# LAW
# ON THE PROTECTION OF PERSONAL DATA

**"Official Gazette of Bosnia and Herzegovina", 49/06**

Pursuant to Article IV.4 a. of the Constitution of Bosnia and Herzegovina, the Parliamentary Assembly of Bosnia and Herzegovina, at the 79th session of the House of Representatives, held on 17 May 2006 and at the 58th session of the House of Peoples, held on 23 May 2005, adopted the

# LAW
# ON THE PROTECTION OF PERSONAL DATA

## Chapter I
## GENERAL PROVISIONS

### *Article 1*
### *Purpose of the Law*

(1) The purpose of this Law is to secure in the territory of Bosnia and Herzegovina for every individual, regardless of his/her nationality or residence, respect for human rights and fundamental freedoms, and in particular the right to privacy with regard to the processing of personal data relating to him/her.

(2) This Law shall establish the Agency for Protection of Personal Data in BiH (hereinafter referred to as: the Agency), define its responsiblity, organization and governance, as well as other matters of relevance for its operation and lawful functioning.

### *Article 2*
### *Scope of the Law*

(1) This Law shall apply to personal data that are processed by all public authorities, natural and legal persons, unless otherwise stipulated by other legislation.

(2) This Law shall not apply to personal data being processed by natural persons exclusively for personal needs.

(3) This Law shall not apply to accidental personal data collection, unless these data are subject to further processing.

### *Article 3*
### *Definitions*

Individual terms used in this Law shall have the following meaning:

**'personal data'** shall be understood to mean any information relating to an identified or identifiable natural person;
**'data subject'** shall mean a natural person whose identity can be determined or identified, directly or indirectly, in particular by reference to a personal identification

number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity;

‘**special categories of data’** shall be understood to mean any personal data revealing:

a) racial origin, nationality, national or ethnic origin, political opinion or party affiliation, trade union affiliation, religious, philosophical or other belief, health, genetic code, sexual life;

b) criminal conviction, and

c) biometric data .

**“personal data filling system”** shall be understood to mean any systemic set of personal data accessible by specific criteria, either centralized, decentralized or classified on functional or geographic basis, or arranged in accordance with specific criteria relating to the person, allowing for an easy access to personal data in the file;

**“processing of personal data'** shall be understood to mean any operation or set of operations performed upon data, whether automatic or not, in particular collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available data access, alignment or combination, blocking, erasure or destruction;

**“anonymous data”** shall be understood to mean data that cannot be related to a data subject in terms of his/her identification, in their original form or following processing thereof;

"**data access**" shall be understood to mean any operation that enables a data user to view personal data without the right to use it thereafter for other purposes;

**“controller”** shall be understood to mean any public authority, natural or legal person, agency or any other body, which, independently or together with another party, manages, processes and determines the purpose and the manner of personal data processing on the basis of laws or regulations;

**“processor”** shall be understood to mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

**“user”** shall be understood to mean a natural or legal person, public authority, agency, or other authority to which/whom access to personal data can be allowed or the personal data may be disclosed.

**"consent of a data subject"** shall be understood to mean any freely given specific and informed indication of a data subject's wish by which the data subject signifies his consent to processing of his/her personal data.

## Chapter II.

## BASIC PRINCIPLES OF LAWFUL PERSONAL DATA PROCESSING

### *Article 4*
### *Principles of Personal Data Processing*

The controller shall be required to:

a) process personal data fairly and lawfully
b) process personal data collected for special, explicit and lawful purposes in no manner contrary to the specified purpose;
c) process personal data only to the extent and scope necessary for the fulfilment of the specified purpose;
d) process only authentic and accurate personal data, and update such data when necessary;
e) erase or correct personal data which are incorrect and incomplete, given the purpose for which the data are collected or further processed;
f) process personal data only within the period of time necessary for the fulfilment of the purpose of their processing.
g) keep personal data in the format that allows identification of the data subject for not longer than required for the purpose for which the data are collected or further processed;
h) ensure that personal data that were obtained for various purposes are not combined or merged.

### *Article 5*
### *Consent by A Data Subject*

(1) The controller may process personal data only with the consent of a data subject.

(2) Such consent shall have to be granted in writing, signed by the data subject, clearly stating data for which the consent has been granted, and must contain the name of the controller, the purpose and period of time for which the consent has been granted.

(3) The consent may be withdrawn in any time, unless otherwise explicitly agreed upon by the data subject and the controller.

(4) The controller shall have to prove at the request of the competent authority, at any time, that there is the consent for the period of personal data processing.

(5) The controller shall be required to keep the consent during processing of personal data for the processing of which the consent has been granted.

