Published in Official Gazette no./
Official Gazette publication date/
Constitutional Court no./

LAW ON PERSONAL DATA PROTECTION (*)

(„Official Gazette of the Republic of North Macedonia“ No. 42/20 and 294/21)

*****This Law is harmonized with the European regulation in the field of personal data protection, specifically: 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) CELEX No. 32016R0679.

I. GENERAL PROVISIONS

Subject matter of the Law

Article 1

This Law regulates the protection of personal data and the right to privacy with regard to the processing of personal data, and in particular the principles related to the processing of personal data, the rights of the data subject, the position of the controller and the processor, the transfer of personal data to other countries, the establishment, status and competencies of the Personal Data Protection Agency, the special operations for the processing of personal data, the legal remedies and liability in the processing of personal data, the supervision over personal data protection, as well as the misdemeanors and misdemeanor proceedings in this area.

Material scope

Article 2

(1) This Law applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

(2) This Law does not apply to the processing of personal data by a natural person in the course of a purely personal or household activities.

Territorial scope

Article 3

(1) Provisions of this Law apply to the processing of personal data if the controller or processor is established on the territory of the Republic of North Macedonia, regardless of whether the processing takes place on the territory of the Republic of North Macedonia or not.

(2) Provisions of this Law apply to the processing of personal data of data subjects from the Republic of North Macedonia by a controller or processor not established in the Republic of North Macedonia, where the personal data processing activities are related to:

- the offering of goods or budgets, irrespective of whether a payment of the data subject from the Republic of North Macedonia is required, or
- the monitoring of the data subject behaviour as far as their behaviour takes place in the Republic of North Macedonia.

(3) Provisions of this Law apply to the processing of personal data by a controller not established in the Republic of North Macedonia, but is established in a place where the law of the Republic of North Macedonia applies according to international agreements ratified in accordance to the Constitution of the Republic of North Macedonia.

Definitions

Article 4

(1) For the purposes of this Law:

1. "**Personal data**" means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly,

in particular by reference to an identifier such as the first and last name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2. "**Processing of personal data**" 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, inquiry, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

3. "**Restriction of processing**" means the marking of stored personal data with the aim of limiting their processing in the future;

4. "**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, and 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;

5. "**Pseudonymisation**" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

6. "**Filing system**" means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

7. "**Controller**" means the natural or legal person, state administration body, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by a law or another regulation, the law or regulation shall stipulate the controller or the specific criteria for its nomination;

8. "**Processor of filing system**" means a natural or legal person, state administration body, public authority, agency or other body which processes personal data on behalf of the controller;

9. "**Recipient**" means a natural or legal person, state administration body, public authority, agency or other body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

10. "**Third party**" means a natural or legal person, state administration body, public authority, agency or another body other than the data subject, controller, processor or person who, under the direct authority of the controller or processor, is authorised to process personal data;

11. "**Consent**" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

12. "**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;

13. "**Special categories of personal data**" are personal data revealing information on the racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation;

14. "**Genetic data**" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from analysis of a biological sample from the natural person in question;

15. "**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;

16. "**Data concerning health**" means personal data related to the physical or mental health of
a natural person, including data on the provided health care services, which reveal information about his or her health status;

17. "**Representative**" means a natural or legal entity established in the Republic of North Macedonia designated by the controller or processor in writing pursuant to Article 31 of this Law, representing the controller or processor with regard to their respective obligations under this Law;

18. "**Binding corporate rules**" means personal data protection policies which are adhered to by a controller or processor established on the territory of the Republic of North Macedonia for transfers or a set of transfers of personal data from the Republic of North Macedonia to a controller or processor in one or more third countries within a group of undertakings (associated undertakings), or group of legal persons engaged in a joint economic activity;

19. "**Information society service**" means a service as defined by electronic trading regulations;

20. "**International organisation**" means an organisation and its subordinate bodies 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;

21. "**Direct marketing**" means any type of communication taking place by any means with the purpose of imparting advertising, marketing or publicity materials targeting directly a specific data subject, as well as personal data processing which includes profiling to the extent that it is related to this type of communication.

22. "**Supervisory authority**" means the Personal Data Protection Agency which has the status of an independent public authority established in accordance with this Law (hereinafter: the Agency);

23. "**Investigation**" within the meaning of this Law is a procedure of examination and verification of the lawfulness of activities taken by certain controller or processor when processing personal data and their protection when implementing this law and regulations pursuant to this Law.

