Official Gazette of BiH, No. 12/25

Pursuant to Article IV.4.a) of the Constitution of Bosnia and Herzegovina, the Parliamentary Assembly of Bosnia and Herzegovina, at the 16th urgent session of the House of Representatives, held on January 23, 2025, and at the 8th urgent session of the House of Peoples, held on January 30, 2025, adopted the

LAW
PART I - GENERAL PROVISIONS ON

PERSONAL DATA PROTECTION

Article 1
(Subject matter)

(1) This Act provides for:

a) rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data;

b) responsibilities of the Personal Data Protection Agency in Bosnia and Herzegovina (hereinafter: the Agency), organisation and management, as well as other matters relevant to its operation and lawful functioning;

c) the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation and detection of criminal offences or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

(2) This Act ensures compliance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and the provisions of Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation and detection of criminal offences or the prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

(3) The reference to the provisions of the Regulation and the Directive referred to in paragraph (2) of this Article shall be made solely with the aim of monitoring and informing about the transposition of the acquis communautaire of the European Union into the legislation of Bosnia and Herzegovina.

Article 2
(Objective of the Act)

This Act protects the fundamental rights and freedoms of natural persons in Bosnia and Herzegovina regardless of their citizenship and residence, and in particular their right to the protection of personal data.

Article 3
(Use of male or female gender)

For the sake of clarity, terms given in only one grammatical gender in this Act apply without discrimination to both male and female genders.

Article 4
(Definitions)

Certain terms used in this Act have the following meanings:

a) 'personal data' means any information relating to an identified or identifiable natural person;

b) 'data holder' means an identified or identifiable natural person, whether directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to that person's physical, physiological, genetic, mental, economic, cultural or social identity;

c) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

d) 'restriction of processing' means the marking of stored personal data with the aim of limiting its processing in the future;

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

f) 'pseudonymisation' means the processing of personal data in such a way that the personal data can no longer be attributed to a specific data holder without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

g) 'collection of personal data' means any structured set of personal data which are accessible according to specific criteria, regardless of whether they are centralised, decentralised or dispersed on a functional or geographical basis;

h) 'data controller' means the natural or legal person, public authority or competent authority which, alone or jointly with others, determines the purposes of the means of processing personal data. Where the purposes and means of such processing are determined by law, the data controller or the specific criteria for its nomination shall be prescribed by law;

i) 'public body' means any legislative, executive and judicial body at all levels of government in Bosnia and Herzegovina;

j) 'competent authority' means an authority which is competent for the prevention, investigation and detection of criminal offences, the prosecution of perpetrators of criminal offences or the execution of criminal penalties, including the safeguarding and prevention of threats to public security, as well as legal persons where they are authorised by law to carry out those tasks as a special category of data controller;

k) 'processor' means a natural or legal person, public authority or body which processes personal data on behalf of the data controller;

l) 'recipient' means a natural or legal person, a public authority, to which the personal data are disclosed, whether a third party or not. Public authorities which may receive personal data within a particular inquiry in accordance with the law shall not be

regarded as recipients, but the processing of those data shall comply with the applicable data protection rules according to the purposes of the processing;

m) 'third party' means a natural or legal person, public authority, the Agency or a body other than the data holder, the data controller, the processor and the persons authorised to process personal data under the direct authority of the data controller or the processor;

n) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes when he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

o) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

p) 'genetic data' means personal data relating to inherited or acquired genetic features of a natural person which provide unique information about the physiology or health of that natural person and which are obtained by specific analysis of a biological sample of that natural person;

r) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person, such as photographs of persons or dactyloscopic data;

s) 'data concerning health' means personal data relating to the physical or mental health of a natural person, including the provision of health services, which provide information on his or her state of health;

t) 'representative' means a natural or legal person domiciled or resident or having its registered office or establishment in Bosnia and Herzegovina; and
Herzegovina, designated in writing by the data controller or processor in accordance with Article 29 of this Act;

u) 'economic operator' means a natural or legal person engaged in an economic activity, irrespective of the legal form of the activity;

v) 'group of economic operators' means an economic operator exercising control and economic operators under its control;

z) 'binding business rule' means a personal data protection policy adhered to by a data controller and processor established in Bosnia and Herzegovina when transferring personal data or sets of transfers of personal data to a data controller or processor in one or more other countries within a group of economic operators or a group of economic operators engaged in a joint economic activity;

aa) 'information society service' means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services, where:

1) 'at a distance' means that the service is provided without the parties being present at the same time;

2) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;

3) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request;

'international organisation' means an organisation with its organs governed by public international law or any other body which is set up by, or on the basis of, an agreement between two or more countries; cc) 'establishment' means the effective and real exercise of an activity through stable arrangements;

dd) "video surveillance" is an information and communication system that has the ability to collect and further process personal data, which includes the creation of a recording that forms or is intended to form part of a storage system.

Article 5
(Main scope)

(1) This Act shall apply to the processing of personal data wholly or partly by automated means and to the non-automated processing of personal data which form part of a personal data collection or are intended to form part of a personal data collection.

(2) This Act shall not apply to the processing of personal data by a natural person solely for the purpose of personal or household activities.

(3) Part Two of this Act shall not apply to the processing of personal data by a competent authority for the protection of natural persons in relation to the processing of personal data for the purposes of the prevention, investigation and detection of criminal offences or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Article 6
(Territorial scope)

(1) This Act shall apply to the processing of personal data by a data controller or processor having its registered office or establishment, domicile or residence in Bosnia and Herzegovina, regardless of whether the processing is carried out in Bosnia and Herzegovina or not.

(2) This Act shall apply to the processing of personal data of a data subject in Bosnia and Herzegovina by a controller or processor who has no seat or establishment, domicile or residence in Bosnia and Herzegovina, if the processing activity is related to:

a) offering goods or services to those data carriers in Bosnia and Herzegovina, irrespective of whether the payment is to be made by the data carrier; or

b) monitoring the behaviour of data subjects, provided that their behaviour is manifested within Bosnia and Herzegovina.

(3) This Act shall apply to the processing of personal data by a data controller or processor not established in Bosnia and Herzegovina but in a place where the law of Bosnia and Herzegovina applies by virtue of international law.

(4) This Article shall not apply to the processing of personal data by a competent authority for the protection of a natural person in relation to the processing of personal data for the purposes of the prevention, investigation and detection of criminal offences or the prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

PART OTHER - PROCESSING PERSONAL DATA FROM A PERSON, LEGAL PERSON OR PUBLIC AUTHORITY AS DATA CONTROLLER
CHAPTER I PRINCIPLES OF PERSONAL DATA PROCESSING

Article 7
(Principles of personal data processing)

(1) The principles of personal data processing are:

a) legality, fairness and transparency vis-à-vis the data subject;

b) Purpose limitation – data must be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with Article 56(1) of this Act, shall not be considered incompatible with the original purposes;

c) data minimisation – data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) Accuracy – data must be accurate and, where necessary, kept up to date. All reasonable measures must be taken to ensure that personal data which are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) Restricted storage – the data must be kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be kept for a longer period if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with Article 56, paragraph 1 of this Act, subject to the implementation of appropriate technical and organizational measures prescribed by this Act in order to protect the rights and freedoms of the data subject;

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

(2) Reliability principle – the data controller shall be responsible for the compliance of the processing of personal data with paragraph (1) of this Article and shall be able to demonstrate such compliance.

Article 8
(Lawfulness of the processing of personal data)

(1) Processing of personal data shall be lawful only if at least one of the following conditions is met:

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

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

c) if processing is necessary for compliance with the legal obligations of the data controller;

d) processing is necessary to protect the essential interests of the data subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;

f) processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require

protection of personal data, in particular where the data subject is a child. This point shall not apply to processing carried out by public authorities in the performance of their tasks.

(2) The legal basis for the processing of personal data referred to in paragraph (1), points (c) and (e) of this Article shall be laid down by the laws of the institutions of BiH, icanton entities in accordance with their respective competences, in such a way as to lay down more precisely specific conditions for processing and other measures to ensure lawful and fair processing, including for other specific processing, as provided for in Chapter V of this Law.

(3) The special law on data processing referred to in paragraph (1), points (c) and (e) of this Article of the institutions of BiH, entities and cantons, in accordance with the competences, prescribes the purpose of processing, which in terms of processing referred to in paragraph (1), point (e) of this Article must be necessary for the performance of a task carried out in the public interest or as part of the exercise of official authority of the data controller. This law provides for: the general conditions governing the lawfulness of the processing carried out by the data controller, the types of data processed, the categories of data subjects, the entities to which the personal data may be disclosed and the purposes for which the data may be disclosed, purpose limitation, retention periods, and processing operations and processing operations, including measures to ensure lawful and fair processing as well as for other specific processing as referred to in Chapter V of this Act. The law must meet an objective of public interest and the processing must be proportionate to the legitimate aim pursued.

(4) Where processing is carried out for a purpose other than that for which the personal data have been collected and is not based on the data subject's consent or on a special law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 25(1) of this Act, the data controller shall, in order to determine whether processing for another purpose is compatible with the purpose for which the personal data were initially collected, take into account, inter alia:

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

b) the context in which the personal data have been collected, in particular as regards the relationship between the data subject and the data controller;

c) the nature of the personal data, in particular whether special categories of personal data are processed in accordance with Article 11 of this Act or whether personal data relating to criminal convictions and offences are processed in accordance with Article 12 of this Act; d) the possible consequences of the intended further processing for the data subjects;

e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

(5) The public and competent authorities of the Entities and Brčko District of BiH shall, in compliance with the provisions of this Law, transfer personal data from their records to an authorized data controller, for the purpose of prior declaration of citizens who have the right to vote on issues for which special regulations allow this right.

Article 9
(Consent)

(1) Where processing is based on consent, the data controller shall demonstrate that the data subject has given consent to the processing of his or her personal data.

(2) Where the data subject gives his or her consent in a written statement which also covers other matters, the request for consent shall be presented in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. The part of the consent that constitutes a violation of this Act shall not apply.

(3) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of data processing based on consent before its withdrawal. Before giving consent, the data subject shall be informed thereof. Withdrawal of consent must be as simple as granting it.

(4) When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the performance of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 10
(Conditions applicable to the consent of the child in relation to an information society service)

(1) Where point (a) of Article 8(1) of this Act applies in relation to the direct offering of an information society service to a child, the processing of the personal data of a child shall be lawful if the child is at least 16 years old. If the child is under the age of 16, such processing is lawful only if and to the extent that consent is given or approved by the parent, adoptive parent, guardian of the child or other representative of the child.

(2) The data controller must make reasonable efforts to verify that consent is given or approved in such cases by the parent, adoptive parent or guardian of the child, taking into account available technology.

(3) Paragraph (1) of this Article shall not affect the general rules of mandatory law concerning the validity, conclusion or effect of a contract in relation to a child.

Article 11
(Processing of special categories of personal data)

(1) The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union affiliation, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health or data concerning a person's sex life or sexual orientation shall be prohibited.

(2) By way of derogation from paragraph (1) of this Article, the processing of special categories of personal data is permitted if one of the following conditions is met:

a) the data subject has given his or her explicit consent to the processing of those personal data for one or more specific purposes, except where a specific law provides that the processing of those data may not be carried out on the basis of consent;

b) where the processing is necessary for the fulfilment of the obligations and the exercise of specific rights of the data controller or of the data subject in the field of labour law and social security and social welfare law, in so far as it is provided for by law or a collective agreement, in accordance with a special law providing for appropriate measures to protect the fundamental rights and the interests of the data subject;

c) if the processing is necessary to protect the vital interests of the data subject or of another natural person, if the data subject is physically or legally incapable of giving consent;

d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-making organisation with a political, philosophical, religious or trade union aim and on condition that the processing relates exclusively to the members or former members of that organisation or to natural persons who have regular contact with it in connection with its purposes, and that the personal data are not disclosed outside that organisation without the consent of the data subject;

e) where the processing relates to personal data which are manifestly made public by the data subject;

f) processing is necessary for the establishment, exercise or defence of legal claims or when courts are acting in their judicial capacity;

g) processing is necessary for reasons of substantial public interest, on the basis of a law which is proportionate to the legitimate aim pursued, respects the essence of the right to the protection of personal data and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h) processing is necessary for the purposes of preventive or occupational medicine for the assessment of the working capacity of the employee, a medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of a special law or pursuant to a contract with a health professional and subject to the conditions and safeguards referred to in paragraph (3) of this Article;

i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products and medical devices, on the basis of a specific law which lays down suitable and specific measures to safeguard the rights and freedoms of data subjects, in particular professional secrecy;

j) where processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 56(1) of this Act, on the basis of a special law, which shall be proportionate to the legitimate aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

(3) Personal data referred to in paragraph (1) of this Article may be processed for the purposes referred to in point (h) of paragraph (2) of this Article when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy in accordance with a specific law or rules established by competent public authorities or other persons subject to the obligation of secrecy in accordance with a specific law or rules established by competent public authorities.

(4) Specific laws may maintain or introduce additional conditions, including limitations, in relation to the processing of genetic data, biometric data or health data.

Article 12
(Processing of personal data relating to criminal convictions and offences)

The processing of personal data relating to criminal convictions and offences or related security measures pursuant to Article 8(1) of this Act may be carried out only under the supervision of a public authority or when the processing is prescribed by a special law providing for appropriate safeguards for the rights and freedoms of the data subject. The register of criminal convictions shall be kept exclusively under the control of a public authority.

Article 13
(Processing that does not require identification)

(1) If the data controller processes personal data for which the purpose of processing is not required or no longer required to identify the data subject, the data controller is not obliged to store, obtain or process additional information for the purpose of identifying the data subject solely for compliance with this Act.

(2) If, in the cases referred to in paragraph 1 of this Article, the data controller can prove that he or she cannot identify the data subject, the data controller shall inform the data subject accordingly, if possible. In such cases, Art. 17 does not apply. – 22 of this Act, unless the data subject, for the purpose of exercising his or her rights under these Articles, provides additional information enabling his or her identification.

CHAPTER II RIGHTS OF DATA HOLDER

Article 14

(Transparent information, communication and how to exercise the rights of data subjects)

(1) The data controller shall take appropriate measures to provide the data subject with all the information referred to in Articles 15 and 16 of this Act and all forms of communication for the exercise of the rights referred to in Article 17 of the GDPR. – 24 of this Act and Article 36 of this Act in relation to data processing, in a concise, transparent, intelligible and easily accessible form, using clear and plain language, which applies in particular to all information specifically addressed to a child. The information shall be provided in writing or by other means, including by electronic means where appropriate. If requested by the data subject, the information may be provided orally, provided that the identity of the data subject is established by other means.

(2) The data controller facilitates the exercise of the data subject's rights under Art. 17 GDPR. – 24 of this Act. In the cases referred to in Article 13(1) of this Act, the data controller may not refuse to act on the data subject's request to exercise his or her rights referred to in Article 17 of the GDPR. – 24 of this Act, unless the data controller proves that he cannot establish the identity of the data subject.

(3) The data controller shall, at the request of the data subject, provide the data subject with information on the action taken pursuant to Article 17. – 24 of this Act without undue delay and in any event within 30 days from the date of receipt of the request. That period may be extended by 60 days where necessary, taking into account the complexity and number of applications received. The data controller shall inform the data subject of any such extension within 30 days from the date of receipt of the request, stating the reasons for the delay. Where the data subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

(4) If the data controller does not act on the request of the data subject, he or she shall, without delay and no later than 30 days from the date of receipt of the request, inform the data subject of the reasons for which he or she did not act on the request and of the possibility of filing a complaint to the Agency or a complaint to the competent court and other legal remedies.

(5) Information provided in accordance with Articles 15 and 16 of this Act and all communications and actions referred to in Article 17 – 24 of this Act and Article 36 of this Act shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the data controller may:

a) charge a fee for actual administrative costs, such as copying, scanning or data carrier costs, as well as a fee for delivery or handling of the request, or

b) refuse to act on the request.

(6) The controller shall bear the burden of proving the manifestly unfounded or excessive character of the request.

(7) Where the data controller has reasonable doubts concerning the identity of the natural person making the request referred to in Article 17. – 23 of this Act, he may, without prejudice to Article 13 of this Act, request additional information necessary to confirm the identity of the data subject.

(8) The information that must be provided to data subjects, in accordance with Articles 15 and 16 of this Act, may be provided in combination with standardized symbols, in order to provide a logical overview of the intended processing in an easily visible, intelligible and clearly legible manner. If the symbols are displayed electronically, they shall be machine-readable.