### *Article 6*
### *The Right to Process Personal Data Without the Data Subject's Consent*

(1) The controller may process data without the consent of a data subject if one of the following conditions has been fulfilled:

a) if he is carrying out personal data processing as provided by law or which is required to comply with the duties specified by law;

b) if it is necessary for the data subject to enter into negotiations on a contractual relationship or to fulfil the obligations agreed upon with the controller;

c) if it is necessary for the protection of interests of the data subject when the consent of the data subject has to be obtained without undue delay or the processing has to be terminated and collected data destroyed;

d) if the personal data processing is required in order to complete the task carried out in the public interest;

e) if it is necessary for the protection of rights and interests exercised by the controller or user, and if such processing is not in contradiction with the right of the data subject to protection of personal privacy and personal life;

f) if it is necessary for carrying out legitimate activities of political parties, political movements, civic associations, trade union organisations, religious communities.

### *Article 7*
### *Data Authenticity*

(1) The controller shall be required to check whether the personal data are authentic and accurate.

(2) If the incomplete and inaccurate data cannot be corrected or amended, and so taking into account the purpose for which they are collected or further processed, the controller must destroy them without delay.

### *Article 8*
### *Consolidation of Records*

(1) The controller who is processing personal data on the basis of a special law shall be required to respect the right to protection of privacy and personal life of the data subject.

(2) Personal data shall not be transferred and files and records shall not be consolidated (combined, merged or otherwise joined) if conditions specified in Paragraph 1 herein have not been fulfilled.

(3) The consolidation of records and files under Paragraph 2 of this Article may be performed only if the data processing is carried out by the same controller.

### *Article 9*
### *Processing of Special Categories of Personal Data*

(1) Processing of special categories of personal data shall be prohibited.

(2) Notwithstanding the provision of Paragraph 1 hereof, processing of the special categories of personal data shall be allowed:

a. if a data subject has explicitly granted the consent;

b. if the data processing is necessary to protect the life and health, property and other vital interests of the data subject or some other person for whom such consent cannot be obtained, in particular, when physically, mentally or legally incapacitated person is concerned, or if the person concerned is missing or for other similar reasons;

c. if the data processing is necessary for the fulfilment of an obligation or exercise of special rights of the controller arising from the labour legislation domain inasmuch as the controller is authorized by law;

d. if the data processing is carried out to serve the needs of preventive medicine, medicinal diagnostics, medical service providing and management, provided that such data are processed by a professional medical officer obligated to keep the professional secret by operation of law or code of conduct of the responsible authority, or other persons who are also obligated to keep the secret.

e. if the data processing is carried out within the scope of legitimate activities of an institution, foundation, association or any other non-profit organization with political, philosophical, religious or trade union objectives, provided that the data processing shall solely relate to the members of the bodies or persons who have regular contacts with them in reference to their objectives, and the data shall not be disclosed to a third party without the consent of the data subject;

f. if the processing is carried out of the data that have been clearly made public by the data subject or it is required in order to initiate, enforce or make defence against legal claims;

g. if it is of special public interest or in other cases stipulated by law. In such cases the law shall have to contain specific provisions on appropriate protection mechanisms.

### *Article 10*
### *Automated Processing of the Special Category of Personal Data*

Special category of personal data may not be automatically processed unless the appropriate protection has been provided for by law.

### *Article 11*
### *Data Security*

(1) The data controller and, within the scope of its competences, the data processor shall take care of data security and shall take all technical and organisational measures and develop rules of procedure required for the enforcement of this Law and other regulations concerning data protection and secrecy.

(2) The controller and the processor shall be required to take measures against unauthorised or accidental access to personal data, their alteration, destruction or loss, unauthorised transfer, other forms of illegal data processing, as well as measures against misuse of personal data. This obligation shall remain valid even after terminating personal data processing.

(3) Any public authority, in the capacity of the controller, shall be required to issue, within the scope of legal competencies, a regulation aimed at enforcing this Law.

(4) The controller and, within the scope of its competencies, the processor shall be required to develop the data security plan, which shall specify technical and organizational measures for security of personal data.

(5) The Council of Ministers of Bosnia and Herzegovina (hereinafter referred to as: the Council of Ministers) shall, upon obtaining the prior opinion from the Agency, prescribe the methodology of safekeeping and special measures of technical protection.

### *Article 12*
### *Data Processing by a Processor*

(1) If law does not exclude data processing by a processor, the controller may conclude a contract with the processor on personal data processing. The contract shall have to be concluded in writing.

(2) The contract shall specify the scope, purpose and the period of time for which the contract has been concluded, as well as adequate guarantees of the processor in terms of technical and organizational protection of personal data.