24. "**State administration body**" within the meaning of this Law are other state administration bodies and institutions established in accordance with the Constitution of the Republic of North Macedonia and in accordance with the Law;

25. "**Icon**" within the meaning of this Law is a visual representation of an installed application or software program in an information-communication system that the data subject uses and is understandable to the system user.

(2) The meaning of expressions referred to in this Law which have not been defined in paragraph (1) of this Article, have been defined in other laws.

Prohibition of discrimination

Article 5

Protection of personal data shall be guaranteed to any natural person free of discrimination based on nationality, race, skin colour, religious belief, ethnic background, gender, language, political or other beliefs, material status, origin by birth, education, social background, citizenship, place or type of residence, or any other personal characteristics of that person.

Application of the Law on general administrative procedure

Article 6

(1) The procedures provided for by this Law shall be conducted in accordance with the provisions of the Law on General Administrative Procedure, unless otherwise provided for by this Law.

(2) The communication regarding the procedures referred to in paragraph (1) of this Article, between the Agency and the parties shall take place in writing, orally or in electronic form, in compliance with this Law and the Law on General Administrative Procedure.

Data submission

Article 7

(1) Any state administration body, public institution or other legal entity maintaining official public registers, publicly available filing systems or other filing systems shall be obliged, free of charge and upon request of the Agency, to submit data from the registers and filing systems for needs of the procedures that are being conducted pursuant to this Law.

(2) Communication between the Agency and state administration bodies, public institutions or other legal entities from paragraph (1) of this Article shall be conducted in written, oral or electronic form, pursuant with the law.

Providing aid
Article 8

(1) The Agency can request to be given aid by the state administration body competent for internal affairs during the implementation of the executive decision in accordance with the Law on General Administrative Procedure and this Law, in the event of physical resistance or such resistance is expected to happen, as well as in other cases determined by law.

(2) In the cases referred to in paragraph (1) of this Article, the state administration body competent for internal affairs shall be obliged to give aid pursuant to the Law.

II. PRINCIPLES

Principles relating to the personal data processing

Article 9

(1) Personal data are:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes, in accordance with Article 86 paragraph (1) of this Law, shall not be considered to be incompatible with the initial purposes ("purpose limitation");
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
- accurate and, where necessary, kept up to date; every reasonable step 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 ("accuracy");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes in accordance with Article 86 paragraph (1) of this Law, subject to implementation of the appropriate technical and organisational measures pursuant to this Law, in order to safeguard the rights and freedoms of the data subject ("storage limitation");
- 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 ("integrity and confidentiality").

(2) The controller shall be responsible for, and be able to demonstrate compliance with paragraph (1) of this Article ("accountability').

Lawfulness of processing

Article 10

(1) Processing shall be lawful only if and to the extent that at least one of the following applies:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- 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;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary to protect the vital interests of the data subject or of another natural person;

- 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 controller;
- processing is necessary for the purposes of the legitimate interests pursued by the 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.

(2) Line 6 of paragraph (1) of this Article shall not apply for the processing of personal data by state administration bodies in the performance of their tasks.

(3) The legal basis for processing personal data stipulated by lines 3 and 5 of paragraph (1) of this Article shall be laid down by law. The law shall mandatorily stipulate provisions concerning: the general conditions governing the lawfulness of processing by the controller, purposes of the processing, the categories of data which are subject to the processing; categories of data subjects, the entities to, and the purposes for which, the personal data may be disclosed, the purpose limitation, storage periods, processing operations and processing procedures, including measures to ensure lawful and fair processing, in order to meet an objective of public interest and be proportionate to the legitimate aim pursued. The Law must also contain data protection impact assessment for the cases provided for in Article 39 of this Law.

(4) Where the processing of personal data for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or based on the law, which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 27 paragraph (1) of this Law, the controller shall, in order to ascertain whether processing for another purpose is compatible with the initial purpose for which the personal data are initially collected, take into account, inter alia:

- any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
- the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
- the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 13 of this Law, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 14, paragraph (1) of this Law;
- the possible consequences of the intended further processing for data subjects;
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Conditions for consent

Article 11

(1) Where processing is based on consent, the controller shall demonstrate that the data subject has consented to the processing of his or her personal data pursuant to Article 4 paragraph (1) point 11

of this Law.

(2) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly

distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Law shall not be binding.