(9) The Agency shall be empowered to adopt regulations for the purpose of specifying the information to be displayed by symbols and procedures for establishing standardised symbols.

Article 15

(Information to be provided if personal data is collected from the data subject)

(1) Where personal data are collected from the data subject, the data controller shall, at the time when personal data are collected, provide the data subject with the following information:

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

b) the contact details of the data protection officer, where applicable;

c) the legal basis for the processing and the purpose of the processing of the personal data;

d) the legitimate interest of the data controller or a third party, if the processing is based on Article 8(1)(f) of this Act;e) the

recipient or category of recipients of the personal data, if any;

f) the fact that the data controller intends to transfer personal data to another country or international organisation and the existence or non-existence of an adequacy decision of the Council of Ministers of Bosnia and Herzegovina, or in the case of transfers referred to in Article 48 of the GDPR;
or 49 of this Act or Article 51(2) of this Act, references to appropriate or appropriate protective measures and the means of obtaining a copy of them or the place where they are made available, where applicable.

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

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

b) the right to request from the data controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to the processing of such data, and the right to data portability;

c) the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent prior to its withdrawal, if the processing is based on Article 8(1)(a) of this Act or Article 11(2)(a) of this Act;

d) the right to lodge a complaint with the Agency or to bring an action before the competent court;

e) information as to whether the provision of the personal data is a legal or contractual obligation or a necessary condition for the conclusion of the contract, as well as whether the data subject is obliged to provide the personal data and what the possible consequences are if such data is not provided;

f) on the existence of automated decision-making, including profiling referred to in Article 24, paragraphs (1) and (4) of this Act, whereby at least it is obliged to provide information on the mode of operation, as well as the significance and envisaged consequences of such processing for the data subject.

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

(4) The data controller shall not be obliged to provide information to the data subject referred to in paragraphs (1), (2) and (3) of this Article to the extent that the data subject already has that information.

Article 16

(Information to be provided if the personal data have not been obtained from the data subject)

(1) If the personal data have not been obtained from the data subject, the data controller shall provide the data subject with the following information:

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

b) the contact details of the data protection officer, where applicable;

c) the legal basis for the processing and the purpose of the processing for which the personal data are intended;

d) the categories of personal data processed;

e) the recipient or categories of recipients of the personal data, where applicable;

f) on the facts that the data controller intends to transfer personal data to a recipient in another country or international organisation and on the existence or non-existence of a decision of the Council of Ministers of Bosnia and Herzegovina on adequacy referred to in Article 47, paragraph (3) of this Act or in the case of transfer of personal data referred to in Articles 48 or 49 of this Act or Article 51, paragraph (2) of this Act with reference to appropriate or appropriate safeguards and methods of obtaining a copy of them or the place where they have been made available, if applicable.

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

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

b) the legitimate interests pursued by the data controller or by a third party where processing is based on point (f) of Article 8(1) of the GDPR;
of the law;

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

d) the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before withdrawal, if the processing is based on Article 8(1)(a) of this Act or Article 11(2)(a) of this Act; e) the right to lodge a complaint with the Agency or to bring an action before the competent court;

f) the source of the personal data and, where applicable, whether it comes from publicly available sources;

g)the existence of automated decision-making, including profiling, referred to in Article 24(1) and (4) of this Act and, at least in those cases, reasonable information about the criterion used, as well as the significance and the envisaged consequences of such processing for the data subject.

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

a) within a reasonable period after obtaining the personal data, but no later than 30 days, having regard to the specific circumstances in which the personal data are processed;

b) if the personal data is used for communication with the data subject, at the latest at the time of the first communication, or

c) if disclosure to another recipient is envisaged, at the latest at the time the personal data are first disclosed.

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

(5) Paragraphs (1) to (4) of this Article shall not apply if and to the extent that:

a) the data subject already possesses the information;

b) the provision of such information is impossible or would require disproportionate efforts, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with the conditions and safeguards referred to in Article 56(1) of this Act or in so far as the obligation referred to in paragraph (1) of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases, the data controller shall take appropriate measures to safeguard the data subject's rights and freedoms and legitimate interests, including making the information available to the public;

c) the obtaining or disclosure of the data is expressly provided for by a special law applicable to the data subject which provides appropriate measures to protect the data subject's legitimate interests; or

d) personal data must remain confidential in accordance with the obligation of professional secrecy prescribed by a special law, including other legal obligations of secrecy.

Article 17
(Data subject's right of access to personal data)

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

b) the category of personal data to be processed;

c) the recipient or categories of recipients to whom the personal data have been or will be disclosed, in particular a recipient in another country or an international organisation;

d) the envisaged period within which the personal data shall be kept, where possible or where that is not possible, the criteria used to determine that period;

e) the right to request from the data controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

f) the right to lodge a complaint with the Agency or to bring an action before the competent court;

g) if the personal data are not collected from the data subject, any available information as to their source;

h) the existence of automated decision-making, including profiling, referred to in Article 24(1) and (4) of this Act and, at least in those cases, reasonable information about the criterion used, as well as the significance and the envisaged consequences of such processing for the data subject.

(2) Where personal data are transferred to another country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 48 of this Act relating to the transfer of data.

(3) The data controller shall provide a copy of the personal data being processed. For any additional copies requested by the data subject, the data controller may charge a reasonable fee based on administrative costs. Where the data subject makes

the request by electronic means, unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

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

Article 18
(Right to rectification)

(1) The data subject shall have the right to obtain from the data controller the rectification of inaccurate personal data without undue delay.

(2) Taking into account the purpose of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of a supplementary statement.

Article 19
(Right to erasure)

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

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

b) the data subject has withdrawn the consent on which the processing is based pursuant to Article 8(1)(a) of this of the Act or Article 11, paragraph (2), item a) of this Act and if there is no other legal basis for processing;

c) the data subject has objected to the processing in accordance with Article 23(1) of this Act and there are no legal grounds for the processing or the data subject has objected to the processing in accordance with Article 23(2) of this Act; d) the personal data has been unlawfully processed;

e) the personal data must be erased in order to comply with a legal obligation to which the data controller is subject;

f) personal data is collected in connection with the offer of information society services referred to in Article 10(1) of this Act.

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

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

a) to exercise the right to freedom of expression and information;

b) for compliance with a legal obligation requiring processing prescribed by a special law applicable to the data controller or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;

c) for reasons of public interest in the area of public health in accordance with Article 11(2)(h) and (i) of this Article, as well as Article 11(3) of this Act;

d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 56(1) of this Act in so far as the right referred to in paragraph (1) of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

e) for the establishment, exercise or defence of legal claims.

Article 20
(Right to restriction of processing)

(1) The data subject shall have the right to restrict the processing of data where one of the following conditions is met:

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

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

c) the controller no longer needs the personal data for the purposes of the processing, but it is required by the data subject for the establishment, exercise or defence of legal claims;

d) the data subject has objected to the processing in accordance with Article 23(1) of this Act and expects confirmation whether his or her reasons override the legitimate reasons of the data controller.

(2) Where processing has been restricted pursuant to paragraph 1 of this Article, that personal data may be processed only with the consent of the data subject, with the exception of retention, or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of substantial public interest.

(3) The data subject who has exercised the right to restriction of processing pursuant to paragraph 1 of this Article shall be informed by the data controller before the restriction of processing is lifted.

Article 21
(Obligation to notify rectification or erasure of personal data or restriction of processing)

(1) The data controller shall inform all recipients to whom the personal data have been disclosed of any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 18, Article 19(1) and Article 20 of this Act, unless this is impossible or involves disproportionate effort.

(2) The data controller shall inform the data subject of those recipients if the data subject so requests.

Article 22
(Right to portability of personal data)

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

a) the processing is carried out in accordance with Article 8(1)(a) of this Act or Article 11(2)(a) of this Act or on the basis of a contract in accordance with Article 8(1)(b) of this Act, b) the processing is carried out automatically.

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

(3) The exercise of the right to data portability referred to in paragraph (1) of this Article shall be without prejudice to Article 19 of this Act. This right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

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

Article 23
(Right to object)

(1) The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her by the controller pursuant to Article 8(1)(e) or (f) of this Act, including profiling based on those provisions. The controller shall no longer process the personal data in the event of the objection, unless we can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.

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

(3) If the data subject opposes the processing for direct marketing purposes, the personal data shall no longer be processed for these purposes.

(4) At the latest at the time of the first communication with the data subject, the data subject shall make express reference to the rights referred to in paragraph 1 and
(2) of this Article and must be done in a clear manner and separately from any other information.

(5) In the context of the use of information society services and without prejudice to regulations in the field of electronic communications, the data subject may exercise his or her right to object by automated means using technical specifications.

(6) Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 56(1) of this Act, the data subject shall have the right, on grounds relating to his or her particular situation, to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out in the public interest.

Article 24
(Automated individual decision-making, including profiling)

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

(2) Paragraph (1) of this Article shall not apply where the decision:

a) necessary for the conclusion or performance of a contract between the data subject and the data controller,

b) permitted by the law applicable to the data controller, which lays down appropriate safeguards for the data subject's rights of freedom and legitimate interests, or

c) based on the explicit consent of the data subject.

(3) In the cases referred to in points (a) and (c) of paragraph 2 of this Article, the data controller shall take appropriate measures to safeguard the data subject's rights of freedom and legitimate interests, at least the right to participate in the decision-making of the natural person, the right to express his or her point of view and the right to contest the decision.

(4) The decision referred to in paragraph (2) of this Article may not be based on special categories of personal data referred to in Article 11, paragraph (1) of this Act, unless Article 11, paragraph (2), item (a) or (g) of this Act applies and appropriate measures are in place to protect the rights and freedoms and legitimate interests of the data subject.

Article 25
(Restrictions)

(1) Under the specific law applicable to the data controller and the processor, the scope of the rights and obligations referred to in Article 7, Article 14 may be limited. – 24 of this Act and Article 36 of this Act in so far as the provisions of that Act correspond to the rights and obligations laid down in Article 14. – 24 of this Act, if such a restriction respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society to safeguard: a) State security;
b) defence;

c) public security;

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

e) other essential objectives of general public interest in Bosnia and Herzegovina, in particular an essential economic or financial interest, including monetary, budgetary and tax matters, public health and social welfare; f) the independence of the judiciary and judicial proceedings;

g) the prevention, investigation, detection and prosecution of breaches of ethics in regulated professions;

h) a supervisory, inspection or regulatory function connected, at least occasionally, with the exercise of official authority in the cases referred to in points (a) to (e) and (g) of this paragraph;

i) the data subject or the rights and freedoms of others;

j) enforcement of civil law claims.

(2) The special law referred to in paragraph (1) of this Article shall contain, where appropriate, special provisions

containing at least the following: the purpose of the processing or category of processing;

b) the category of personal data;

c) the scope of restrictions imposed;

d) safeguards to prevent abuse or unlawful access or transfer;

e) the designation of the data controller or category of data controller;

f) the retention period and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;g) the risk to the rights and freedoms of data subjects;

h) the right of the data subject to be informed of the restriction, unless this may be prejudicial to the purpose of the restriction.

CHAPTER III DATA CONTROLER AND EDUCER

Article 26
(Obligation of the data controller)

(1) The data controller shall apply appropriate technical and organisational measures taking into account the nature, scope, circumstances and purposes of the processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, in order to ensure and demonstrate the performance of processing in accordance with this Act. Those measures shall be reviewed and updated as necessary.

(2) Where the measures referred to in paragraph 1 of this Article are proportionate in relation to processing activities, they shall include the implementation of appropriate data protection policies against the data controller.

(3) Compliance with the approved codes of conduct referred to in Article 42 of this Act or the approved certification mechanisms referred to in Article 44 of this Act may serve as an element to demonstrate compliance with the obligations of the data controller.

Article 27
(Data protection by design and by default)

(1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons arising from data processing, the data controller shall, when determining the means of processing and at the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, to enable the effective application of data protection principles, such as data minimisation, and the integration of safeguards into the processing in order to meet the requirements of this Act and protect the rights of data subjects.

(2) The data controller shall implement appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This obligation applies to all personal data collected, the scope of their processing, the period of their retention and their availability. Those measures shall ensure that personal data are not automatically accessible, without the intervention of a natural person, to an unlimited number of other natural persons.

(3) The approved certification mechanism referred to in Article 44 of this Act may serve as an element to demonstrate compliance with the requirements referred to in paragraphs (1) and (2) of this Article.

Article 28
(Joint Data Controllers)

(1) Where two or more data controllers jointly determine the purposes and means of processing, they shall be regarded as joint data controllers. They shall in a transparent manner, by mutual agreement, determine the responsibilities of each of them with a view to fulfilling the obligations under this Act, in particular with regard to the exercise of the rights of data subjects and the duties of each of them in relation to the provision of the information referred to in Articles 15 and 16 of this Act, unless the responsibilities of each of the data controllers are determined by the law applicable to data controllers. The agreement may designate a contact point for data holders.

(2) The agreement referred to in paragraph 1 of this Article shall adequately reflect the respective roles and relationships of the joint data controllers vis-à-vis the data holders. The essence of the agreement shall be made available to the data subject.

(3) Notwithstanding the terms of the agreement referred to in paragraph (1) of this Article, the data subject may exercise his or her rights under this Act in relation to and against each of the data controllers.

Article 29

(Representative of a data controller or processor not established in Bosnia and Herzegovina)

(1) Where Article 6(2) of this Act applies, the data controller or processor shall be obliged to appoint in writing its representative in Bosnia and Herzegovina.

(2) The obligation referred to in paragraph 1 of this Article shall not apply to:

a) processing which is occasional, does not involve the processing of special categories of data referred to in Article 11(1) of this Act or the processing of personal data relating to criminal convictions and offences referred to in Article 12 of this Act, and which is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, circumstances, scope and purposes of the processing; or

b) public authorities.

(3) The data controller or processor shall authorise the representative to be addressed, in addition to or instead of the data controller or processor, in particular by the Agency and the data subject with regard to all issues relating to the processing of personal data in order to ensure compliance of the processing of personal data with this Act.

(4) The designation of a representative of the data controller or processor shall not affect legal claims which may be made against the data controller or processor itself.

Article 30
(Processor)

(1) If the processing of personal data is carried out on behalf of the data controller, the data controller shall use only a processor who sufficiently guarantees the application of appropriate technical and organisational measures so that the processing complies with the requirements of this Act and that the processing ensures the protection of the rights of the data subject.

(2) The processor may not engage another processor without the prior specific or general written consent of the data controller. In the event of a general written authorisation, the processor shall inform the data controller of any intended changes concerning the addition or replacement of other processors in order to allow the data controller to object to those changes.

(3) Processing by a processor shall be governed by a contract or other legal act pursuant to the law by which the processor is bound to the data controller, specifying the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, as well as the obligations and rights of the data controller.

(4) The contract or other legal act referred to in paragraph (3) of this Article shall stipulate that the processor shall:

a) process the personal data only on documented instructions from the data controller, including with regard to the transfer of the personal data to another country or international organisation, unless required to do so by a specific law applicable to the processor, in which case the processor shall inform the data controller of that legal requirement prior to the processing, unless that law prohibits such communication for important reasons of public interest;

b) ensure that persons authorised to process personal data have committed themselves to confidentiality or are bound by the relevant law to respect confidentiality;

c) take all necessary measures in accordance with Article 34 of this Act;

d) comply with the conditions set out in paragraphs (2) and (5) of this Article for engaging another processor;

e) taking into account the nature of the processing, assist the data controller by appropriate technical and organizational measures, insofar as this is possible, to fulfill the obligation of the data controller to respond to requests for exercising the rights of the data subject from
Chapter II of this Act;

f) assist the data controller in ensuring compliance with the obligations referred to in Article 34. – 38 of this Act, taking into accountthe nature of the processing and the information available to the processor;

g) at the choice of the data controller, delete or return all personal data to the data controller after the end of the provision of services related to processing and delete existing copies, unless a special law prescribes the obligation to store personal data;

h) make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in this Article and to the data controller or another auditor mandated by the data controller to enable and assist in the performance of audits, including inspections;

i) in the case referred to in point h) of this paragraph, the processor shall immediately inform the data controller if, in his opinion, a particular instruction infringes this Act or other data protection rules.