(3) Data processing by the processor shall have to be regulated by a contract, which shall bound the processor towards the controller, in particular that the processor shall act only on the basis of the controller's instructions in accordance with the provisions of this Law.

(4) The processor shall be responsible for personal data processing according to the data controller's instructions. While exercising his/her duties, the processor shall not transfer its responsibility to other processors, unless explicitly instructed by the data controller to do so.

***Article 13***
***Personal Data Filing System***

]

The personal data filing system controller shall establish and maintain the records for each personal data filing system, which shall contain the basic information on the system, and in particular:

a) title of personal data filing system;
b) first and last name and address of data controller and data processor, the actual place of data processing (including technical processing), as well as any activity of data processor related to the processing of personal data;
c) purpose of the data processing;
d) legal basis for the processing;
e) type of data to be processed;
f) categories of data subjects;
g) data source and method of collection;
h) type of transferred data, the recipients of such data, and the legal basis for transfer;
i) deadlines for erasure of certain types of data;
j) an indication whether the data have been transferred into or abroad from Bosnia and Herzegovina with the indication of the country or international organization and foreign user of such personal data and the purpose for this transfer to or abroad from BiH as prescribed by an international agreement, law or other regulation, or a written consent of the person to whom this data refer;
k) indication of measures taken towards protecting the personal data.

**Article 14**
***Central Registry***

(1) The personal data filing system controller shall provide the Agency with the data referred to in Article 13. The agency shall consolidate such data into the Central Registry.

(2) Prior to the establishment of a personal data filing system, the controllers of personal data filing systems shall be under the obligation to submit to the Agency the request for planned establishment of personal data filing system along with the data referred to in Article 13 prior to initiating any processing activity.

(3) The Agency shall examine the data processing operations following the receipt of the request for personal data processing from the data controller. These data processing operations may commence only after the Agency approves the processing, or upon the expiration of two (2) months following the day the request has been received by Agency.

(4) The obligation to submit a prior notification shall not apply to the establishment of personal data filing system in cases where law identifies the processing purpose, data or data categories to be processed, the category of persons affected by the data, users or categories of users to whom/which such data shall be disclosed and the time within which the data shall be maintained.

(5) In the cases referred to in Paragraph (3) of this Article, personal data filing system controllers shall be under the obligation to submit the data on the creation of personal data filing systems, as well as any data amendments concerning personal data filing systems to the Agency, not later than within fourteen (14) days following the establishment or update of such data.

(6) The public shall have access to the data from the Central Registry.

(7) The Agency shall publish the records from the Central Registry.

### *Article 15*
### *Record Keeping*

The method of keeping the records referred to in Article 13 of this Law and the recording format, as well as the exemptions from the obligation to report certain filing systems under Article 14 shall be prescribed by the Council of Ministers, with the prior opinion obtained from the Agency.

### *Article 16*
### *Confidentiality Requirement*

(1) Employees in the office of the controller or processor and other persons who are engaged in the processing of personal data on the basis of a contract with the

controller or processor, may process personal data only under the conditions and in the scope as specified by the controller or the processor.

(2) Employees in the office of the controller or processor, other natural persons who process personal data on the basis of a contract concluded with the controller or processor and other persons who, within the scope of exercise of rights and duties stipulated by law, come into contact with personal data in the premises of the controller or processor, shall be required to maintain confidentiality of personal data and abide by the specified security arrangement.

(3) Personal data processed by the controller or processor shall be official secret for the employees.

(4) The obligation to maintain the confidentiality of data shall remain in force after termination of employment and/or the specific task.

(5) Exemption from the obligation to maintain confidentiality of data may only be prescribed by law.

### *Article 17*
### *Providing Personal Data to Users*

(1) The data controller may not provide personal data to any users prior to notifying thereof the data subject. If the data subject does not consent to providing of the personal data, the data shall not be disclosed to the third party unless such disclosure is in the public interest.

(2) The personal data controller is authorized to provide personal data to other users based on the user's written request if this is necessary for carrying out tasks within the competence specified by law or for exercising of lawful interests of the user.

(3) The written request shall indicate the purpose and legal grounds for the personal data use, and the type of personal data requested.

(4) It is prohibited to provide personal data to other users who have not been authorized to process or use them pursuant to the provisions of Article 5 and Article 6 of this Law, and if the purpose for the use of such personal data requested is contrary to provisions of Article 4 of this Law.

(5) The personal data controller shall keep separate records on the personal data provided for use and the purpose for which this data have been provided.

(6) The data subject may not exercise the right to blocking or destroying the personal data if the controller has the obligation to process data pursuant to a special law or if that would violate the rights of third persons.