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

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

Conditions applicable to child's consent in relation to information society service

Article 12

(1) Where the data subject has given consent for data processing for one or more specific purposes, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 14 years old. Where the child is below the age of 14 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

(2) In cases of paragraph (1) of this Article, the controller shall make reasonable effort to verify in such cases that consent is given by the holder of parental responsibility over the child, taking into consideration available technology.

Processing of special categories of personal data

Article 13

(1) Processing of special categories of personal data specified in Article 4 paragraph (1) point 13 of this Law is prohibited.

(2) Notwithstanding paragraph (1) of this Article, processing of special categories of personal data may take place provided if:

1) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where the law provides that the prohibition referred to in paragraph (1) of this Article may not be lifted by the data subject;

2) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of labour law and social security and social protection law in so far as it is authorised by law or collective agreement providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

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

4) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, citizen association or any other non-profit organisation with a political, philosophical, religious or trade union aim and under the condition that the processing relates solely to the members of these organisations or to their former members or to persons who have regular contact with them in connection with their purposes and under the condition that the personal data are not disclosed outside that organisation without the consent of the data subjects;

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

6) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial authority;

7) processing is necessary for reasons of public interest, on the basis of the law, proportionate to the aim pursued and respect the essence of the right to data protection and provision of suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

8) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, 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 law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph (3) of this Article;

9) 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 or medical devices, based on the law, which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

10) processing is necessary for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes in accordance with Article 86 paragraph (1) of this Law, based on the Law, which shall be proportionate to the aim pursued, with 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 8) of paragraph (2) of this Article, when those data are processed by or under the responsibility of a professional body subject to the obligation of professional secrecy pursuant to law or rules established by national competent bodies in the Republic of North Macedonia or by another person also subject to the obligation of professional secrecy in accordance with law or the regulations stipulated by authorised bodies in the Republic of North Macedonia.

Processing of personal data relating to criminal convictions and offences

Article 14

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 10 paragraph (1) of this Law, is carried out only under the control of official authority or when the processing is authorised by law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions and offences shall be kept only under the control of official authority.

Processing which does not require identification

Article 15

(1) If the purposes for which a controller processes personal data do not or do no longer require the further identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Law.

(2) Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 19 to 24 of this Law shall not apply, except where the data subject, for the purpose of exercising its rights under these articles, provides additional information enabling his or her identification.

III. RIGHTS OF THE DATA SUBJECT

1. Transparency

Transparent information, communication and modalities for the exercise of the rights of the data subject

Article 16

(1) The controller shall take appropriate measures to provide any information referred to in Articles 17 and 18 of this Law and any communication under Articles 19 to 26 as well as Article 38 of this Law relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where applicable, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

(2) The controller shall facilitate the exercise of data subject rights under Articles 19 to 26 of this Law. In the cases referred to in Article 15 paragraph (2) of this Law, the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 19 to 26 of this Law, unless the controller demonstrates that it is not in a position to identify the data subject.

(3) The controller shall provide information on action taken for the request based on Articles 19 to 26 of this Law to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request in electronic form, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

(4) If the controller fails to take action upon the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for failure to act and of the possibility of lodging a request with the Agency as well as the possibility of seeking a judicial remedy.

(5) Information provided under Articles 17 and 18 of this Law and any communication and any actions taken under Articles 19 to 26 as well as Article 38 of this Law 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 controller may either:

- charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or - refuse to act on the request.
The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.
(6) Notwithstanding Article 15 of this Law, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 19 to 25 of this Law, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

(7) The information to be provided to data subjects pursuant to Articles 17 and 18 of this Law may be provided in combination with standardised icons in order to ensure an easily visible, intelligible and clearly legible manner and in order to provide a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

(8) The Agency shall adopt by-laws for identifying the information to be presented in form of icons and the procedures for providing standardised icons.

2. Information and access to personal data

Information to be provided where personal data are collected from the data subject

Article 17

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

1) the identity and the contact details of the controller and, where applicable, of the controller's authorised representative in the Republic of North Macedonia;
2) the contact details of the data protection officer, where applicable;
3) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4) where the processing is based on Article 10, paragraph (1) line 6 of this Law, the legitimate interests pursued by the controller or by a third party;
5) the recipients or categories of recipients of personal data, if applicable;
6) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and in case of transfer of personal data referred to in Article 50 or 51, or Article 53 paragraph (1), second subparagraph of this Law, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

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

1) the period for which the personal data will be stored, or if that is impossible, the criteria used to determine that period;
2) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
3) where the processing is based on line 1, paragraph (1), Article 10 of this Law or point (1), paragraph (2), of Article 13 of this Law, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
4) the right to lodge a request with the Agency, in accordance with this Law;
5) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
6) The existence of automated decision-making process, including profiling, referred to in Article 26 paragraphs (1) and (4) of this Law, and, at least in those cases, when meaningful information about the processing logic is involved, as well as the significance and the envisaged consequences of such processing for the data subject.