(5) Where a processor engages another processor to carry out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the contract or other legal act between the data controller and the processor referred to in paragraph (4) of this Article shall be imposed on that other processor by way of a contract or other legal act in accordance with a specific law, in particular the obligation to provide sufficient guarantees for the application of appropriate technical and organisational measures in a manner that ensures that the processing meets the requirements of this Act. Where that other processor does not comply with the data protection obligations, the first processor shall remain fully liable to the data controller for compliance with the obligations of that other processor.

(6) Compliance with approved codes of conduct by processors referred to in Article 42 of this Act or an approved certification mechanism referred to in Article 44 of this Act may serve as an element to demonstrate the provision of sufficient guarantees referred to in paragraphs (1) and (5) of this Article.

(7) Without prejudice to an individual contract between the data controller and the processor, the contract or other legal act referred to in paragraphs (3), (4) and (5) of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs (8) and (9) of this Article, including, but not limited to, clauses which are part of a certificate granted to the data controller or processor pursuant to Article 44; and
45 of this law.

(8) The Agency may adopt standard contractual clauses for the matters referred to in paragraphs (3), (4) and (5) of this Article with a view to the consistent application of this Act.

(9) The contract or other legal act referred to in paragraphs (3), (4) and (5) of this Article shall be in writing, including in electronic form.

(10) Without prejudice to Articles 112, 113, 114 and 115 of this Act, if a processor infringes this Act by determining the purpose of a data processing operation, the processor shall be considered a data controller in relation to that processing.

Article 31
(Processing of personal data under the supervision of the data controller or processor)

The processor and the person working under the supervision of the data controller or processor, who has access to personal data, may not process this data without the order of the data controller, except where this is required by a special law.

Article 32
(Personal Data Processing Record)

(1) Each data controller and, where applicable, the data controller's representative shall keep a record of the processing activities under his or her responsibility. The records shall contain the following information:

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

b) the purposes of the processing;

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

d) the categories of recipients to whom the personal data have been or will be disclosed, including recipients in other countries or international organisations;

e) where applicable, the transfer of personal data to another country or international organisation, including the identification of another country or international organisation and, in the case of transfers referred to in Article 51(2) of this Act, the documentation of appropriate safeguards;

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

g) where possible, a general description of the technical and organisational security measures referred to in Article 34(1) of this Act.

(2) Each processor and, where applicable, the processor's representative shall keep a record of all processing activities carried out on behalf of the data controller, containing:

a) the name and contact details of the processor or processors and of each data controller on whose behalf the processor is acting and, where applicable, of the data controller's or processor's representative as well as of the data protection officer;

b) the types of processing carried out on behalf of each data controller;

c) where applicable, information on the transfer of personal data to another country or international organisation, identifying that other country or international organisation and, in the case of the transfer referred to in Article 51(2) of this Act, documentation of appropriate safeguards;

d) where possible, a general description of the technical and organisational security measures referred to in Article 34(1) of this Act.

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

(4) The data controller or the processor and the representative of the data controller or the processor, where applicable, shall make the logs available upon request by the Agency.

(5) The obligations referred to in paragraphs (1) and (2) of this Article shall not apply to an economic operator or an organisation employing fewer than 250 persons, except where the processing it carries out is likely to present a high risk to the rights and freedoms of data subjects where the processing is not occasional or where the processing covers special categories of data referred to in Article 11(1) of this Act or where personal data relating to criminal convictions and offences are concerned.

Article 33
(Cooperation with the Agency)

The data controller and the processor, and where their representatives have been designated, shall, on a reasoned and legally justified request, cooperate with the Agency in the performance of its tasks.

Article 34
(Security of personal data processing)

(1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, in carrying out the procedure referred to in Article 37 of this Act, the data controller and the processor shall implement appropriate technical and organisational measures to achieve a level of security appropriate to the risk, which shall include, where appropriate:

a) pseudonymisation and encryption of personal data;

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

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

d) a process for regularly testing, assessing and assessing the effectiveness of technical and organisational measures to achieve the safety of the processing.

(2) When assessing the appropriate level of security, account shall be taken, in particular, of the risks posed by processing, in particular the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

(3) The application of an approved code of conduct referred to in Article 42 of this Act or an approved certification mechanism referred to in Article 44 of this Act may be used as an element to demonstrate compliance with the requirements referred to in paragraph (1) of this Article.

(4) The data controller and the processor shall take measures to ensure that any natural person acting under the authority of the data controller or the processor, who has access to personal data, does not process that data unless instructed to do so by the data controller, except in cases where required by a specific law.

Article 35
(Reporting of a personal data breach to the Agency)

(1) The data controller shall notify the personal data breach to the Agency without undue delay and, if possible, not later than 72 hours after having become aware of it, unless it is likely that the personal data breach will not endanger the rights and freedoms of a natural person. If the reporting is not done within 72 hours, the data controller shall provide the Agency with the reasons for the delay.

(2) The processor shall, upon becoming aware of a personal data breach, notify the data controller thereof without undue delay.

(3) The report referred to in paragraph 1 of this Article shall contain at least the following:

a) a description of the nature of the personal data breach, and where possible, specifying the categories and approximate number of data holders, as well as the categories and approximate number of personal data records;

b) the name and contact details of the data protection officer or other contact point from which further information may be obtained;

c) a description of the likely consequences of the personal data breach;

d) a description of the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse consequences.

(4) If and to the extent that it is not possible to submit the information at the same time, the information may be provided in parts, without undue further delay.

(5) The data controller shall document any personal data breach, including the facts relating to the personal data breach, its consequences and the remedial action taken. The documentation referred to in this paragraph shall enable the Agency to comply with this Article.

Article 36
(Notification of a personal data breach to the data subject)

(1) The data controller shall, without delay, notify the data subject in writing of a personal data breach if the personal data breach is likely to result in a high risk to the rights and freedoms of a natural person.

(2) In the notification referred to in paragraph (1) of this Article, the data controller shall describe in clear and plain language the nature of the personal data breach and shall at least specify the information and measures referred to in Article 35(3), points (b), (c) and (d) of this Act.

(3) The communication to the data subject referred to in paragraph 1 of this Article shall not be required if one of the following conditions is met:

a) the data controller has implemented appropriate technical and organisational safeguards and those measures have been applied to the personal data in relation to which the personal data breach occurred, in particular measures that render the personal data unintelligible to a person who is not authorised to access it, such as encryption;

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

c) where this would involve a disproportionate effort, a public notice must be published or a similar measure must be taken to inform data holders in an equally effective manner.

(4) If the data controller has not notified the data subject of the personal data breach, the Agency, having considered the degree of likelihood of the personal data breach resulting in a high risk to the rights and freedoms of natural persons, may require the data controller to do so if any of the conditions referred to in paragraph (3) of this Article is not met.

Article 37
(Assessment of the impact of processing on the protection of personal data)

(1) Where a type of processing, in particular using new technologies, and taking into account the nature, scope, context of execution of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the data controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing on the protection of personal data.

(2) When carrying out an assessment of the impact of processing on the protection of personal data, the data controller shall seek the advice of the personal data protection officer, if one has been appointed.

(3) The assessment of the impact of the processing on the protection of personal data referred to in paragraph 1 of this Article shall be mandatory in particular in the case of:

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

b) processing on a large scale of special categories of personal data referred to in Article 11(1) of this Act or of data relating to criminal convictions and offences referred to in Article 12 of this Act; or

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

(4) The Agency shall establish and make publicly available a list of the types of processing operations subject to the obligation to carry out an assessment of the impact on the protection of personal data, in accordance with paragraph (1) of this Article.

(5) The Agency may establish and make publicly available a list of types of processing operations which do not require an impact assessment on the protection of personal data.

(6) The impact assessment shall cover at least:

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

b) an assessment of the necessity and proportionality of the processing related to their purposes;

c) an assessment of the risks to the rights and freedoms of data subjects;

d) envisaged measures to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act, taking into account the rights and legitimate interests of data subjects and other persons involved.

(7) Compliance with the codes of conduct referred to in Article 42 of this Act approved by data controllers or processors shall be taken into account when assessing the impact of processing applied by those data controllers or processors, in particular for the purposes of assessing the impact on the protection of personal data.

(8) The data controller shall, where appropriate, ask the data subject or his or her representative for an opinion on the intended processing, without prejudice to commercial or public interests or the security of processing operations.

(9) Where processing pursuant to Article 8(1)(c) or (e) of this Act has a legal basis in a special law applicable to the data controller, insofar as that law regulates specific processing or a set of operations concerned and where a personal data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of a legal basis, paragraphs (1) to (6) of this Article shall not apply, unless a special regulation stipulates that such an assessment must be carried out prior to processing.

(10) The data controller shall, where necessary, review whether processing has been carried out in accordance with the assessment of the impact on the protection of personal data, at least when there is a change in the level of risk posed by processing operations.

Article 38
(Prior consultation of the data controller with the Agency)

(1) The controller shall consult the Agency prior to processing if the assessment of the impact on the protection of personal data referred to in Article 37 of this Act shows that the processing of data would result in a high risk to the rights and freedoms of natural persons in the absence of measures adopted by the data controller to mitigate the risk.

(2) If the Agency finds that the intended processing referred to in paragraph (1) of this Article would violate this Act, in particular if the data controller has not sufficiently identified or mitigated the risk to the rights and freedoms of individuals, the Agency shall, within a maximum of 56 days of receipt of the request for consultation, provide written advice to the data controller and, where applicable, to the processor, and may exercise the powers referred to in Article 103 of this Act.

(3) If necessary, the period referred to in paragraph (2) of this Article may be extended by 42 days, depending on the complexity of the intended processing.

(4) The Agency shall, within 30 days of receipt of the request, inform the data controller and, where applicable, the processor, of the extension of the time limit referred to in paragraph (3) of this Article and the reasons for the delay.

(5) The deadlines referred to in paragraphs (2) and (3) of this Article may be suspended until the Agency obtains the information it has requested for the purpose of consultation.

(6) When consulting the data controller shall provide the Agency with:

a) where applicable, the respective responsibilities of the data controllers, joint data controllers and processors involved in the processing, in particular in the case of processing within a group of economic operators;

b) the purposes and means of the intended processing;

c) safeguards and other measures to protect the rights and freedoms of data subjects under this Act;

d) the contact details of the data protection officer, where applicable;

e) a data protection impact assessment as provided for in Article 37 of this Act;

f) any other information requested by the Agency.

(7) Before submitting a proposal for a law regulating the processing of personal data to the parliamentary procedure, the proposer may consult the Agency in advance.

(8) Notwithstanding paragraph (1) of this Article, a special law may impose an obligation on the data controller to consult and obtain prior authorisation from the Agency in relation to the processing it performs for the performance of tasks in the public interest, including processing related to social and health protection.

Article 39
(Appointment of a Data Protection Officer)

(1) The data controller and the processor shall designate a personal data protection officer in cases where:

a) the processing is carried out by a public authority, with the exception of courts acting within the limits of their jurisdiction;

b) where the core activities of the data controller or processor consist of processing operations which, by reason of their nature, scope or purposes, require regular and systematic monitoring of a data subject in large numbers; or

c) where the core activities of the data controller or processor consist of processing on a large scale of special categories of data on the basis of Article 11 of this Act and personal data relating to criminal convictions and offences referred to in Article 12 of this Act.

(2) A group of economic operators may appoint a single personal data protection officer, provided that the personal data protection officer is easily accessible from each head office or establishment.

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

(4) In cases other than those referred to in paragraph (1) of this Article, the data controller or processor or association and another body representing a category of data controllers or processors may, or must in cases where required by a special law,

appoint a personal data protection officer. The Data Protection Officer may perform tasks on behalf of these associations and other bodies representing data controllers or processors.

(5) The Personal Data Protection Officer shall be appointed on the basis of his or her professional qualifications and, in particular, his or her professional knowledge in personal data protection law and practice and the ability to perform the tasks referred to in Article 41 of this Act.

(6) The personal data protection officer may be employed by the data controller or processor or may perform tasks on the basis of a service contract.

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

Article 40
(Status of the Data Protection Officer)

(1) The data controller and the processor shall ensure that the personal data protection officer is involved in an appropriate and timely manner in all matters concerning the protection of personal data.

(2) The data controller and the processor shall support the personal data protection officer in performing the tasks referred to in Article 41 of this Act, providing him or her with the necessary means to perform those tasks and gain access to personal data and processing operations, as well as to maintain his or her expert knowledge.

(3) The data controller and the processor shall ensure that the personal data protection officer does not receive any instructions regarding the performance of those tasks. The data controller or processor may not dismiss or penalise him or her for performing his or her tasks. The data protection officer shall report directly to the highest level of management of the data controller or processor.

(4) The data subject may contact the Data Protection Officer for all matters concerning the processing of his or her personal data and the exercise of his or her rights under this Act.

(5) The personal data protection officer, in connection with the performance of his tasks, is obliged to keep all data arising from data processing as an official secret in accordance with the law.

(6) The Data Protection Officer may also perform other tasks and duties. The data controller or processor shall ensure that those tasks and duties do not give rise to a conflict of interest.

Article 41
(Assignment of the Data Protection Officer)

(1) The Data Protection Officer shall perform the following tasks:

a) informing and advising data controllers or processors and employees who perform data processing of their obligations under this Act and other laws regulating the protection of personal data;

b) monitoring compliance with this Act and other laws providing for the protection of personal data, as well as the policies of data controllers or processors in relation to the protection of personal data, including the division of responsibilities, awareness raising and training of employees involved in processing operations, as well as related audits;

c) providing advice, where requested, with regard to the assessment of the impact on the protection of personal data and monitoring its execution in accordance with Article 37 of this Act;

d) cooperation with the Agency;

e) acting as the contact point for the Agency on matters relating to processing, including the prior consultation referred to in Article
38 of this Act, and counselling, as appropriate, on all other matters.

(2) In performing his or her tasks, the Data Protection Officer shall take into account the risk associated with the processing operation and shall take into account the nature, scope, context and purposes of the processing.

Article 42
(code of conduct)

(1) The Agency shall issue a recommendation for the drawing up of a code of conduct with a view to the proper application of this Act, taking into account the specificity of the different processing sectors and the specific needs of micro, small and medium-sized economic operators.

(2) The Association and other entities representing categories of data controllers or processors may draw up codes of conduct, or amend and extend such codes of conduct, for the purpose of specifying the application of this Act, relating to: a) fair and transparent processing;

b) the legitimate interests pursued by the data controller in specific contexts;

c) collection of personal data;

d) pseudonymisation of personal data;

e) informing the public and data holders;

f) the exercise of the rights of the data subject;

g) information and protection of children and the manner of obtaining the consent of the holder of parental authority over the child;

h) measures and procedures referred to in Articles 26 and 27 of this Act, as well as measures to achieve the security of processing referred to in Article 34 of this Act;

i) reporting personal data breaches to the Agency and communicating such breaches to data holders;

j) the transfer of personal data to other countries or international organisations; or

k) out-of-court procedures and other procedures for the settlement of disputes between the data controller and the data subject in relation to processing, without prejudice to the rights of the data subject under Articles 108 and 110 of this Act.

(3) The code of conduct referred to in paragraph (2) of this Article shall contain provisions enabling the legal person referred to in Article 43(1) of this Act to carry out mandatory monitoring of compliance by data controllers or processors who have committed themselves to its application, without prejudice to the competences of the Agency.

(4) The Association and the entity referred to in paragraph (2) of this Article intending to draw up a code of conduct or to amend and extend an existing code of conduct shall submit to the Agency a draft code of conduct or an amendment or extension of a code of conduct.

(5) The Agency shall give an opinion on whether the draft code complies with this Act and shall approve the draft code if it assesses that it provides sufficient appropriate safeguards.

(6) Where the Agency approves a draft code of conduct, or an amendment or supplement to a code of conduct, in accordance with paragraph (5) of this Article, the Agency shall register and publish the code of conduct.

(7) A data controller or processor to which this Act does not apply, in accordance with Article 6 of this Act, may apply a code of conduct approved in accordance with paragraph (5) of this Article, to provide appropriate safeguards in the context of the transfer of personal data to another country or international organisation, subject to the conditions referred to in Article 48, paragraph (2), item d) of this Act.

(8) The data controller or processor referred to in paragraph (7) of this Article shall, by means of contractual or other legally binding instruments, make binding and enforceable commitments to apply the safeguards, including measures relating to the rights of the data subject.

Article 43
(Monitoring of the approved code of conduct)

(1) A legal person with an appropriate level of expertise in the subject matter of a code of conduct may monitor compliance with the code of conduct if it has been accredited for that purpose by an agency.