### *Article 18*
### *Data Transfer Abroad*

(1) Personal data shall not be transferred from Bosnia and Herzegovina to a controller or processor abroad regardless of data medium or the manner of transfer unless the requirements specified in Article 4 hereof have not been fulfilled in the receiving country and provided that that the foreign controller shall comply with equal data protection principles for all data.

(2) Exceptionally, the personal data may be transferred abroad if the data subject has consented to the transfer, where it is required for the purpose of fulfilling the contract or legal claim and when it is required for the protection of public interest.

### *Article 19*
### *Data Processing in Mass Media*

(1) Data processing for journalistic purposes, the purposes of artistic or literary expression, shall be carried out in accordance with a separate regulation and codes of conduct

(2) Provisions of this Law shall not apply to data processing for the purposes referred to in Paragraph (1) of this Article, except for the provisions concerning the data security and confidentiality as well as liability for damages.

### *Article 20*
### *Data Processing for Statistical, Scientific and Archival Purposes*

(1) Upon the expiry of the period necessary for the fulfilment of the purposes for which the data were collected, such data may be processed only for statistical, scientific and archival purposes. The data collected and stored for such purposes shall not be used for other purposes.

(2) Personal data may be processed for statistical, archival or scientific purposes without the consent of the data subject. When processed for the aforesaid purposes, personal data must be made anonymous.

(3) When personal data are processed for the aforesaid purposes, the right to protect privacy and personal life of the data subject shall be required to complied with.

### *Article 21*
### *Disclosing Personal Data to Research Institutes*

An organisation or a person performing personal data processing for scientific research purposes may disclose information obtained from personal data, if the data subject gives his/her written consent to this end.

## Chapter III

## RIGHTS OF A DATA SUBJECT

### *Article 22*
### *Notification on Data Collection*

Before collecting any personal data, the controller shall notify a data subject, unless the data subject has already been informed, on:

a) the purpose of processing,
b) controller, receiving authority or third party whom the data will be accessible,
c) if forwarding of data for processing is legal obligation,
d) consequences in the case that the data subject refuses to proceed so,
e) the cases in which the data subject has right to refuse to provide personal data,
f) if the personal data collection is voluntary,
g) the right to access and the right to correct data referring to him/her.

### *Article 23*
### *Personal Data Source*

If the controller failed to collect personal data from a data subject, he/she shall be required to notify the data subject without delay about the identity of the third party that provided the controller with the personal data.

### *Article 24*
### *The Right to Personal Data Access*

(1) The data controller shall notify the data subject on the progress of processing of his/her personal data performed either by the data controller or by a data processor, the purpose of the data processing, legal grounds for and duration of processing, if the data were collected from the data subject or a third party, the right to access personal data, as well as who has received or will receive data and for what purpose.

(2) The controller shall not be obliged to provide information on the processing of personal data in the following cases:

a) If he is processing personal data exclusively for statistical, scientific-research or archival purposes;
b) If the obligation of the controller to process personal data is imposed thereon by law, or the data are necessary to exercise the rights and obligations stipulated by law;
c) Where law stipulates that the controller does not have the obligation to provide such information;

d) If he processes only such personal data that have already been published;

e) If he processes personal data with the consent of the data subject pursuant to Article 5 of this Law.

**Article 25**
***Information Provision Method***

(1) Unless stipulated otherwise by law, on the basis of a written request of the data subject, the controller shall be obliged to provide, once per calendar year, the data subject with information on personal data processed in relation to the data subject and to do so free of charge.

(2) Otherwise, such information shall be provided at any time for a reasonable fee not exceeding the costs required for the provision of information.

(3) The data controller shall furnish such information in writing, in an intelligible form, within 30 days from the submission of a request.

**Article 26**
***Rejection of Request***

(1) The data controller may not refuse to provide the information to the data subject, unless otherwise stipulated by the law in specific cases.

(2) The data controller shall state a reason for rejecting the information request.

(3) The data controller shall submit an annual report to the Agency on rejected requests of data subjects.

**Article 27**
***Corrigenda and Deletion of Data***

The data subject and any other person to whom data are transferred for processing purposes shall be informed of any corrigenda and deletion of the data. Such information may be dispensed with, in view of the purpose of processing, if the legitimate interest of data subject is not infringed thereby.

**Article 28**
***Exceptions in Terms of Rights***

(1) The data controller shall not be obliged to provide information on processing of personal data or to enable access to personal data if that action could cause significant damage to legitimate interests of the following categories in Bosnia and Herzegovina:

a) state security

b) defence

c) public security

d) prevention, investigation, detection of crimes and prosecution of perpetrators as well as violations of ethical regulations of the profession

e) economic and financial interests, including monetary, budgetary and tax issues

f) inspection and duties related to control

g) protection of data subjects or rights and freedoms of other people.

