or a ban imposed by the Agency (Article 71).

A responsible person in a legal person, responsible person in a state or other authority and a natural person tasked with acting as personal data filing system controller, processor or recipient of personal data shall be imposed a fine ranging from one to twenty-fold amount of minimum wage in Montenegro for the misdemeanour referred to paragraph 1 of this Article.

IX TRANSITORY AND FINAL PROVISIONS

Article 75

The Chairman and members of the Council of the Agency shall be appointed within six months from the day on which this law enters into force.

The Director of the Agency shall be appointed within three months from the day of the appointment of the Council of the Agency.

Article 76

Bylaws for implementation of this law shall be adopted within three months from the day of the appointment of the Council of the Agency.

Article 77

The personal data filing systems set up until the entry into force of this law shall be brought into compliance with this law within nine months from the day on which this law enters into force.

Personal data filing system controllers shall set up the records referred in Article 26 of this law within 15 months from the day on which this law enters into force.

The public sector, commercial enterprise, other legal person and the entrepreneur shall bring records on entries and exits from premises and performance of video surveillance into compliance with the provisions of this law within 18 months from the day on which this law enters into force.

Article 78

The Law on the Protection of Personal Data (Official Gazette of Federal Republic of Yugoslavia 24/98) shall be repealed as of the day when this law becomes applicable.

Article 79

This law shall enter into force on the eighth day of its publication in the Official Gazette of Montenegro and shall be applied after the expiry of a period of six months from the day of its entry into force.