(2) A legal person referred to in paragraph (1) of this Article may be accredited to monitor compliance with a code of conduct if:

a) it has demonstrated to the Agency its independence and expertise in relation to the subject matter of the code of conduct;

b) establish procedures enabling it to assess the qualification of data controllers and processors to apply the code of conduct, to monitor their application of the provisions of the code of conduct and to periodically review its functioning;

c) put in place procedures and structures to address complaints about breaches of the code of conduct or how the code of conduct has been or has been applied by the data controller or processor and to make those procedures and structures transparent to data holders and the public; and

d) demonstrate to the Agency that its tasks and duties do not give rise to a conflict of interest.

(3) The legal person referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in the event of a breach of the code of conduct by the data controller or the processor, including suspension or exclusion from the code of conduct.

(4) The legal person referred to in paragraph (1) of this Article shall notify the Agency of the actions and reasons referred to in paragraph (3) of this Article.

(5) The Agency shall withdraw accreditation from a legal person that no longer meets the conditions for accreditation or if a legal person violates the provisions of this Act.

(6) This Article shall not apply to the processing of personal data by a public authority.

Article 44
(Certification)

(1) The Agency recommends the establishment of a procedure for certification of personal data protection, data protection seals and marks with the aim of proving compliance with the provisions of this Act, especially taking into account the needs of micro, small and medium-sized legal entities.

(2) The procedure for certification of the protection of personal data, seals and marks may also be established for the purpose of proving the existence of adequate safeguards provided by the data controller and processor to which this Act, in accordance with Article 6 of this Act, does not apply in the context of the transfer of personal data to another country or international organisation, subject to the conditions referred to in Article 48 paragraph (2) item d) of this Act.

(3) The data controllers or processors referred to in paragraph 2 of this Article shall accept, by means of contractual or other legally binding instruments, the application of appropriate safeguards, including in relation to the data subject.

(4) Certification is voluntary and available through a transparent process.

(5) Certification, in accordance with this Article, shall not reduce the responsibility of the data controller or processor for compliance with this Act and shall be without prejudice to the competences of the Agency.

(6) Certification, in accordance with this Article, shall be issued by the certification body referred to in Article 45 of this Act on the basis of criteria approved by the Agency.

(7) The data controller or processor shall, in the certification process, provide the certification body with all the information and give access to the processing activities necessary for the certification process.

(8) The certificate shall be issued to the data controller or processor for a maximum period of three years and may be renewed under the same conditions.

(9) A certification body shall withdraw a certificate from a controller or processor if it no longer meets the conditions for issuing the certificate.

(10) The Agency shall enter the process of certification of the protection of personal data, seals and marks in the records and make it publicly available.

Article 45
(Certification authority)

(1) The Agency shall carry out the accreditation of a certification body with an appropriate level of expertise in the field of personal data protection.

(2) The certification body shall notify the Agency of the decision to issue and renew the certificate so that the Agency can apply the powers referred to in Article 103, paragraph (2), item h) of this Act.

(3) A certification body may be accredited only if:

a) demonstrate to the satisfaction of the Agency its independence and competence in the subject matter of the certification;

b) undertakes to comply with the criteria referred to in Article 44(6) of this Act;

c) establish procedures for the issuance, periodic review and withdrawal of certification, data protection seals and marks;

d) establish procedures and structures to address complaints about breaches of certification or how the certification is or has been applied by the data controller or processor and make those procedures and structures transparent to data holders and the public; e) demonstrates to the Agency that its tasks and duties do not give rise to a conflict of interest.

(4) The accreditation of a certification body shall be carried out on the basis of the criteria laid down by the Agency.

(5) Accreditation shall be issued for a maximum period of five years and may be renewed under the same conditions provided that the certification body continues to comply with the requirements of this Article.

(6) Without prejudice to Part Four of this Act, the Agency shall revoke the accreditation of a certification body if the conditions referred to in paragraph (3) of this Article are not met or are no longer met, or if the actions taken by the certification body violate this Act.

(7) The certification body shall be responsible for the proper assessment leading to certification or withdrawal of certification, without prejudice to the responsibility of the data controller or processor for compliance with this Act.

(8) The certification body shall inform the Agency in writing of the reasons for issuing or withdrawing the certificate.

(9) The Agency shall make publicly available the criteria referred to in Article 44(6) of this Act.

CHAPTER IV TRANSFER OF PERSONAL DATA TO OTHER COUNTRY OR INTERNATIONAL ORGANISATION

Article 46
(General principles for transfers)

Any transfer of personal data in the course of processing or intended for further processing after its transfer to another country or international organisation may take place only if such transfer complies with the provisions of this Act, including the onward transfer of personal data from another country or international organisation to another country or international organisation.

Article 47
(Transfer based on adequacy of the level of protection of personal data)

(1) The transfer of personal data to another country, to a part of its territory or to one or more sectors within that country, or to an international organisation may take place where it is established that that other country, part of its territory or one or more sectors within that country, or that international organisation ensures an adequate level of protection of personal data.

(2) An adequate level of protection as referred to in paragraph 1 of this Article shall be deemed to be ensured in a country, parts of its territory or one or more sectors thereof, or an international organisation which the European Union has determined ensures an adequate level of protection for personal data.

(3) The decision on the adequacy of the level of protection of personal data referred to in paragraph (1) of this Article shall be adopted by the Council of Ministers of Bosnia and Herzegovina on the proposal of the Agency.

(4) The Agency shall prepare a proposal for the decision referred to in paragraph (3) of this Article taking into account:

a) the principle of the rule of law, respect for human rights and fundamental freedoms, sectoral legislation, including legislation on public security, defence, State security, criminal law and access to personal data by public authorities, as well as the application of such legislation, rules on the protection of personal data, professional rules and measures to ensure the protection of personal data, including rules on the onward transfer of personal data to another country or international organisation which are applied in the practice of courts and other authorities in another country or international organisation, as well as the effectiveness of the exercise of the rights of the data subject, in particular the effectiveness of administrative and judicial procedures for the protection of the rights of the data subject;

b) the existence and effectiveness of the work of a supervisory authority in another country or an authority competent for an international organisation in this field, with the power to ensure the application of personal data protection rules and initiate

procedures for the protection of personal data in the event of their non-compliance, to provide assistance and advice to the holders of personal data in the exercise of their rights, as well as to cooperate with the supervisory authorities of other countries;

c) international obligations entered into by another country or international organisation, or other obligations arising from legally binding international treaties or other legal instruments, as well as membership of multilateral or regional organisations, in particular in relation to the protection of personal data.

(5) The Agency shall continuously monitor the situation in the field of personal data protection in another country, part of its territory, one or more sectors within that country or an international organisation and report thereon to the Council of Ministers of Bosnia and Herzegovina as appropriate.

(6) The report referred to in paragraph (5) of this Article shall include available information and information collected from international organisations relevant to the review of the existence of an adequate level of protection of personal data, on the basis of which the Council of Ministers of Bosnia and Herzegovina shall adopt the decision referred to in paragraph (3) of this Article.

(7) A decision taken pursuant to paragraph (3) of this Article shall be without prejudice to the transfer of personal data to another country, to a territory or to one or more specified sectors within that other country or to an international organisation pursuant to Article 48. 51 of this Act.

(8) The list of countries, part of their territory, one or more sectors within the country and international organizations, for which the Council of Ministers of Bosnia and Herzegovina has decided that they do not ensure or no longer ensure an adequate level of protection of personal data, is published in the "Official Gazette of BiH" and on the official website of the Agency.

Article 48
(Transfer subject to appropriate safeguards)

(1) The data controller or processor may transfer personal data to another country, a part of its territory, to one or more sectors within that country or to an international organisation for which the list referred to in Article 47(8) of this Act does not determine the existence of an adequate level of protection of personal data only if the data controller or processor has ensured appropriate safeguards for that data and if the holder of the personal data is provided with enforceable rights and effective judicial protection.

(2) Appropriate safeguards referred to in paragraph 1 of this Article may be provided, without specific authorisation

from the Agency, for: a) a legally binding act drawn up between public authorities;

b) binding business rules in accordance with Article 49 of this Act;

c) an approved code of conduct pursuant to Article 42 of this Act with binding and enforceable obligations on the data controller or processor in another country to apply appropriate safeguards, including as regards the rights of the data subject; or

d) an approved certification procedure in accordance with Article 44 of this Act with binding and enforceable obligations on data controllers or processors in another country to apply appropriate safeguards, including as regards the rights of data holders.

(3) Appropriate safeguards referred to in paragraph 1 of this Article may be provided by standard contractual clauses on data protection adopted by the Agency.

(4) Subject to the approval of the Agency, appropriate safeguards referred to in paragraph 1 of this Article may also be specifically provided for:

a) a contract between the data controller or the processor and the data controller, the processor or the recipient of the personal data to another country or international organisation; or

b) provisions which shall be inserted into agreements between public authorities and which contain enforceable and effective rights for data subjects.

Article 49
(Binding Business Rules)

(1) Binding business rules shall specify at least:

a) the structure and contact details of the group of economic operators engaged in a joint economic activity and of each of its members;

b) data transfers or sets of transfers, specifying the category of personal data, the type of processing and its purposes, the categories of data holders and the designation of the other country or countries concerned;

c) their legally binding nature;

d) the application of data protection principles, in particular purpose limitation, data minimisation, retention period limitation, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to achieve data security and conditions in relation to onward transfers to bodies not bound by binding business rules;

e) the rights of the data subject in relation to the processing and the means of exercising those rights, including the right not to be subject todecisions based solely on automated processing, including profiling in accordance with Article 24 of this Act, the right to object to the Agency and the right to judicial protection, in accordance with Article 110 of this Act, and, in appropriate cases, the right to compensation for breaches of binding business rules;

f) that the data controller or processor based or established on the territory of Bosnia and Herzegovina accepts responsibility for any breach of the binding business rules from any member not based or established in Bosnia and Herzegovina or exempted the data controller or processor from liability in whole or in part if it proves that that member of the group of economic operators is not responsible for the event giving rise to the damage;

g) how, in addition to the information referred to in Articles 15 and 16 of this Act, information on binding business rules, in particular the provisions referred to in points d), e) and f) of this paragraph, is provided to data subjects;

h) the tasks of any data protection officer appointed in accordance with Article 39 of this Act or any other person or entity responsible for monitoring compliance with binding business rules in a group of economic operators engaged in a joint economic activity, as well as monitoring training and handling complaints; opposition proceedings;

j) the mechanisms within the group of economic operators carrying out a joint economic activity to ensure the verification of compliance with the binding business rules, including data protection auditing and methods to ensure corrective measures to protect the rights of data holders. The results of such verification shall be communicated to the person or entity referred to in point (h) of this paragraph and to the management body of the group of economic operators carrying out a joint economic activity and shall be made available to the Agency upon request;

k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the Agency;

l) the cooperation mechanism with the Agency to ensure compliance by each member of a group of economic operators engaged in a joint economic activity, in particular by making available to the Agency the results of the verifications of the measures referred to in point j) of this paragraph;

m) the mechanisms for reporting to the Agency any legal obligations relating to a member of a group of economic operators engaged in a joint economic activity and applicable in another country which are likely to have a significant adverse effect on the guarantees contained in the binding business rules;

n) appropriate training on personal data protection for staff with permanent or regular access to personal data.

(2) Binding business rules shall be approved by the Agency provided that:

a) are legally binding and apply to and apply to any interested member of a group of economic operators engaged in a joint economic activity, including their employees;

b) expressly grant data subjects enforceable rights in relation to the processing of their personal data;c) meet

the conditions referred to in paragraph (1) of this Article.

(3) The Agency may specify the format and procedures for the exchange of information between data controllers, processors and the Agency for binding business rules within the meaning of this Article.

Article 50
(Transfer or disclosure of information that is not allowed)

Any judgment of a court, tribunal or decision of an administrative authority of another country requiring a data controller or processor to transfer or disclose personal data may only be recognised or implemented if it is based on an international agreement, such as a mutual legal assistance agreement, between the other requesting country and Bosnia and Herzegovina, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 51
(Derogation in specific cases)

(1) A transfer or set of transfers of personal data to another country or international organisation, in the absence of an adequacy decision pursuant to Article 47(3) of this Act or appropriate safeguards pursuant to Article 48 of this Act, including binding business rules referred to in Article 49 of this Act, shall be carried out only on one of the following conditions:

a) the data subject expressly agrees to the proposed transfer, after having become aware of the potential risks of such transfers due to the absence of an adequacy decision and appropriate safeguards referred to in Article 48 of this Act;

b) the transfer is necessary for the performance of a contract between the data subject and the data controller or the performance of pre-contractual measures at the request of the data subject;

c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and another natural or legal person;

d) the transfer is necessary for essential reasons of public interest;

e) the transfer is necessary for the establishment, exercise or defence of legal claims;

f) the transfer is necessary to protect the essential interests of the data subject or of other persons where the data subject is physically or legally incapable of giving consent;

g) the transfer is made from a register which, according to legal regulations in Bosnia and Herzegovina, serves to provide information to the public and which is available for inspection by the public or any person who can prove the existence of a

legitimate interest, but only to the extent that the conditions prescribed by a special law for inspection in that particular case are met.

(2) A transfer or set of transfers of personal data to another country or international organisation where the basis for the transfer may be Art. 47 or 48 of this Act, including the binding business rules referred to in Article 49 of this Act, and where no derogation applies in the specific cases referred to in paragraph 1 of this Article, may be carried out only if the transfer is not repetitive, relates only to a limited number of data subjects and is necessary for the purposes of the essential, legitimate interests of the data controller over which the interests or rights and freedoms of the data subject do not prevail, and the data controller has assessed all the circumstances surrounding the data transfer and on the basis of that assessment has provided appropriate safeguards with regard to the protection of personal data. The controller shall inform the Agency of the transfer. In addition to the information referred to in Articles 15 and 16 of this Act, the data controller shall inform the data subject of the transfer and of important legitimate interests.

(3) A transfer pursuant to point (g) of paragraph 1 of this Article shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only if those persons so request or if they are the recipients.

(4) Paragraphs (1) (a), (b) and (c)(2) of this Article shall not apply to activities carried out by public authorities in the exercise of their public powers.

(5) The public interest referred to in paragraph (1), point d) of this Article must be prescribed by the law applicable to the data controller.

(6) In the absence of an adequacy decision, for essential reasons of public interest, a special regulation may expressly provide for restrictions on the transfer of certain categories of personal data to another country or international organisation.

(7) The data controller or processor shall document the assessment, as well as the appropriate safeguards referred to in paragraphs (1) and (2) of this Article, of the records referred to in Article 32 of this Act.

CHAPTER V SPECIAL PROCESSING CASE

Article 52
(Processing of personal data and freedom of expression and information)

(1) The processing of personal data in the exercise of the right to freedom of expression and information, which includes processing solely for monetary purposes, for the purposes of academic, artistic or literary expression, is carried out in accordance with special regulations.

(2) The special regulations referred to in paragraph (1) of this Article shall establish exceptions or derogations from the application of Chapter I, Chapter II, Chapter III, Chapter IV, Chapter V of this Part and Part Four of this Act, where such exceptions or derogations are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

Article 53
(Processing of personal data and public access to official documents)

(1) The public authority and the competent authority may, in accordance with the law applicable to that authority, disclose, in the public interest, personal data contained in official documents held by them in order to reconcile public access to official documents with the right to the protection of personal data in accordance with this Act.

(2) This Act shall apply in the application of the regulations on freedom of access to information in Bosnia and Herzegovina.

Article 54
(Processing of the unique identification number of a natural person)

(1) Specific conditions for the processing of the unique identification number of a natural person or any other identifier of general application shall be laid down by a special law.

(2) The unique registration number of a natural person or any other identifier of general application referred to in paragraph (1) of this Article shall be processed only subject to appropriate safeguards for the rights and freedoms of the data subject in accordance with this Act.

Article 55
(Processing of personal data in the employment context)

(1) A specific law or collective agreement shall specify rules aimed at ensuring the protection of rights and freedoms in relation to the processing of personal data in the employment context, in particular for the purposes of employment, the enforcement of employment contracts, including the fulfilment of obligations laid down by law or collective agreements, for the purposes of management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, the protection of employer's or customer's property and for the purposes of the individual or collective exercise and enjoyment of rights and benefits from an employment relationship, as well as for the purposes of the termination of an employment relationship.