(2) These restrictions shall be allowed only to the extent required in a democratic society for any of the aforesaid purposes.

**Article 29**
***Issuing Decisions Based on Automatic Data Processing***

(1) The controller shall not issue a decision producing legal effects in regard of the data subject or a decision which may considerably affect the data subject while being aimed at evaluating certain personal characteristic of the data subject, solely on the basis of automatic data processing.

(2) Notwithstanding the provision of Paragraph 1 hereof, the decision issued solely on the basis of automated data processing shall generate legal effects for the data subject in the following cases:

a) in a procedure of entry into a contract or implementation of the contract, provided that the request of the data subject is fulfilled or that there are appropriate protection measures of his lawful interests such as a procedure that allows him/her to protect his/her position; or

b) if the controller is authorised by a law, which also defines protection measures relevant to lawful interests of the data subject, to issue such a decision.

***Article 30***
***Filing Complaints***

(1) When the data subject finds or suspects that the controller or processor breached the data subject's right, or that there is a direct risk of breach of right, the data subject may file a complaint with the Agency for the purposes of protecting his/her rights and thereby request the following:

a) That the controller or processor refrain from such activities and remedy the factual situation caused by such activities;

b) That the controller or processor carry out a correction or supplementation of personal data so as to make them authentic and accurate;

c) That the personal data be blocked or liquidated.

(2) The Agency shall issue a decision on the data subject's request referred to in Paragraph 1 of this Article, which shall be submitted to the complainant and the controller.

(3) No appeal shall be allowed against Agency's decision, but it is possible to initiate an administrative dispute proceedings before the Court of Bosnia and Herzegovina.

(4)In deliberating the complaints, the Agency shall be required to comply with the Law on Administrative Procedure.

***Article 31***
***Release from Responsibility***

(1) The Agency my release the controller from responsibility if it proves that the controller could not prevent the breach of data subject's rights caused by the personal data processor.

(2) Nevertheless, the data subject may demand from the controller or the processor to suspend the irregularities, remedy an illegal state of affairs, make a corrigenda, supplementation, blockage, or to destroy the personal data.

***Article 32***
***Liability for Damage***

(1) The data controller shall be obliged to compensate for physical and consequential damage to the data subject if it was inflicted to him as a result of violation of the right to privacy.

(2) In compensation disputes, data subject shall file a complaint with the competent court with territorial jurisdiction over his/her permanent or temporary residence, or with the competent court with territorial jurisdiction of the controller's seat.

(3) The competent court shall establish the compensation for physical damage, unless the parties reach an amicable settlement on the compensation before the court.

(4) Consequential damage shall be compensated by means of public apology and payment of a just compensation.

(5) The data controller shall be liable if the damage to a data subject's rights foreseen by this law was caused also by the data processor.

### *Article 33*
### *Release from Liability for Damage*

(1) The data controller may be exempted from liability for damage, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

(2) No compensation shall be paid for the damage caused by the injured person's intentional or seriously negligent conduct.

## CHAPTER IV.

## BODY IN CHARGE OF PROTECTION OF DATA

### *Article 34*
### *Scope of Regulation*

For all organizational and management issues and other issues relevant for the functioning of Agency as an administrative organization, such as enactment of Rulebook on Internal Organization and other by-law regulations, administrative supervision, relations between the institutions of BiH, and the Agency's relation to legal and natural persons, to the extent not prescribed by this Law, the Law of BiH on Ministries and Other Administrative Bodies and the Law of BiH on Administration shall apply.

### *Article 35*
### *Definition of the Agency*

The Agency is an independent administrative organization established for the purpose of ensuring the protection of personal data and is headed by its Director.

### *Article 36*
### *Financing*

The funds required for operation of the Agency shall be provided from the Budget of the Institutions of Bosnia and Herzegovina and International Obligations of Bosnia and Herzegovina.

### *Article 37*
### *Establishment of Agency*

(1) The seat of the Agency is in Sarajevo.

(2) The Agency may have its departments and other organizational units, which shall be established by the Book of Rules on Internal Organization.

### *Article 38*
### *Employment Relations in the Agency*

(1) The Agency's staff shall be civil servants and employees (administrative and technical staff).

(2) The employment relations of the civil servants working in the Agency shall be regulated by the Law on Civil Service in the Institutions of Bosnia and Herzegovina.