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

(4) Paragraphs (1), (2) and (3) of this Article shall not apply where and insofar as the data subject already has the information.

Information to be provided where personal data have not been obtained from the data subject

Article 18

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

1) the identity and the contact details of the controller and, where applicable, of the controller's authorised representative in the Republic of North Macedonia;
2) the contact details of the data protection officer, where applicable;
3) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4) the categories of personal data concerned;
5) the recipients or categories of recipients of the personal data, if any;
6) where applicable, that the controller intends to transfer personal data to a third country or international organisation and in the case of personal data transfers referred to in Article 50, Article 51, or Article 53, paragraph (1) second subparagraph of this Law, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

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

1) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
2) where the processing is based on line (6), paragraph (1) Article 10 of this Law, the legitimate interests pursued by the controller or by a third party;
3) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
4) where processing is based on point (1), paragraph (1) Article 10 of this Law or based on Article 13 paragraph (2) point 1) of the Law, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
5) the right to lodge a request with the Agency, in accordance with this Law;
6) the source of personal data and, if applicable, whether it came from publicly accessible sources;
7) the existence of automated decision-making, including profiling, referred to in Article 26, paragraphs (1) and (4) of this Law, at least in those cases, where meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(3) The controller shall provide the information referred to in paragraphs (1) and (2) of this article: 1) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

2) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

3) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

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

(5) Paragraphs (1) to (4) of this Article shall not apply where and insofar as:

1) the data subject already has the information:

2) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 86 paragraph (1) of this Law, 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 controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

3) obtaining or disclosure is expressly laid down by law which provides appropriate measures to protect the data subject's legitimate interests; or

4) the personal data must remain confidential subject to an obligation of professional secrecy regulated by law, including a statutory obligation of secrecy.

Right of access by the data subject

Article 19

(1) The data subject shall have the right to obtain from the controller confirmation as to whether personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

1) the purposes of the processing;

2) the categories of personal data being processed;

3) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

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

5) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject, or to object to such processing; 6) the right to lodge a request with the Agency in accordance with Article 97 of this

Law; 7) where the personal data are not collected from the data subject, any available information as to their source;

8) the existence of automated decision-making, including profiling, referred to in Article 26 paragraphs (1) and (4) of this Law, and, at least in those cases where meaningful information about the processing logic is involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(2) Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 50 of this Law relating to the transfer.

(3) The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. If the controller charges a fee, the amount of the same depends on the volume, complexity and time required to provide the copies.Where the data subject makes the request by electronic means, the information shall be provided in a commonly used electronic form, unless otherwise requested by the data subject.

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

3. Rectification and erasure

Right to rectification

Article 20

The data subject shall have the right to obtain from the controller within 15 days from the day of receipt of the request, the rectification of inaccurate personal data concerning 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.

Right to erasure (“right to be forgotten”)

Article 21

(1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her and the controller shall have the obligation to erase personal data within 30 days from the day of receipt of the request where one of the following grounds applies:

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

2) the data subject withdraws consent on which the processing is based according to Article 10 paragraph (1) point (1), or Article 13 paragraph (2) of this Law, and where there is no other legal ground for the processing;
3) the data subject objects to the processing pursuant to Article 25 paragraph (1) of this Law and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 25, paragraph (2) of this Law;
4) the personal data have been unlawfully processed;
5) the personal data should be erased for compliance with a legal obligation stipulated by law to which the controller is subject;
6) the personal data have been collected in relation to the offer of information society services referred to in Article 12 paragraph (1) of this Law.

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

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

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

b) for compliance with a legal obligation stipulated by Law, to which the controller is subject, requesting processing, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

c) for reasons of public interest in the area of public health in accordance with Article 13 paragraph (2) points (8) and (9) as well as Article 13 paragraph (3) of this Law.

d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 86 paragraph (1) of this Law 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.

Right to restriction of processing

Article 22

(1) The data subject shall have the right to obtain from the controller restriction of processing where one of the following conditions applies:

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

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

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

d) the data subject has objected to processing pursuant to Article 25 paragraph (1) of this Law pending the verification whether the legitimate grounds of the controller override those of the data subject.