(2) The rules referred to in paragraph 1 of this Article shall include appropriate and specific measures to protect the human dignity of the data subject, his or her legitimate interests and fundamental rights, in particular with regard to transparency of processing, the transfer of personal data within a group of economic operators or a group of economic operators carrying out a joint economic activity, as well as monitoring systems at the workplace.

Article 56
(Safeguards and derogations concerning the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes)

(1) The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall be subject to appropriate safeguards in accordance with this Act with respect to the rights and freedoms of the data subject.

(2) The safeguards referred to in paragraph 1 of this Article shall ensure the application of technical and organisational measures, in particular those ensuring the application of the principle of data minimisation, which may include pseudonymisation, where the purposes can be achieved in this way.

(3) If the purposes referred to in paragraph 1 of this Article can be achieved by further processing which does not allow or no longer allowsidentification of the data subject, those purposes shall be achieved in that manner.

(4) Where personal data are processed for scientific or historical research purposes or statistical purposes, only a special law may provide for derogations from the rights referred to in Articles 17, 18, 20 and 23 of this Act, subject to the conditions and safeguards referred to in paragraph (1) of this Article, if it is likely that those rights could prevent or seriously jeopardise the achievement of those specific purposes and such derogations are necessary to achieve those purposes.

(5) Where personal data are processed for archiving purposes in the public interest, only a special law may provide for derogations from the rights referred to in Articles 17, 18, 20, 21, 22 and 23 of this Act, subject to the conditions and safeguards referred to in paragraph (1) of this Article, if those rights are likely to prevent or seriously jeopardise the achievement of that specific purpose and such derogations are necessary to achieve that purpose.

(6) Where the processing referred to in paragraphs (2) and (3) of this Article serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Article 57
(Video surveillance)

(1) Monitoring of a specific area via video surveillance is allowed only if it is necessary for the protection of persons and property and if the interests of the data subject do not prevail.

(2) Video surveillance may only cover premises or parts of premises the surveillance of which is necessary to achieve the purpose referred to in paragraph
(1) of this article.

(3) The establishment of video surveillance of publicly accessible facilities of large areas, such as sports facilities, entertainment centres, shopping centres or parking lots or public transport vehicles, shall be permitted solely for the purpose of protecting the life, health and freedom of a person and property.

(4) The data controller using video surveillance is obliged to make a decision that will contain the rules of processing in order to respect the right to protection of privacy and personal life of the data subject, if video surveillance is not prescribed by law.

(5) The data controller or processor shall prominently display the video surveillance tag. The video surveillance tagcontains the following information: that the space is under video surveillance, data on the data controller or processor and contact details through which the data subject can exercise his rights. The mark shall be visible at the latest when entering the field of view of the recording.

(6) The data controller or processor shall, in the video surveillance system of publicly accessible facilities referred to in paragraph (3) of this Article, record records of the use of the system and keep them for at least 12 months. Records make it possible to determine the date and time and the identity of the person who accessed the video surveillance system.

(7) The establishment of video surveillance in residential or commercial-residential buildings requires the consent of co-owners who make up at least 2/3 of the co-ownership parts. Video surveillance may only cover access to and exit from a residential building and common areas in residential buildings.

(8) Monitoring of public spaces by video surveillance for the purposes referred to in Article 1, paragraph (1), item c) of this Act is allowed only if it is prescribed by a special law.

Article 57a
(Processing of biometric data for the purpose of secure identification)

(1) The processing of biometric data may only take place if it is required by law or if it is necessary for the protection of the person, property, classified information, trade secrets or for the individual and secure identification of the service user, taking into account that the interests of the data holder which conflict with the processing of biometric data referred to in this Article do not prevail.

(2) The legal basis for the processing of biometric data of the data subject, for the secure identification of service users, is the explicit consent of such data subject given in accordance with the provisions of this Act.

Article 57b
(Processing of biometric data in offices)

The processing of employees' biometric data for the purpose of recording working time and for the purpose of entering and leaving official premises shall be allowed, if required by law or if such processing is carried out as an alternative to another solution for recording working time or entering and leaving official premises, provided that the employee has given explicit consent for such processing of biometric data in accordance with the provisions of this Act.

Article 58
(Existing rules on the protection of personal data of churches and religious communities)

(1) Where churches and religious communities apply comprehensive rules regarding the processing of personal data, those existing rules may continue to apply provided that they comply with this Act.

(2) Churches and religious communities that apply comprehensive rules shall be supervised by the Agency, unless the church or religious community establishes a special independent supervisory body, provided that it meets the conditions laid down in Part Four of this Act.

Article 59
(Obligation of professional secrecy)

(1) A special regulation may lay down a limitation of the Agency referred to in Article 103(1)(f) and (g) in respect of controllers of data or processors who, on the basis of a special regulation adopted by a competent authority, are subject to an obligation of professional secrecy and other equivalent obligations of secrecy, where this is necessary and proportionate to reconcile the right to the protection of personal data with the obligation of secrecy.

(2) The special regulation referred to in paragraph 1 of this Article shall apply only to personal data which the data controller or processor has obtained as a result of or received in the course of an activity covered by the obligation of confidentiality.

PART THREE — PROCESSING PERSONAL DATA FROM THE COMPETENT AUTHORITY AS A DATA CONTROL IN PURPOSE PREVENTION, RESEARCH AND DISCOUNT OF PERFORMANCE PARTS OR PERFORMANCE OF PERFORMERS OF PERFORMANCE PARTS, EXECUTIVENESS INTERESTED SANCTIONS, INCLUDING PROTECTION FROM THE PROTECTION OF PUBLIC SAFETY AND THEIR PREVENTION

Article 60
(Principles of processing of personal data by the competent authority)

(1) The principles governing the processing of personal data by the competent authority are:

a) legality and fairness;

b) purpose limitation – data must be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;

c) data minimisation – data must be adequate, relevant and limited to what is necessary for the purposes for which they are processed;

d) accuracy – the data must be accurate and, where necessary, kept up to date, all reasonable steps must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) retention limitation – the data must be kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data are processed;

f) integrity and confidentiality – data must be processed in such a way as to ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

(2) Processing carried out by the same or another competent authority for the purposes referred to in Article 1(1)(c) of this Act other than that for which the personal data have been collected shall be permitted:

a) the competent authority is authorised to process such personal data for such a purpose in accordance with a special

regulation or b) the processing is necessary and proportionate to another legitimate purpose.

(3) Processing by the same or another competent authority may include archiving in the public interest, scientific, statistical or historical purposes, for the purposes referred to in Article 1(1)(c) of this Act, subject to appropriate safeguards for the rights and freedoms of the data subject.

(4) The competent authority shall be responsible for, and be able to demonstrate, compliance with paragraphs (1), (2) and (3) of this Article.

Article 61
(Deadline for storing and deleting personal data)

(1) The deadline for the deletion of personal data or for the periodic review of the need for their storage is prescribed by a special law.

(2) The competent authorities shall establish rules and procedures to ensure compliance with the time limit referred to in paragraph (1) of this Article.

Article 62
(Difference between different categories of data holders)

The competent authority shall, where appropriate and where possible, make a clear distinction between personal data of different categories of data holders, such as:

a) a person in respect of whom there are grounds for suspecting that he or she has

committed or intends to commit a criminal offence; b) a person convicted of criminal

offences;

c) a person who has been the victim of a criminal offence or in respect of whom there are certain facts giving rise to a suspicion that that person may be the victim of a criminal offence;

d) a person who is associated with a criminal offence, such as a person who may be called to testify in investigations or subsequent criminal proceedings, a person who can provide information on criminal offences, or a contact person or associates of the persons referred to in points (a) and (b) of this paragraph.

Article 63
(Difference between personal data and verification of the quality of personal data)

(1) The competent authority shall establish a mechanism to ensure that personal data based on bills of exchange are distinguished, as far as possible, from personal data based on personal assessments.

(2) The competent authority shall take all reasonable measures to ensure that personal data that are inaccurate, incomplete or not up to date are not transmitted or made available. The competent authority shall, where possible, verify the quality of the personal data before they are transmitted or made available. Whenever personal data are transmitted, as far as possible, the necessary information shall be provided to the receiving competent authority, it shall be possible to assess the degree of accuracy, completeness and reliability of the personal data, as well as the extent to which they are up to date.

(3) If it is established that incorrect personal data have been transmitted or that personal data have been unlawfully transmitted, the competent authority must inform the recipient without delay. In this case, personal data must be corrected or deleted or the processing restricted in accordance with Article 72 of this Act.

Article 64
(Lawfulness of the processing of personal data by the competent authority)

(1) The processing of personal data by the competent authority shall be lawful only if it is necessary and only to the extent that it is necessary for the performance of the tasks of the competent authority for the purposes referred to in Article 1(1)(c) of this Act and if it is prescribed by a special law.

(2) The special law referred to in paragraph 1 of this Article shall prescribe at least the purposes of the processing, the personal data being processed and the purposes of the processing.

Article 65
(Specific processing conditions)

(1) Personal data collected by the competent authority for the purposes set out in Article 1, paragraph (1), item c) of this Act may not be processed for other purposes, unless such processing is prescribed by a special law, in which case the provisions of this Part of the Act shall not apply.

(2) Where a special law entrusts the competent authority with the performance of tasks other than those performed for the purposes referred to in Article 1(1)(c) of this Act, the provisions of this Part of the Act shall not apply, including for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

(3) Where specific conditions for processing are laid down in a specific law relating to the transmitting competent authority, the transmitting competent authority shall inform the recipient of those conditions and of the requirements to comply with those conditions.

Article 67
(Automated individual decision-making by the competent authority)

(1) The competent authority shall be prohibited from taking decisions solely on the basis of automated processing, including profiling, which produces adverse legal effects concerning the data subject or significantly affects him or her, unless authorised by a specific law providing for appropriate safeguards for the rights and freedoms of the data subject, at least the right for a natural person to participate in the decision-making.

(2) The decision referred to in paragraph (1) of this Article may not be based on special categories of personal data referred to in Article 66 of this Act, unless appropriate measures are in place to protect the rights and freedoms and legitimate interests of the data subject.

(3) The competent authority shall be prohibited from profiling that results in discrimination against persons on the basis of special categories of personal data referred to in Article 66 of this Act.

Article 68
(Information and how to exercise the rights of the data subject)

(1) The competent authority shall take all appropriate measures to provide the data subject with all the information referred to in Article 69 of this Act and to make all notifications with regard to Article 67, Article 70 of the GDPR. – 74 and Article 87 of this Act in relation to processing.

(2) The information referred to in paragraph 1 of this Article shall be provided in a concise, intelligible and easily accessible form, using clear and plain language.

(3) The information referred to in paragraph (1) of this Article shall be provided to the data subject in the form in which the request is made or in the manner indicated in the request, within 30 days from the date of the submission of the request.

(4) The competent authority shall facilitate the exercise of the rights of data subjects referred to in Articles 67 and 70. 74 of this Act.

(5) The competent authority shall inform the data subject in writing of any follow-up given to his or her request without delay.

(6) The competent authority shall, free of charge, provide information or take measures pursuant to Article 69 of this Act, as well as any information provided or measures taken pursuant to Article 67, Article 70. – 74 of this Act and Article 87 of this Act.

(7) Where a request from a data subject is manifestly unfounded or excessive, in particular because of its repetitive character, the competent authority may:

a) charge a fee for actual administrative costs, such as copying, scanning or data carrier costs, as well as reimbursement of the costs of delivering or taking the requested action; or

b) refuse to act on the request.

(8) The burden of demonstrating that the request referred to in paragraph (7) of this Article is manifestly unfounded or excessive shall be on the competent authority.

(9) Where the competent authority has reasonable doubt as to the identity of the natural person making the request referred to in Articles 70 or 72 of this Act, the competent authority may request additional information necessary to confirm the identity of the data holder.

Article 69
(Information made available or provided to the data holder)

(1) The competent authority shall make available to the data holder as a minimum the following information:

a) the identity and contact details of the competent authority;

b) the contact details of the personal data protection officer, where applicable;

c) the purpose of the processing of personal data;

d) the right to lodge a complaint with the Agency and the contact details of the Agency or to bring an action before the competent court;

e) of the existence of the right to request from a competent authority access to and rectification or erasure of personal data or restriction of processing of personal data.

(2) In addition to the information referred to in paragraph 1 of this Article, for the purposes of exercising its rights, the competent authority shall provide the data subject with the following additional information:

a) the legal basis for the processing of personal data;

b) the period within which the personal data will be kept or, where that is not possible, the criteria used to determine that period;

c) the categories of recipients of the personal data, including other countries or international organisations, where applicable;

d) where necessary, additional information where the personal data are collected without the knowledge of the data subject.

(3) A specific law may provide for measures to delay, restrict or withhold the provision of the information referred to in paragraph 2 of this Article to the data subject to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society, with due regard for the fundamental rights and the legitimate interests of the data subject, in order to:

a) preventing obstruction of official and regulated information gathering, investigations or procedures;

b) avoiding obstructing the prevention, investigation and detection of criminal offences or the prosecution of criminal offences or the execution of criminal penalties;

c) the protection of public security;

d) the protection of national security;

e) Protecting the rights and freedoms of others.

(4) A special law may prescribe categories of processing which may, in whole or in part, be covered by any of the points referred to in paragraph (3) of this Article.

Article 70
(Data subject's right of access to personal data by the competent authority)

(1) The competent authority shall, within 30 days of receipt of a request for access to personal data, issue a confirmation to the data subject as to whether or not personal data concerning him or her are being processed and, where that is the case, access to personal data and information on:

a) the purpose of the processing and the legal basis for the processing;

b) the category of personal data processed;

c) the recipient or category of recipients to whom the personal data have been disclosed, in particular a recipient in another country or an international organisation;

d) the envisaged period within which the personal data will be stored where possible or, where that is not possible, the criteria used to set that period;

e) the existence of the right to request from a competent authority rectification or erasure of personal data or restriction of processing of personal data;

f) the right to lodge a complaint with the Agency and the contact details of the Agency or to bring an action before the competent court;

g) the personal data undergoing processing and any available information as to the source of the personal data.

(2) The certificate referred to in paragraph (1) of this Article shall be issued in accordance with the provisions of Article 71 of this Act.

Article 71
(Restriction of the right of access to personal data)

(1) A specific law concerning a competent authority may restrict, wholly or partly, the data subject's right of access to personal data to the extent that, and for as long as, such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society, while respecting the fundamental rights and legitimate interests of the data subject, in order to:

a) prevent obstruction of official or regulated information gathering, investigations or procedures;

b) avoid obstructing the investigation and detection of criminal offences or the prosecution of criminal offences or the execution of criminal penalties;

c) protect public security;

d) protect national security;

e) protect the rights and freedoms of others.

(2) A special law may specify categories of processing which may, in whole or in part, be covered by any of the points referred to in paragraph (1) of this Article.

(3) In the cases referred to in paragraphs (1) and (2) of this Article, the competent authority shall, without delay, inform the data holder in writing of any refusal or restriction of access to personal data and of the reasons for the refusal or restriction, unless providing such information would jeopardise one of the purposes referred to in paragraph (1) of this Article.

(4) The competent authority shall inform the data subject of the possibility of lodging a complaint with the Agency or bringing an action before the competent court.

(5) The competent authority shall document the factual or legal reasons on which the decision is based.

(6) The documentation referred to in paragraph (5) of this Article shall be made available to the Agency.

Article 72
(Right to rectification or erasure of personal data and restriction of processing by a competent authority)

(1) The competent authority shall:

a) without undue delay, allow the data subject to rectify inaccurate personal data relating to him or her.Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement;

b) allow the data subject to delete personal data without undue delay if the processing violates the provisions of Articles 60, 64 or 66 of this Act or if the personal data must be deleted in order to comply with a legal obligation under a special law; c) restrict processing if:

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

2) personal data must be retained as evidence;

d) inform the data subject before removing the restriction of processing where processing is restricted pursuant to point (c)(i) of this paragraph;

e) inform the data subject in writing of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal. A specific law concerning a competent authority may restrict, wholly or partly, the data subject's right of access to the extent that, and for as long as, such a complete or partial restriction constitutes a necessary and proportionate measure in a democratic society, while respecting the fundamental rights and legitimate interests of the data subject, in order to:

1) avoid obstructing the official or statutory collection of information, investigations or procedures;

2) avoid obstructing the prevention, investigation and detection of criminal offences or the prosecution of criminal offences or the execution of criminal penalties;

3) protect public safety,

4) protect national security,5) protect the rights and freedoms of others;

f) inform the data subject of the possibility of lodging a complaint with the Agency or bringing an action before the competent court;

g) notify the competent authority from which the inaccurate personal data originates of the correction of the incorrect personal data.