(3) The employment relations of the employees shall be regulated by the Labour Law for Institutions of Bosnia and Herzegovina.

(4) Positions of the civil servants and other employees shall be regulated by the Rulebook on Internal Organisation.

### *Article 39*
### *National Representation*

The structure of civil servants and other employees within the Agency shall generally reflect the national structure of the population of BiH in accordance with the 1991 census.

### *Article 40*
### *Competencies of the Agency*

(1) Tasks falling under Agency's competence are:

a) To supervise the implementation of this Law and other laws on personal data processing;

b) To act on data subject's complaints;

c) To submit to the Parliamentary Assembly of Bosnia and Herzegovina annual reports on personal data protection;

d) To follow the personal data protection requirements by giving proposals as to enacting or amending legislation governing the data processing, give opinions on the proposed laws and take care of fulfilment of the criteria relevant to data protection originating from international treaties that are binding for Bosnia and Herzegovina.

(2) The Agency shall have powers to:

a) Perform supervision, through inspection, over fulfilment of obligations stipulated by this law;
b) Keep the Central Registry;
c) Accept incentives and complaints of citizens concerning breaches of this Law;
d) Adopt implementing regulations, guidelines or other legal documents in line with the Law;
e) Order blocking, erasing or destroying of data, temporarily or permanent ban of processing, issue warning or reprimand to the controller;
f) File a request for filing the misdemeanour proceedings pursuant to this Law;
g) Provide advice and opinions in the area of personal data protection;
h) Co-operate with similar authorities in other countries;
i) Exercise other duties as foreseen by law;
j) Supervise the transfer of the personal data out from Bosnia and Herzegovina.

***Article 41***
***Control Carried Out by the Agency***

(1) When the Agency observes an unlawful processing of data, it shall require the controller to discontinue the processing as well as order different measures. The controller shall take the necessary measures without any delay and inform the Agency in writing within 15 days thereof.

(2) In the exercise of its functions the Agency may request from a controller or processor to furnish the Agency with information on any matter, and may inspect any documents and records likely to bear personal data.

(3) The Agency is entitled to enter any premises where data are being processed. The property and premises of non-statutory data controllers may only be entered and inspected during business hours.

(4) State and official secrets shall not prevent the Agency from exercising its rights stated in this Article, but the confidentiality provisions shall also be binding for the Agency.

(5) Upon its request, all authorities shall be obliged to support the Agency in carrying out its duties.

**Article 42**
***Management – Director***

(1) The Agency shall be managed by the Director (hereinafter: Director).

(2) The Director shall be responsible for his/her work and the work of the Agency to the Council of Ministers.

***Article 43***
***Appointment of the Director***

(1) The Director shall be appointed by the Council of Ministers in accordance with the Law on Ministerial and Government Appointments of Bosnia and Herzegovina.

(2) The Director shall be appointed for a renewable term of office of four years.

***Article 44***
***Special Requirements for Appointment of the Director***

Apart from conditions defined by the Law on Ministerial and Government Appointments, the candidate applying for the position of the Director shall meet the following criteria:

a) Bachelor of Law degree;
b) Five years working experience on the tasks of management in administration;
c) Proven experience in the field of human rights observance;
d) Recognized high moral standing.

***Article 45***
***Conditions for Dismissal of the Director***

The Council of Ministers may dismiss the director before the expiration of his/her term of office:

a) At his/her own request;
b) If he/she is unable to perform his/her duties;
c) If the illegal operation of the Agency is discovered;
d) If his/her disciplinary responsibility is ascertained by a final decision;
e) If he/she has been pronounced a legally valid sentence for a criminal act.

***Article 46***
***Duties and Responsibilities of the Director***

(1) The Director shall:

a) Represent the Agency;

b) Make the annual work plan in accordance with the guidelines of the Chair of the Council of Ministers, as well as the annual budget of the Agency, and propose them to the Council of Ministers for adoption;

c) Manage and direct the tasks from Agency's competence;

d) Propose to a competent body initiation of negotiations regarding the making of international agreements on cooperation regarding the issues of personal data protection;

e) Make continuous analyses for the rational distribution of employees and of technical resources.

(2) Apart for duties and responsibilities referred to in Paragraph (1) of this Article, the Director also does other tasks, such as:

a) Proposing the Rulebook on Internal Organisation to the Council of Ministers, including the total number of employees and criteria for staffing, other rulebooks and regulations stipulated by law, in accordance with the Law on Ministerial and Government Appointments of Bosnia and Herzegovina;

b) Appointing the heads of Agency's organizational units;

c) Assigning tasks to deputy directors in accordance with law;

d) Deciding on rights and duties of the civil servants' and other employees' employment in accordance with applicable legislation from this field;

e) Procurement of equipment and other material resources for the Agency's needs;

f) Submitting the annual progress report to the Council of Ministers, and as required or at a minister's request, also the submitting special reports;

g) Forwarding reports to the Parliamentary Assembly of Bosnia and Herzegovina and Council of Ministers;

h) Carrying out other tasks prescribed by law.