(2) The competent authority shall, where personal data have been rectified or erased or processing has been restricted pursuant to paragraph 1, be obliged to do so.
a), b) or c) of this Article, inform recipients, and recipients are obliged to correct or delete personal data or restrict the processing of personal data within the limits of their responsibility.

Article 73
(Exercise of rights by data subjects and verification by the Agency)

(1) The competent authority shall inform the data subject of the possibility of exercising his or her rights by way of a complaint to the Agency or to the competent court.

(2) If the data subject is dissatisfied with the procedure of the competent authority, he or she may file a complaint with the Agency or bring an action before the competent court in the cases referred to in Article 69(3), Article 71(3) and Article 72(1) point d) of this Act.

(3) In the case referred to in paragraph (1) of this Article, the Agency shall inform the data subject that checks by an inspector have been carried out and of the right to a judicial remedy.

Article 74
(Rights of data subjects in criminal investigations and proceedings)

The data subject shall exercise the rights referred to in Articles 69, 70 and 72 of this Act in accordance with the laws on criminal proceedings where personal data contained in a judicial decision or in a record or case file have been processed in the course of criminal investigations and proceedings.

Article 75
(Obligation of the competent authority)

(1) The competent authority shall apply appropriate technical and organisational measures having regard to the nature, scope, circumstances of the execution of the processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, in order to ensure and be able to demonstrate the performance of processing in accordance with this Act. Those measures shall be reviewed and updated as necessary.

(2) Where the measures referred to in paragraph 1 of this Article are proportionate in relation to processing activities, they shall include the implementation of appropriate data protection policies by the competent authority.

Article 76
(Personal data protection by design and by default from the competent authority)

(1) The competent authority shall, taking into account the state of the art and the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity for the rights and freedoms of persons posed by the processing, both at the time of the determination of the means for processing and at the time of the processing itself, apply appropriate technical and organisational measures, such as pseudonymisation, to enable the effective application of data protection principles, such as data minimisation and the integration of safeguards in the processing, in order to meet the requirements of this Act and protect the rights of data subjects.

(2) The measures referred to in paragraph 1 of this Article shall refer to the amount of personal data collected, the scope of their processing, the time limit for their preservation and their availability, which ensures that personal data are not automatically, without the intervention of a natural person, accessible to an unlimited number of persons.

Article 77
(Competent authority as joint data controller)

(1) Where two or more competent authorities determine the purposes and means of the processing of personal data, they shall be considered to be joint controllers of the data. They shall determine in a transparent manner by mutual agreement the responsibilities of each of them in order to fulfil the obligations under this Act, in particular as regards the exercise of the rights of data subjects and the duties of each of them to provide the information referred to in Article 69 of this Act, unless the responsibilities of the competent authorities are determined by the law applicable to those competent authorities. The agreement shall designate a contact point for data holders. The law may specify which of the joint data controllers may act as a single point of contact for the exercise of the rights of the data subject.

(2) Notwithstanding the terms of the agreement referred to in paragraph (1) of this Article, the data subject may exercise his or her rights under this Act in relation to and against each of the competent authorities.

Article 78
(Using the service of the processor by the competent authority)

(1) The competent authority shall use the service only of the processor who can sufficiently ensure that the appropriate technical and organisational measures prescribed by this Act are implemented.

(2) The use of the processor's service by the competent authority shall be governed by a contract or other legal act governing the subject matter, technical and organisational measures prescribed by this Act, the duration of the processing, the scope, content and purpose of the processing, the type of personal data, the categories of data subjects and the obligations and rights of the competent authority, as well as that the processor:

a) act only on the instructions of the competent authority;

b) ensure that persons authorised to process the personal data have committed themselves to confidentiality or are subject to legal provisions on confidentiality;

c) assist the competent authority, by any appropriate means, in ensuring compliance with the provisions concerning the rights of data holders;

d) at the choice of the competent authority, deletes or returns all personal data to the competent authority after the end of the provision of data processing services and deletes existing copies, unless there is a legal requirement to store personal data;

e) make available to the competent authority all information necessary to comply with the provisions of this Article;

f) complies with the provisions of paragraph (3) of this Article for engaging another processor.

(3) The processor may not use the service of another processor without the prior written authorisation of the competent authority.

(4) Upon receipt of the authorisation, the processor shall notify the competent authority of any intended changes concerning the use of the service of other processors.

(5) The competent authority may refuse the consent of the processor to use the service of another processor.

(6) Where a processor determines the purposes and means of processing in breach of the provisions of this Act, that processor shall be deemed to be the competent authority in respect of the processing entrusted to it.

Article 79
(Processing under the supervision of the competent authority)

A person acting under the supervision of a competent authority or a processor who has access to personal data shall not process those data without the order of the data controller, except where required by a specific law.

Article 80
(Records of processing by the competent authority)

(1) The competent authority shall keep records of the processing for which it is responsible. That record shall contain the following information:

a) the name and contact details of the competent authority, the joint competent authority and the personal data

protection officer; b) the purpose of the processing;

c) the category of recipients to whom the personal data have been or will be disclosed, including a recipient in another country or international organisation;

d) a description of the category of the data subject and of the categories of personal data;

e) the use of profiling, where applicable;

f) the category of transfers of personal data to another country or international organisation, where applicable;

g) the legal basis for the processing operation, including transfers, for which the personal data are intended;

h) the envisaged time limits for erasure of different categories of personal data, where possible;

i) a general description of the technical and organisational security measures referred to in Article 85(1) of this Act, where possible.

(2) The competent authority shall ensure that each processor keeps a record of all categories of processing activities carried out on behalf of the data controller, containing:

a) the name and contact details of the processor or processors and of each data controller on behalf of which the processor is acting, and of the data protection officer, where applicable;

b) the category of processing carried out for each data controller;

c) where applicable, data concerning the transfer of personal data to another country or international organisation, where there is an explicit instruction from the data controller to that effect, including the identification of that other country or international organisation;

d) where possible, a general description of the technical and organisational security measures referred to in Article 85(1) of this Act.

(3) The records referred to in paragraph (1) of this Article shall be in writing, including in electronic form.

(4) At the request of the Agency, the competent authority shall make the records available for inspection.

Article 81
(Record)

(1) The competent authority shall, in the case of an automated personal data-processing system, establish access to a system which shall automatically record at least the following information: collection, alteration, consultation, disclosure, including transfers, and combination and erasure. Records of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, where possible, the identity of the person who consulted or disclosed personal data and the identity of the recipients of such personal data.

(2) The log shall be used only for the purposes of verifying the lawfulness of the processing, self-monitoring and ensuring the integrity and security of personal data, and for criminal proceedings.

(3) The competent authority shall, at the request of the Agency, make the records available for inspection.

Article 82
(Cooperation of the competent authority and the processor with the Agency)

The competent authority and the processor shall cooperate with the Agency, on a reasoned and legally justified request, in the exercise of its competence.

Article 83
(Assessment of the impact on the protection of personal data from the competent authority)

(1) The competent authority shall, prior to the processing, assess the impact of the envisaged processing operations on the protection of personal data where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of that processing, is likely to result in a high risk to the rights and freedoms of persons.

(2) The assessment referred to in paragraph 1 of this Article shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of the data subject, the envisaged risk measures, safeguards and security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act, taking into account the rights and legitimate interests of the data subject and other persons concerned.

Article 84
(Prior consultation of the Agency by the competent authority)

(1) The competent authority or the processor shall consult the Agency prior to the processing of personal data to be included in a new personal data collection where:

a) a data protection impact assessment, as provided for in Article 83 of this Act, indicates that the processing could result in a high risk if the competent authority does not take measures to mitigate the risk; or

b) the type of processing, in particular where new technologies, mechanisms or procedures are applied, poses a high risk to the rights and freedoms of data holders.

(2) The Agency may establish a list of processing operations which are subject to prior consultation pursuant to paragraph 1 of this Article.

(3) The competent authority shall provide the Agency with a data protection impact assessment pursuant to Article 83 of this Act and shall provide the Agency with any other information necessary to enable the Agency to assess the compliance of the processing, in particular the risks to the protection of personal data of the data subject and the related safeguards.

(4) Within 42 days of receipt of the written request referred to in paragraph (1) of this Article, the Agency shall provide written advice to the competent authority and may use any of its powers if it considers that the intended processing referred to in paragraph (1) of this Article would infringe the provisions of this Act, in particular if the competent authority has not sufficiently identified or mitigated the risk.

(5) The period referred to in paragraph (4) of this Article may be extended by 30 days where necessary, taking into account the complexity of the intended processing.

(6) Within 30 days of receipt of the request, the Agency shall inform the competent authority and, where applicable, the processor, of any extension and the reasons for the delay.

(7) The proposer may consult the Agency before submitting the draft law regulating the processing of personal data to the parliamentary procedure.

Article 85
(Safety of processing by competent authority and processor)

(1) The competent authority and the processor shall, taking into account the state of the art, the costs of implementation, the nature, scope, context of execution of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, apply appropriate technical and organisational measures to achieve an appropriate level of security appropriate to the risk, in particular as regards the processing of special categories of personal data.

(2) With regard to automated processing, the competent authority or the processor shall, following a risk assessment, put in place measures to ensure that:

a) deny unauthorised persons access to the equipment used for processing;

b) prevent the unauthorised reading, copying, modification or removal of data media;

c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data;

d) prevent the use of automatic processing systems by an unauthorised person using data communication equipment;

e) the person authorised to use an automated processing system has access only to the personal data to which his or her access authorisation relates;

f) may verify and establish to whom the personal data have been or may be transmitted or made available using data transmission equipment;

g) can subsequently verify or establish which personal data have been input into the automated processing system and by whom and when;

h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transfers of data media;

i) allow the reinstatement of installed systems in the event of interruption of their operation;

j) maintain the correct functionality of the system, that the appearance of faults in the functioning of the system is reported and that stored personal data cannot be compromised due to deficiencies in the functioning of the system.

Article 86
(Notification of a personal data breach by the competent authority to the Agency)

(1) In the event of a personal data breach, the competent authority shall, without delay and no later than 72 hours after having become aware of it, notify the Agency of the personal data breach, unless the personal data breach jeopardises the rights and freedoms of a natural person.

(2) The processor shall, in the event of a personal data breach, notify the competent authority without delay after becoming aware of the personal data breach.

(3) If the notification to the Agency referred to in paragraph (1) of this Article is not made within 72 hours, a written explanation shall be drawn up stating the reasons for the delay.

(4) The notification referred to in paragraph (1) of this Article shall contain at least the following information:

a) a description of the personal data breach, including, where possible, the categories and approximate number of data holders, as well as the categories and approximate number of personal data records concerned;

b) the name and contact details of the data protection officer or other contact point from which further information may be obtained;

c) a description of the likely consequences of the personal data breach;

d) a description of the measures taken or proposed to be taken by the competent authority to address the personal data breach, including, where appropriate, measures to mitigate possible adverse consequences.

(5) Information may be provided in parts, without delay, if and to the extent that it is not possible to provide all information at the same time.

(6) The competent authority shall document any personal data breaches referred to in paragraph 1 of this Article, including the facts surrounding the personal data breach, its consequences and the measures taken to remedy the situation.

(7) The documentation referred to in paragraph (4) of this Article shall be made available to the Agency in order to verify the application of this Article.

(8) In the event of a personal data breach involving personal data transmitted by or to the data controller of another country, the competent authority shall ensure that the information referred to in paragraph (4) of this Article is transmitted to the data controller of that country without undue delay.

Article 87
(Notification of a personal data breach to the data subject)

(1) Where the personal data breach is likely to result in a high risk to the rights and freedoms of a natural person, the competent authority shall communicate the personal data breach to the data holder without delay.

(2) The notification referred to in paragraph (1) of this Article shall describe in clear and plain language the nature of the personal data breach and shall specify at least the information and measures referred to in Article 86(4)(b), (c) and (d) of this Act.

(3) Information to the data subject shall not be required where one of the following conditions is met:

a) the competent authority has taken appropriate technical and organisational protection measures and those measures have been applied to the personal data in relation to which the personal data breach has occurred, in particular measures that render the personal data unintelligible to a person who is not authorised to access it, such as encryption;

b) the data controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;

c) if it would involve a disproportionate effort. In such a case, a public notice shall be published or a similar measure shall be taken whereby data holders are informed in an equally effective manner.

(4) Where the competent authority has not, by that time, notified the personal data breach to the data holder, the Agency, having considered the degree of likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph (3) of this Article are met.

(5) The information of the data subject may be delayed, restricted or denied in accordance with the conditions and on the basis of the grounds referred to in Article 69, paragraph (3) of this Act.

Article 88
(Appointment of a personal data protection officer by the competent authority)

(1) The competent authority shall appoint a personal data protection officer.

(2) When courts and other independent judicial authorities act within the limits of their judicial competence, they are not required to appoint a personal data protection officer.

(3) The Personal Data Protection Officer shall be appointed on the basis of his or her professional qualifications and, in particular, expert knowledge in personal data protection law and practice and the ability to perform the tasks referred to in Article 90 of this Act.

(4) Several competent authorities may appoint a single personal data protection officer, taking into account their organisational structure and size.

(5) The competent authority shall publish the contact details of the data protection officer and communicate them to the Agency.

Article 89

(Personal Data Protection Officer of the competent authority)

(1) The competent authority shall ensure that the personal data protection officer is appropriately and timely involved in all matters concerning the protection of personal data.

(2) The competent authority shall support the data protection officer in carrying out his or her tasks by providing him or her with the necessary means to carry out those tasks and access to personal data and processing operations, as well as to maintain his or her expert knowledge.

Article 90
(Assignments of the data protection officer of the competent authority)

The competent authority shall entrust the personal data protection officer with at least the following tasks:

a) informing and advising the competent authority and employees who carry out processing of their obligations under this Act and other laws providing for the protection of personal data;

b) monitoring the application of this Act and other laws providing for the protection of personal data, as well as the policy of the competent authority in relation to the protection of personal data, including the division of responsibilities, awareness raising and training of employees involved in processing operations, as well as related audits;

c) providing advice, where requested, regarding the assessment of the impact on the protection of personal data and monitoring its performance in accordance with Article 83 of this Act;

d) cooperation with the Agency;

e) acting as a contact point for the Agency on matters concerning processing, including the prior consultation referred to in Article 84 of this Act and advising, where appropriate, on any other matter.

Article 91
(General principles for the transfer of personal data to another country or international organisation

by the competent authority)

(1) A competent authority shall only transfer personal data which are undergoing processing or are intended for processing after transfer to another country or international organisation, including onward transfer to another country or international organisation, subject to the provisions of this Part of the Act, if the following conditions are met:

a) the transfer is necessary for the purposes laid down in Article 1(1)(c) of this Act;

b) personal data are transferred to a competent authority in another country or to an international organisation which is a public authority competent for the purposes referred to in Article 1(1)(c) of this Act;

c) where personal data have been transferred or made available from another country, that country has given prior authorisation for the transfer in accordance with its law;

d) if the Council of Ministers of Bosnia and Herzegovina, on the proposal of the Agency, has adopted an adequacy decision referred to in Article 92, paragraph (3) of this Law or if the Council of Ministers of Bosnia and Herzegovina has not adopted an adequacy decision referred to in Article 92, paragraph (3) of this

If the Council of Ministers of Bosnia and Herzegovina has not taken a decision on the adequacy referred to in Article 92, paragraph (3) of this Law and no appropriate safeguards referred to in Article 93 of this Law are provided or exist, the derogations for specific situations referred to in Article 94 of this Law shall apply.
of the law;

e) in the case of an onward transfer to another country or international organisation, the competent authority that carried out the first transfer or another competent authority in Bosnia and Herzegovina may, after taking into account all relevant facts, including the seriousness of the criminal offence, the purpose for which the personal data were first transferred and the level of protection of personal data in the other country or international organisation, authorise the onward transfer.

(2) A competent authority shall be permitted to transfer, without prior authorisation from another country, in accordance with paragraph 1(c) of this Article, exceptionally if the transfer of personal data is necessary for the prevention of an immediate and serious threat to public security of Bosnia and Herzegovina or of another country or to essential interests of Bosnia and Herzegovina, and prior authorisation cannot be obtained in good time.

(3) The competent authority shall inform the authority in the other country responsible for granting the prior authorisation of the case referred to in paragraph
(2) of this article.

(4) All provisions regarding the transfer of personal data to another country or international organisation shall be applied to ensure that the level of protection of natural persons guaranteed by this Part of the Act is not undermined.

Article 92
(Transfer from competent authority based on adequacy decision)

(1) A transfer of personal data to another country or international organisation may take place if the Council of Ministers of Bosnia and Herzegovina decides that another country, territory or one or more specified sectors within that other country or international organisation ensures an adequate level of protection, in which case such a transfer shall not require a specific authorisation.

(2) An adequate level of protection as referred to in paragraph 1 of this Article shall be deemed to be ensured in a country, parts of its territory or one or more sectors thereof, or in an international organisation which the European Union has determined to ensure an adequate level of protection of personal data.

(3) The decision on the adequacy of the level of protection of personal data referred to in paragraph (1) of this Article shall be adopted by the Council of Ministers of Bosnia and Herzegovina at the proposal of the Agency.

(4) The Agency shall prepare a proposal for the decision referred to in paragraph (3) of this Article taking into account:

a) the rule of law, respect for human rights and fundamental freedoms, relevant general and sectoral legislation, including legislation on public security, defence, State security, criminal law and access to personal data by public authorities, as well as the application of that legislation, rules on the protection of personal data, professional rules and security measures, including rules for the onward transfer of personal data to another country or international organisation, which are complied with in that other country or international organisation, case-law, as well as the existence of effective and enforceable rights of data subjects and effective administrative and judicial protection of data subjects;

b) the existence and effective functioning of one or more independent supervisory authorities in another country or of an authority to which an international organisation is subject, responsible for ensuring and enforcing data protection rules, including appropriate enforcement powers to assist data subjects in exercising their rights, as well as for cooperation with the Agency;

c) international commitments entered into by another country or international organisation, or other obligations arising from legally binding conventions or instruments, as well as from its participation in multilateral or regional organisations, in particular in relation to the protection of personal data.

(5) The Agency shall continuously monitor the situation in the field of personal data protection in another country, part of its territory, one or more sectors within that country or in an international organisation and report thereon to the Council of Ministers of Bosnia and Herzegovina as appropriate.

(6) The report referred to in paragraph (5) of this Article shall include available information and information collected from international organisations relevant to the review of the existence of an adequate level of protection of personal data, on the basis of which the Council of Ministers of Bosnia and Herzegovina shall adopt the decision referred to in paragraph (3) of this Article.

(7) The decision taken pursuant to paragraph (3) of this Article shall be without prejudice to the transfer of personal data to another country, territory or to one or more specified sectors within that other country or to an international organisation, in accordance with Articles 93 and 94 of this Act.

(8) The list of countries, parts of their territories, one or more sectors within those countries and international organisations for which the Council of Ministers of Bosnia and Herzegovina has decided that they do not ensure or no longer ensure an adequate level of protection of personal data is published in the "Official Gazette of BiH" and on the official website of the Agency.

Article 93
(Transfer from competent authority subject to appropriate safeguards)

(1) A competent authority may transfer personal data to another country or international organisation if no decision pursuant to Article 92(3) of this Act has been taken under the following conditions:

a) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or

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

(2) The competent authority shall notify the Agency of the categories of transfers in accordance with point (b) of paragraph 1 of this Article.

(3) Where a transfer of personal data is based on point (b) of paragraph 1 of this Article, the competent authority shall document such a transfer and make the documentation, upon request, available to the Agency, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and which personal data have been transferred.

Article 94
(Deviation in specific cases of transfer of personal data from the competent authority)

(1) In the absence of an adequacy decision as referred to in Article 92(3) of this Act or of appropriate safeguards as referred to in Article 93 of this Act, a transfer or a set of transfers of personal data to another country or international organisation shall take place only if the transfer is necessary and meets one of the following conditions:

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

b) in order to protect the legitimate interests of the data subject, where required by a specific law;

c) for the prevention of an immediate and serious threat to public security in the territory of Bosnia and Herzegovina or another country;

d) in individual cases for the purposes set out in Article 1(1)(c) of this Act; or

e) in an individual case for the establishment, exercise or defence of legal claims relating to the purposes referred to in Article 1(1)(c) of this Act.

(2) Personal data shall not be transferred if the transferring competent authority determines that fundamental rights and freedoms of the data subject override the public interest in the transfer referred to in points (d) and (e) of paragraph 1 of this Article.

(3) Where a transfer is made pursuant to paragraph 1 of this Article, the competent authority shall document such a transfer and make the documentation available to the Agency upon request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and which personal data have been transferred.

Article 95
(Transfer of personal data to a recipient established or established in another country)

(1) The competent authority may, in accordance with a special law, by way of derogation from Article 91(1)(b) of this Act and without prejudice to any international agreement referred to in paragraph (2) of this Article, in individual and special cases transfer personal data directly to recipients established or established in another country only if they comply with the provisions of this Part of the Act and the following conditions are met:

a) if the transfer is strictly necessary for the performance of the task of the transferring competent authority as prescribed by a special law for the purposes specified in Article 1, paragraph (1), item c) of this Act;

b) the transferring competent authority determines that the fundamental rights and freedoms of the data subject concerned do not override the public interest necessitating the transfer in the case at hand;

c) if the transferring competent authority considers that the transfer to an authority competent to act for the purpose referred to in Article 1(1)(c) of this Act to another country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time;

d) if the authority competent in another country to act for the purpose referred to in Article 1(1)(c) of this Act is notified without delay, unless this is ineffective or inappropriate;

e) the transferring competent authority notifies the recipient of the specific purpose or purposes for which that recipient may exclusively process the personal data, only if such processing is necessary.

(2) An international agreement referred to in paragraph 1 of this Article shall mean any bilateral or multilateral international agreement in force between Bosnia and Herzegovina and another country in the field of judicial cooperation in criminal matters and police cooperation.

(3) The transferring competent authority shall notify the Agency of transfers in accordance with this Article.

(4) The competent authority transferring personal data pursuant to paragraph (1) of this Article shall document such a transfer.

PART Four — PERSONAL DATA PROTECTION AGENCY IN BOSNIA AND HERZEGOVINA

Article 96
(Agency)

(1) The Agency shall be an independent supervisory body for monitoring the application of this Act, with the aim of protecting the fundamental rights and freedoms of natural persons in relation to the processing of personal data in Bosnia and Herzegovina.

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

(3) All matters of organisation and management and other matters relevant to the functioning of the Agency shall be subject to the regulations governing the organisation of the work of administrative bodies, unless otherwise provided for in this Act.

Article 97
(Independence of the Agency)

(1) The Agency shall act with complete independence in the exercise of its competences in accordance with this Act.

(2) The Director, Deputy Director and employees of the Agency in the performance of their duties and powers in accordance with this Act shall not be exposed to direct or indirect external influence and shall not seek or receive instructions from anyone.

(3) The Director, the Deputy Director and the staff of the Agency shall refrain from any action incompatible with their duties and shall not, during their term of office and employment, engage in any incompatible occupation, whether gainful or not.

(4) The Agency shall have the human, technical and financial resources, premises and infrastructure necessary for the effective exercise of its competences, including powers relating to international mutual assistance and cooperation.

(5) Employees of the Agency are civil servants and employees and are subject to the Law on Civil Service in Institutions of Bosnia and Herzegovina and the Law on Work in Institutions of Bosnia and Herzegovina.

(6) The Rules on the internal organisation of the Agency shall be approved by the Parliamentary Assembly of Bosnia and Herzegovina at the proposal of the Director of the Agency.

(7) In accordance with the provisions of the Law on Financing of Institutions of Bosnia and Herzegovina, the Agency prepares the draft annual budget and submits it to the parliamentary commission for approval. The Agency, after obtaining the approval of the Parliamentary Commission, in accordance with the deadlines prescribed by the provisions of the Law on Financing of Institutions of Bosnia and Herzegovina, shall submit the draft budget to the Ministry of Finance and Treasury of Bosnia and Herzegovina for inclusion in the budget of the institutions of Bosnia and Herzegovina and the international obligations of Bosnia and Herzegovina. The Ministry of Finance and Treasury of Bosnia and Herzegovina, the Council of Ministers of Bosnia and Herzegovina and the Presidency of Bosnia and Herzegovina may issue an opinion on the draft budget of the Agency, without the possibility of amending the draft budget previously approved by a parliamentary commission.

(8) The Agency shall be subject to financial control in accordance with financial control regulations.

Article 98
(Management of the Agency)

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

(2) The director has one deputy.

(3) The Deputy Director shall replace the Director in the performance of his/her duties if the Director is unable to perform his/her duties in accordance with his/her powers and obligations.

(4) The Director shall be responsible for the lawful operation of the Agency.

Article 99

(Conditions for the appointment, temporary suspension and dismissal of the Director and Deputy Director)

(1) The Director and Deputy Director shall be appointed by the Parliamentary Assembly of Bosnia and Herzegovina (hereinafter: Parliamentary Assembly) on the basis of a public call for proposals.

(2) The Director and the Deputy Director shall be appointed for a term of six years, renewable once.

(3) The conditions for the appointment of the Director and Deputy Directors shall be:

a) is over 18 years old;

b) that he is a citizen of Bosnia and Herzegovina (all citizens of the Federation of BiH, Republika Srpska and Brčko District of BiH are citizens of BiH);

c) has not been convicted and is not subject to criminal proceedings;

d) it is not covered by the provision of Article IX.1. Constitution of Bosnia and Herzegovina;

e) is medically fit;

f) have completed the Faculty of Social Studies, VSS/VII degree or higher education of the Bologna study system with at least 240 ECTS credits;

g) have at least 10 years' professional experience, of which at least 5 years' professional experience in management;

h) to have expertise and experience in the field of personal data protection;

i) He is not a member of a political party.

(4) The Parliamentary Assembly may temporarily suspend the Director and Deputy Director if serious misconduct is discovered. The temporary suspension shall continue until such time as a final decision has established serious misconduct.

(5) The Parliamentary Assembly may dismiss the Director and Deputy Director before the end of their term of

office: at his request,

b) serious misconduct has been established;

c) when he reaches 65 years of age and has completed at least 20 years of insurance or 40 years of insurance, irrespective of his life years;

d) if he no longer fulfils the conditions required for his appointment.

Article 100

(Incompatibility of function and professional secrecy obligations)

(1) The Director and Deputy Director and employees of the Agency shall be prohibited from acting, operating or benefiting from any activity that is incompatible with the principle of independence and impartiality, for the duration of their term of office or employment and for one year after their termination.

(2) The Director, Deputy Director and employees of the Agency during their term of office or employment relationship and after the termination of the contract or employment relationship shall be obliged to maintain professional secrecy relating to all confidential information that comes to their knowledge in the course of performing their duties or powers, in accordance with the regulations in Bosnia and Herzegovina. During their term of office, the duty of professional secrecy shall apply in particular to reports by natural persons of breaches of this Act.

Article 101
(Responsibilities of the Agency)

(1) The Agency shall be responsible for:

a) performing the tasks and powers conferred by this Act,

b) supervision of personal data processing operations by data controllers and processors.

(2) The Agency is not competent to supervise personal data processing operations by courts when exercising judicial function.

Article 102
(Tasks of the Agency)

(1) The Agency shall perform the following tasks:

a) monitor and apply this Act;

b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data, and pay particular attention to activities specifically aimed at children;

c) advise, in accordance with this Act, public authorities and other institutions and bodies on legislative and administrative measures relating to the protection of the rights and freedoms of natural persons in relation to processing;

d) raise the awareness of data controllers and processors of their obligations under this Act;

e) at the request of any data subject, provide information regarding the exercise of his or her rights under this Act;

f) consider the complaint of the data subject or of a body, organisation or association in accordance with Article 111 of this Act and issue a decision on the complaint within 90 days, of which it shall notify the complainant;

g) carry out checks in relation to the application of this Act, including on the basis of information received from public authorities;

h) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

i) adopt standard contractual clauses referred to in Article 30(8) and Article 48(3) of this Act;

j) establish and maintain a list of processing operations in connection with the obligation to carry out a data protection impact assessment in accordance with Article 37(4) of this Act;

k) give advice on the processing of personal data referred to in Article 38, paragraph (2) of this Act and Article 84, paragraph (4) of this Act;

l) encourage the drawing up of codes of conduct and issue opinions and approve such codes of conduct which provide sufficient safeguards in accordance with Article 42(5) of this Act;

m) encourage the establishment of data protection certification mechanisms as well as data protection seals and marks in accordance with Article
44, paragraph (1) of this Act, and approve the criteria for certification in accordance with Article 44, paragraph (6) of this Act;

n) in certain cases, periodically review issued certificates in accordance with Article 44(8) and (9) of this Act;

o) draw up and publish the criteria for the accreditation of a body for monitoring codes of conduct pursuant to Article 43 of this Act and the accreditation of a certification body pursuant to Article 45 of this Act;

p) accredit code of conduct monitoring bodies in accordance with Article 43 of this Act and accredit a certification body in accordance with Article 45 of this Act;

r) approve appropriate protective measures referred to in Article 48(4) of this Act;

s) approve binding business rules in accordance with Article 49 of this Act;

t) keep internal records of violations of this Act and measures taken in accordance with Article 103, paragraph (2) of this of the law;

u) gives an opinion on the draft law to institutions at the level of Bosnia and Herzegovina relating to the processing of personal data;v) performs all other tasks related to the protection of personal data.

(2) The Agency shall prescribe the format and content of the complaint form.

(3) The Agency shall perform tasks free of charge for data holders and, where applicable, for personal data protection officers.

(4) The Agency shall perform tasks free of charge for data holders and personal data protection officers referred to in Part Three of this Act.

(5) Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Agency may recover actual administrative costs or refuse to act on the request, bearing the burden of proving that the request is manifestly unfounded or excessive.

(6) The Agency shall charge a fee for issuing an accreditation to a certification body.

(7) The Agency charges a fee for the provision of opinions and other services to business entities for the purpose of performing their regular activities.

(8) The criteria for determining the amount of the fee referred to in paragraphs (5), (6) and (7) of this Article shall be established by the Agency with the prior approval of the Council of Ministers of Bosnia and Herzegovina and shall be published in the "Official Gazette of BiH".

(9) The fee shall be paid to the Single Treasury Account of the institutions of Bosnia and Herzegovina.

Article 103
(Powers of the Agency)

(1) The Agency shall have the following powers:

a) review certificates issued in accordance with Article 44(8) and (9) of this Act;

b) carry out inspections;

c) carry out a data protection audit;

d) to order the data controller and the processor, and, where applicable, the representative of the data controller or the processor, to supply all information necessary for the performance of its tasks;

e) to notify the data controller or the processor of an alleged breach of this Act;

f) gain access to all personal data and to all information held by the data controller and the processor that is necessary for the performance of its tasks;

g) gain access to all premises of the data controller and the processor where the processing of personal data is carried out, including all data processing equipment and means.

(2) The Agency shall have the following corrective powers:

a) issue a warning to the data controller or the processor that the intended processing could easily constitute a breach of this of the law;

b) issue a warning to the data controller or processor if the processing infringes this Act;

c) order the data controller or the processor to comply with the data subject's request to exercise his or her rights in accordance with this Act;

d) order the data controller or the processor to bring the processing into compliance, if necessary, with the provisions of this Act in a specified manner and within a specified period;

e) order the data controller to notify the data subject of a personal data breach;

f) temporarily or permanently restrict or prohibit processing;

g) order the rectification or erasure of personal data or restriction of processing and the communication of such actions to recipients to whom the personal data have been disclosed;

h) withdraw a certificate issued in accordance with Articles 44 and 45 of this Act or order the certification body not to issue a certificate if the requirements for certification are not met or to withdraw the certificate if the requirements are no longer met;

i) issue a misdemeanour order in misdemeanour proceedings or file a request to initiate misdemeanour proceedings in accordance with this
by law;

j) order the suspension of data transfers to a recipient in another country or international organisation.