(3) The Director shall be responsible for the lawful operation of the Agency and lawful expenditure of funds allocated to the Agency from the Budget of the Institutions of Bosnia and Herzegovina and International Obligations of Bosnia and Herzegovina.

### *Article 47*
### *Control of Agency's Activities*

The Parliamentary Assembly of Bosnia and Herzegovina may, as required, request carrying out the control of Agency's operation.

## CHAPTER V.

## PENALTY PROVISIONS

### Article 48

(1) The controller shall be fined in the amount ranging between KM 50,000 and 100,000 for violation if:

a) Illegally processes a special category of personal data (Article 9);

b) Transfers personal data abroad if in the data receiving state the conditions specified in Article 5 of this Law have not been fulfilled and provided that the foreign controller does not comply with equal data protection principles for all data (Article 18);

(2) The controller, as a responsible person, shall be fined for violation referred to in Paragraph 1 of this Article in the amount ranging between KM 1,000 and 15,000.

(3) The controller, as an employee, shall be fined for violation referred to in Paragraph 1 of this Article in the amount ranging between KM 500 and 10,000.

### Article 49

(1) The controller shall be fined violation in the amount ranging between KM 10,000 and 100,000 if the controller:

a) Processes personal data contrary to Article 4 of this Law;

b) Processes personal data without the data subject's consent (Article 5, Paragraph 1);

c) Processes personal data without the data subject's consent, whilst none of conditions referred to in Article 6 is fulfilled;

d) Fails to check whether the personal data that he is processing are authentic and correct (Article 7, Paragraph 1);

e) Fails to destroy inaccurate and incomplete data without delay (Article 7, Paragraph 2);

f) Processes personal data on the basis of a special law but fails to respect the right to protection of privacy and personal life of data subject (Article 8, Paragraph 1);

g) Transfers personal data, that is, consolidates files and records without fulfilling specified conditions (Article 8, Paragraph 2);

h) Automatically processes the special category of personal data without ensuring protection provided for by law (Article 10);

i) Does not take all necessary measures and procedures against unauthorised or accidental access to personal data, their alteration, destruction or loss, unauthorised transfer, other forms of illegal data processing, as well as measures against misuse of personal data (Article 11, Paragraph 2);

j) Fails to develop the data security plan (Article 11, Paragraph 4);

k) Entrusts the processing of personal data to a processor without concluding a contract with the processor on that matter (Article 12, Paragraph 1);

l) The data processor if transferring the responsibility to other processor without being explicitly instructed by the data controller to do so (Article 12, Paragraph (4));

m) Illegally provides personal data to a user (Article 17);

n) Uses for other purposes data collected and stored for statistical, archival and scientific purposes (Article 20, Paragraph 1);

o) Publishes an information acquired in the processing of personal data for statistical, archival and scientific purposes without consent of a data subject (Article 21);

p) Fails to comply with request by the Agency to discontinue the illegal processing of personal data and to take the measures ordered (Article 41, Paragraph 1);

q) The controller or processor who fails to furnish the information on Agency's request, or fails to allow the Agency to inspect any documents and records likely to bear personal data (Article 41, Paragraph 2);

r) Denies to the Agency's employees to enter any premises where the data are being processed (Article 41, Paragraph 3).

(2) For violation referred to in Paragraph 1 of this Article, the controller as the responsible person shall be fined in the amount ranging between KM 500 and 10,000 KM.

(3) For violation referred to in Paragraph 1 of this Article, the controller as the person in employment relationship shall be fined in the amount ranging between KM 300 and 5,000 KM.

**Article 50**

(1) The controller shall be fined for violation in the amount ranging between KM 5,000 and 150,000 KM, if:

a) Processes personal data on the basis of consent of the data subject that has not been made in accordance with Article 5, Paragraph 2;

b) Cannot prove that there is the consent and if does not keep the consent during the processing of personal data for which the consent has been granted (Article 5, paragraphs 4 and 5);

c) Entrusts the processing of personal data to a data processor without a contract containing specified elements (Article 12, Paragraph 2);

d) The data processor commences the processing on the basis of contract or legal act that does not bound the processor towards the controller (Article 12, Paragraph 3);

e) Fails to establish and does not maintain the prescribed records (Article 13);