(3) The Agency shall have the following authorisation and advisory powers:

a) advise the data controller in accordance with the prior consultation procedure referred to in Articles 38 and 84 of this Act;

b) to give opinions on all matters concerning the protection of personal data, on its own initiative or at the request of legislative bodies, governments or, in cases where a special law so provides, other institutions and bodies, as well as the public;

c) authorise the processing referred to in Article 38(8) of this Act, if a special law provides for such prior authorisation;

d) issue opinions and approve draft codes of conduct in accordance with Article 42(5) of this Act;

e) accredit certification bodies in accordance with Article 45 of this Act;

f) approve the certification criteria in accordance with Article 44(6) of this Act;

g) adopt standard data protection clauses referred to in Article 30(8) and Article 48(3) of this Act;

h) approve appropriate protective measures referred to in Article 48(4)(a) of this Act;

i) approve appropriate protective measures referred to in Article 48(4)(b) of this Act;

j) approve binding business rules in accordance with Article 49 of this Act.

(4) The decision of the Agency shall be final in administrative proceedings and shall not be subject to appeal, but an administrative dispute may be initiated before the Court of Bosnia and Herzegovina.

(5) In the decision-making process, the Agency shall apply the rules of administrative procedure, unless otherwise provided for in this Act.

(6) Where necessary, the Agency shall be authorised to notify the competent investigating bodies of infringements of this Act or initiate legal proceedings or otherwise participate in such proceedings for the purpose of implementing this Act.

(7) Any processing of personal data which has a certain level of confidentiality on the basis of a special law shall be carried out in accordance with the law governing the protection of confidential data.

(8) The processing of personal data referred to in paragraph (7) of this Article shall be carried out by officials of the Agency who have a permit for access to secret data, in accordance with the law governing the protection of secret data.

Article 104
(International cooperation for the protection of personal data)

The Agency shall take appropriate measures in relation to other countries and international organisations to:

a) the development of international cooperation mechanisms to facilitate the effective application of legislation on the protection of personal data;

b) ensuring mutual international assistance in the application of legislation on the protection of personal data, including notification, referral of complaints, assistance in investigations and exchange of information, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

c) involving relevant stakeholders in discussions and activities aimed at enhancing international cooperation in the application of legislation on the protection of personal data;

d) promoting the exchange and documentation of legislation and practice relating to the protection of personal data, including jurisdictional disputes with other countries.

Article 105

(Confidential reporting of violations of the Act)

(1) The competent authority processing personal data for the purposes referred to in Article 1(1)(c) of this Act shall ensure the application of effective mechanisms for confidential reporting of breaches of this Act.

(2) The mechanisms applied in accordance with paragraph 1 of this Article shall ensure that the infringement can be reported to the competent authority or the Agency.

(3) These mechanisms include awareness-raising on the protection of personal data and measures on the protection of persons reporting breaches.

Article 106
(Agency reports)

(1) The Agency shall submit to the Parliamentary Assembly an annual report on the protection of personal data for the previous year no later than the end of June of the current year and make it available to the public.

(2) The annual report on the protection of personal data referred to in paragraph 1 of this Article shall contain information on:

a) any activities of the Agency, in particular the types of personal data breaches and the measures taken;

b) the state of personal data protection in Bosnia and Herzegovina;

c) key issues in the field of personal data protection;

d) the Agency's capabilities.

Article 107
(Inspection)

(1) Inspection of the implementation of this Act shall be carried out by an inspector of the Agency.

(2) The inspector shall prove his identity, capacity and authority by means of an inspector's card.

(3) Inspection supervision provides an immediate insight into the legality of the work and actions of the data controller and processor with the aim of checking the compliance of its work with this Act and other regulations related to the protection of personal data.

(4) Inspections may be regular, extraordinary and auditing.

(5) Regular inspections shall be carried out on the basis of an annual and monthly inspection plan, which shall be adopted at the level of the Agency.

(6) The decision from the regular inspectional supervision is issued by the inspector, and against the decision it is allowed to appeal to the Director of the Agency within 15 days from the day of its receipt.

(7) Extraordinary inspections shall be carried out on the basis of a complaint or acting ex officio when, in relation to a particular case, an inspection needs to be carried out.

(8) Minutes from the extraordinary inspection supervision are evidence in the procedure on complaint or ex officio, which is carried out and resolved by the Agency.

(9) Audit inspection is carried out after regular or extraordinary inspection with the aim of verifying the execution of the ordered administrative measures.

(10) The decision in the procedure after conducting the extraordinary and audit inspection supervision shall be adopted by the Director of the Agency and shall be final in the administrative procedure.

(11) After the inspection has been carried out, the inspector shall draw up a record of the established facts, which shall be signed by the inspector and the authorised person of the data controller or processor.

(12) The inspector has the right to inspect all business premises and facilities in which personal data, the work process, devices, documents and documentation are processed, as well as to perform other actions related to the purpose of the inspection, in accordance with Article 103 paragraph
(1) points (f) and (g) and Article 103(7) and (8) of this Act.

(13) The data controller and the processor shall enable the inspector to carry out the inspection without hindrance.

(14) If the inspector is prevented from carrying out the inspection or is physically resisted or reasonably expected during the inspection, the inspector may request the assistance of the police.

(15) The inspector shall keep records of the inspection carried out.

PART 5 – LEGAL MEASURES, LIABILITY AND IMPRISONMENTS

Article 108
(Right to object to the Agency)

(1) The data subject shall have the right to lodge a complaint with the Agency if he or she considers that the processing of personal data relating to him or her infringes this Act, without prejudice to other administrative or judicial remedies.

(2) The Agency shall inform the complainant of the progress and outcome of the procedure, including the possibility of applying a legal remedy pursuant to Article 109 of this Act, and shall provide additional assistance at the request of the complainant.

Article 109
(Right to an effective remedy against decisions of the Agency)

(1) The natural person, data controller or processor shall have the right to bring an administrative dispute against the Agency's decision before the Court of Bosnia and Herzegovina within 60 days from the date of receipt of the decision, without prejudice to other administrative or non-judicial remedies.

(2) The data subject shall have the right to bring an administrative dispute before the Court of Bosnia and Herzegovina if the Agency does not resolve the complaint within 90 days or does not inform the data subject of the progress or outcome of the complaint procedure, without prejudice to other administrative or non-judicial remedies.

Article 110
(Right to an effective remedy against a data controller or processor)

(1) The data subject shall have the right to judicial redress against the data controller or processor if he or she considers that his or her rights under this Act have been infringed as a result of the processing of personal data, without prejudice to other administrative or non-judicial remedies, including the right to lodge a complaint with the Agency referred to in Article 108(1) of this Act.

(2) The judicial redress procedure referred to in paragraph (1) of this Article shall be conducted in accordance with the laws governing civil proceedings.

Article 111
(Representation of the data subject)

The data subject shall have the right to give the authority to a non-profit-making body, organisation or association established in accordance with the law, the purpose of which is to achieve objectives of public interest and which is active in the field of protection of the rights and freedoms of the data subject in relation to the protection of personal data, to exercise the rights referred to in Articles 108, 109 and 110 of this Act on his or her behalf, as well as to exercise the right to compensation for damage on his or her behalf and for his or her account.

Article 112
(Right to compensation and liability)

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

(2) Each data controller shall be liable for damage caused by processing in breach of this Act. The processor shall be liable for the damage caused by the processing only if it has not complied with the obligations under this Act specifically imposed on processors or if it has exceeded or acted contrary to the lawful instructions of the data controller.

(3) The data controller or processor shall be exempt from liability if it proves that it is in no way responsible for the event giving rise to the damage.

(4) Where more than one data controller or processor is involved in the same processing, or both the data controller and the processor are involved in the same processing and where they are responsible for the damage caused by the processing, each data controller or processor shall be liable for the entire damage.

(5) Where the data controller or processor has paid full compensation in accordance with paragraph (4) of this Article, that data controller or processor shall have the right to recover from the other data controllers or processors involved in the same processing the part of the compensation corresponding to their respective share of liability for the damage.

(6) The right to compensation for damage shall be exercised in court proceedings, and territorial jurisdiction shall be determined in accordance with Article 110(2) of this Act.

Article 113
(General conditions for imposing a fine)

(1) The Agency shall ensure that the imposition of a fine, in accordance with this Article and in relation to infringements of this Act, is effective, proportionate and dissuasive in each individual case.

(2) The Agency shall issue a misdemeanour order or submit a request to initiate misdemeanour proceedings to the competent court, in addition to the measures referred to in Article 103(2)(a) to (h) and (j) of this Act, depending on the circumstances of each individual case. When deciding on the fine and the amount of the fine in each individual case, account shall be taken in particular of:

a) the nature, gravity and duration of the infringement, having regard to the nature, scope and purpose of the processing in question, as well as the number of data subjects and the degree of damage suffered by them;

b) whether the infringement is intentional or negligent;

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

d) the degree of responsibility of the data controller or processor, taking into account the technical and organisational measures applied by them, in accordance with Articles 27 and 34 of this Act;

e) any identified previous infringements by the data controller or processor;

f) the degree of cooperation with the Agency in remedying the infringement and mitigating the potential adverse consequences

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

h) the manner in which the infringement became known to the Agency, in particular whether and to what extent the data controller or processor notified the infringement;

i) if measures referred to in Article 103(2) of this Act have previously been imposed on the data controller or processor in respect of the same subject matter, and compliance with such measures;

j) compliance with approved codes of conduct pursuant to Article 42 of this Act or approved certification mechanisms pursuant to Article 44 of this Act;

k) any other aggravating or mitigating factor, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

(3) If the data controller or processor intentionally or negligently violates several provisions of this Act for the same or related processing, the total amount of the fine shall not exceed the amount determined for the most serious violation.

(4) A fine of BAM 10 000 to BAM 20 000 000 or, in the case of an undertaking, up to 2% of the total annual worldwide turnover for the preceding financial year, whichever is higher, shall be imposed on:

a) the data controller and the processor for the processing of personal data carried out contrary to Articles 10 and 13, Article 27 of the GDPR; 41, 44 and 45 of this
of the law;

b) a certification body acting contrary to Articles 44 and 45 of this Act;

c) a monitoring body for approved codes of conduct if it acts contrary to Article 43(3) of this Act.

(5) A fine of BAM 20,000 to BAM 40,000,000 or, in the case of an undertaking, up to 4% of the total worldwide annual turnover for the preceding financial year, whichever is higher, shall be imposed on:

a) who processes personal data contrary to Articles 7, 8, 9 and 11 of this Act;

b) who violates the rights of the data subject referred to in Articles 14 to 24 of this Act;

c) who transfers personal data to a recipient in another country or international organisation contrary to Art. 46 para. – 51 of this Act;

d) who acts contrary to obligations under special laws adopted pursuant to Part Two, Chapter V of this Act;

e) who fails to comply with the Agency's order or temporary or permanent restriction of processing or temporary suspension of data transfer in accordance with Article 103, paragraph (2) of this Act or refuses access contrary to Article 103, paragraph (1) of this Act.

(6) For failure to comply with the order of the Agency referred to in Article 103, paragraph (2) of this Act, in accordance with paragraph (2) of this Article, a fine in the amount of BAM 20,000 to BAM 40,000,000 or, in the case of an undertaking, up to 4 % of the total worldwide annual turnover for the preceding financial year, whichever is higher.

(7) For the violation referred to in paragraphs (4), (5) and (6) of this Article, a fine of BAM 5,000 to BAM 70,000 shall be imposed on the responsible person, and a fine of BAM 500 to BAM 5,000 shall be imposed on the employee of the data controller or processor.

(8) A fine in the amount of 5,000 BAM to 70,000 BAM shall be imposed on the responsible person, and a fine in the amount of 500 BAM to 5,000 BAM shall be imposed on an employed person in a public and competent authority for misdemeanour:

a) from Art. 7. 11, 13, 14 – 24, Art. 27 41, 44, 45, 52 59, 60, 64, 66, 67 – 73, Art. 76, and 77 and 79. 90 of this Act;

b) who transfers personal data to a recipient in another country or international organisation contrary to Art. 46 para. 51 and 91 – 95 of this Act;

c) who fails to comply with the Agency's order or temporary or permanent restriction of processing or temporary suspension of data transfer in accordance with Article 103, paragraph (2) of this Act or refuses access contrary to Article 103, paragraph (1) of this Act.

(9) The limitation period for imposing a fine shall be five years from the date on which the infringement was committed.

(10) Without prejudice to the competences and powers of the Agency, no fines may be imposed on the public body and the competent authority in violation of this Act, except on the responsible and employed person referred to in paragraph (8) of this Article.

(11) The provisions of the Law on Misdemeanours of Bosnia and Herzegovina shall apply to the procedure for imposing fines referred to in this Article, and the amounts of fines shall be laid down in this Law.

(12) By way of derogation from paragraph (11) of this Article, income derived from the collection of fines shall be divided in the manner prescribed in Article 114 of this Act.

Article 114
(Enforcement and recovery of the fine)

The fine shall be paid into the Single Treasury Account of the institutions of Bosnia and Herzegovina and shall be divided as follows:

a) if the registered office or establishment of a legal person or the residence of a natural person in Bosnia and Herzegovina, funds from the Uniform Treasury Account of the institutions of Bosnia and Herzegovina shall be paid into the account of the Entity or the Brcko District of BiH, depending on the registered office or establishment of the legal person or the residence of the natural person;

b) if the seat or establishment of a legal person or the residence of a natural person is outside Bosnia and Herzegovina, the funds from the Single Treasury Account of the institutions of Bosnia and Herzegovina shall be allocated in accordance with the Decision on the Establishment of Temporary Coefficients for the Allocation of Funds from the Single Account. In the Federation of Bosnia and Herzegovina, funds are distributed between cantons and municipalities in accordance with the Law on Affiliation of Public Revenues in the Federation of Bosnia and Herzegovina.

Article 115
(Penalties)

The Criminal Codes provide for penalties for the criminal offence of unlawful processing of personal data, in the event of a gross violation of the provisions of this Act.

PART 6 – TRANSITIONAL AND FINAL PROVISIONS

Article 116
(Transitional measures)

(1) The provisions of other laws relating to the processing of personal data shall be brought into line with this Act within two years of its entry into force.

(2) Data controllers and processors who have begun processing personal data shall comply with this Act within two years of its entry into force.

(3) Decisions adopted on the basis of Article 18, paragraph (4) of the Law on Personal Data Protection ("Official Gazette of BiH", No. 49/06,76/11 and 89/11) shall remain in force until amended, replaced or repealed by a decision of the Agency.

(4) The Director and Deputy Director of the Agency appointed in accordance with the Law on Personal Data Protection ("Official Gazette of BiH", No. 49/06, 76/11 and 89/11) shall continue to perform their duties until the end of their term of office.

(5) The Agency shall continue its work for a transitional period.

Article 117
(Subordinate legislation)

All subordinate legislation prescribed by this Act shall be adopted within 210 days of the date of entry into force of this Act.

Article 118
(Relation to previously concluded agreements)

International agreements involving the transfer of personal data to other countries or international organisations concluded by Bosnia and Herzegovina prior to the adoption of this Law, which comply with the Law on Personal Data Protection ("Official Gazette of BiH", No. 49/06, 76/11 and 89/11), shall remain in force until amended, replaced or repealed.

Article 119
(Expiration)

(1) The Law on the Protection of Personal Data ("Official Gazette of BiH", No. 49/06, 76/11 i89/11) shall cease to apply at the beginning of the application of this Law.

(2) When this Act becomes applicable, subordinate legislation adopted pursuant to the Act referred to in paragraph (1) of this Article shall cease to be valid:

Ordinance on the procedure for the objection of the personal data holder at the Personal Data Protection Agency in Bosnia and Herzegovina
("Official Gazette of BiH", No. 51/09), Rulebook on Inspections in the Field of Personal Data Protection ("Official Gazette of BiH", No. 51/09), Instruction on the Method of Verification of Personal Data Processing Before Establishing a Personal Data Collection ("Official Gazette of BiH", No. 51/09), Rulebook on the Method of Keeping and Form of Records of Personal Data Collections ("Official Gazette of BiH", No. 52/09) and Rulebook on the Method of Keeping and Special Measures of Technical Protection of Personal Data ("Official Gazette of BiH", No. 67/09).

Article 120

(Entry into force)

This Law shall enter into force on the eighth day from the day of its publication in the "Official Gazette of BiH" and shall be applied after the expiration of 210 days from the day of its entry into force.

Number 01.02-02-1-2548/24
30 January 2025
Sarajevo
Chair
the Chamber of Deputies
of the Parliamentary Assembly of
BiH Dr. **Denis Zvizdić**

Chair
the House of Peoples
BiH Parliamentary Assembly of BiH
Dr. **Dragan Covic**