f) Fails to furnish the Agency with data referred to in Article 13 (Article 14, Paragraph 1);

g) Establishes the personal data filing system before submitting a request with the Agency (Article 14, Paragraph 2);

h) Commences the establishment of personal data filing system without obtaining the Agency's consent, or that two months have not passed from the submitting the request with the Agency (Article 14, Paragraph 3);

i) Fails to furnish the Agency within 14 days with the information on the establishment of personal data filing system or on changes in the established personal data filing systems (Article 14, Paragraph 5);

j) Fails to maintain a special record on personal data that were given to the user (Article 17, Paragraph 5);

k) Processes the personal data for journalistic purposes, purposes of artistic and literary expressions contrary to the provisions on security and confidentiality of data (Article 19, Paragraph 2);

l) Fails to make data anonymous following the processing of personal data for statistical, archival and scientific purposes (Article 20, Paragraph 2);

m) Fails to ensure, in the processing of personal data for statistical, archival and scientific purposes, the level of their protection required by this Law (Article 20, Paragraph 3);

n) Fails to notify the data subject before the start of collection of personal data, unless he/she has already been informed thereof (Article 22);

o) Fails to notify the data subject about the third party that furnished him/her with personal data (Article 23);

p) Fails to notify the data subject about the processing of his/her data (Article 24);

q) Fails, on the basis of data subject's written request, to furnish once a year, without compensation, the information regarding the processing of his/her personal data (Article 25, Paragraph 1);

r) Fails to furnish the information in a written and intelligible form, within 30 days from the submission of a request (Article 25, Paragraph 3);

s) Refuses to provide the information to the data subject, unless otherwise stipulated by law (Article 26, Paragraph 1);

t) Fails to state the reasons for rejecting the information request (Article 26, Paragraph 2);

u) Fails to submit an annual report to the Agency on rejected requests (Article 26, Paragraph 3);

v) Makes a decision solely on the basis of automatic data processing (Article 29).

(2) For violation referred to in Paragraph 1 of this Article, the controller as the responsible person shall be fined in the amount ranging between KM 200 and 5,000 KM.

(3) For violation referred to in Paragraph 1 of this Article, the controller as an employee shall be fined in the amount ranging between KM 100 and 1,000 KM.

***Article 51***

A person who processes the personal data contrary to the conditions and extent determined by the controller or data processor shall be fined in the amount ranging between KM 500 and 5,000 KM (Article 16, Paragraph 1).

### *Article 52*

A responsible person within the public authority shall be fined for violation in the amount ranging between KM 500 and 5,000 KM who:

a) Fails to issue a regulation aimed at enforcing this Law (Article 11, Paragraph 3);

b) Fails to extend the support to the Agency in carrying out its duties (Article 41, Paragraph 5).

## CHAPTER VI.

## TRANSITIONAL AND FINAL PROVISIONS

### *Article 53*
### *Enactment of Bylaws*

(1) The Council of Ministers shall enact the regulations referred to in articles 11 and 15 of this Law within six months from the day of entry into force of this Law.

(2) The Council of Ministers may as well issue other regulations necessary for enforcement of this Law.

### *Article 54*
### *Procedure for Accessing Information of Public Interest*

Provisions of this Law shall be taken into consideration in application of the Law on Freedom of Access to Information.

### *Article 55*
### *Measures to Be Taken in the Transitional Period*

(1) The controller who has processed personal data by the date of entry into force of this Law and who is subject to the obligation referred to in Article 15, shall be obliged to fulfil this obligation not later than within six months of the date of the entry into force of this Law.

(2) Personal data processing carried out prior to the entry into force of this Law shall be brought into accord with this Law by December 31, 2006.

### *Article 56*
### *Appointments*

(1) The Agency shall commence its operation on the basis of special decision by the Council of Ministers, but not before January 1, 2007.

(2) Until the completion of appointment of the Director, the Commission for Personal Data Protection, appointed in accordance with the Law on the Protection of Personal Data ("Official Gazette of BiH", No.: 32/01), shall continue to work in accordance with this Law.

### *Article 57*
### *Cessation of Validity of the Former Law*

(1) On the day of entry into force of this Law, the Law on Personal Data Protection ("Official Gazette of BiH", No.: 32/01) shall no longer apply.

(2) Regulations enacted on the basis of the Law on Personal Data Protection ("Official Gazette of BiH", No.: 32/01), shall be applied until issuance of regulations on the basis of the present Law.

### *Article 58*
### *Entry into Force*

This Law shall enter into force on the eight day after the date on which it is published in the "Official Gazette of BiH".

PS BiH No 308/06
May 23, 2006
Sarajevo