(2) Where processing has been restricted under paragraph (1) of this Article, such personal data shall, with the exception of storage, only be processed with the data subject's consent 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 important public interest.

(3) In case a data subject obtained restriction of processing pursuant to paragraph (1) of this Article, the controller shall inform the data subject before the restriction of processing is lifted.

Notification obligation regarding rectification or erasure of personal data or restriction of processing

Article 23

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 20, Article 21 paragraph (1) and Article 22 of this Law to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Right to data portability

Article 24

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

a) the processing is based on consent pursuant to Article 10 paragraph (1), line (1) or Article 13 paragraph (2) point 1) of this Law, or pursuant to a contractual obligation from Article 10 paragraph (1), line 2 of this Law; and

b) the processing is carried out in automated manner.

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

(3) The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to the right stipulated by Article 21 of this Law. That 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 controller.

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

4. Right to object and automated individual decision-making

Right to object

Article 25

(1) The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on lines (5) or (6) of Article 10 paragraph (1) of this Article, including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject 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) Where the data subject objects to processing for direct marketing purposes, the controller shall stop processing of personal data for such purposes.

(4) At the latest by the time of the first communication with the data subject, the right referred to in paragraphs (1) and (2) shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

(5) In the context of the use of information society services, and notwithstanding the electronic communications regulation, 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 86 paragraph (1) of this Law, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Automated individual decision-making, including profiling

Article 26

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

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

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

b) is authorised by law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or c) is based on the data subject's explicit consent.

(3) In the cases referred to in points (a) and (c) of paragraph (2) of this Article, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, the right to express his or her point of view and the right to contest the decision.

(4) Decisions referred to in paragraph (2) of this Article shall not be based on special categories of personal data referred to in Article 13 paragraph (1) of this Law, unless point 1) or 7) of Article 13 paragraph (2) of this Law applies as well as suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

5. Restrictions

Restrictions

Article 27

(1) The applicable law to which the data controller or processor is subject may restrict the scope of the obligations and rights provided for in Articles 16 to 26 of this Law, and Article 38, as well as Article 9 of this Law, in so far as its provisions correspond to the rights and obligations provided for in Articles 16 to 26, and when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

1) national security;
2) defence;
3) public security;
4) 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; 5) other important objectives of general public interest of the Republic of North Macedonia, in particular an important economic or financial interest to the Republic of North Macedonia, including monetary, budgetary, taxation matters, public health and social security; 6) the protection of judicial independence and judicial proceedings;
7) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

8) a monitoring, inspection supervision or regulatory function connected, even occasionally, to the exercise of official authority of state administration bodies in the cases referred to in points 1) to 5) and 7) of this paragraph;

9) the protection of the data subject or the rights and freedoms of others; 10) the enforcement of civil law claims.

(2) In particular, any legislative measure referred to in paragraph (1) of this Article, shall contain specific provisions at least, where relevant, as to:

1) the purposes of the processing or categories of processing;
2) the categories of personal data;
3) the scope of the restrictions introduced;
4) the safeguards to prevent abuse or unlawful access or transfer;
5) the specification of the controller or categories of controllers;
6) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
7) the risks to the rights and freedoms of data subjects; and
8) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

IV. CONTROLLER AND PROCESSOR

1. General obligations

Responsibility of the controller

Article 28

(1) Taking into account 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, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Law. The technical and organisational measures shall be reviewed and updated where necessary.

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

(3) Adherence to approved codes of conduct as referred to in Article 44 or approved certification mechanisms as referred to in Article 46 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Data protection by design and by default

Article 29

(1) Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed with the goal of effective implementation of data-protection principles, such as data minimisation, and to integrate the necessary safeguards into the processing in order to meet the requirements of this Law and to protect the rights of data subjects.

(2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. Such measures shall, in particular, ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

(3) An approved certification mechanism pursuant to Article 46 of this Law may be used as an element to demonstrate compliance with the requirements set out in paragraphs (1) and (2) of this Article.

Joint controllers

Article 30

(1) Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall, in a transparent manner determine their respective responsibilities for compliance with the obligations under this Law, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 17 and 18 of this Law, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by separate law. The arrangement may designate a contact point for data subjects.

(2) The arrangement referred to in paragraph (1) of this Article shall duly reflect the respective roles and relationships of the joint controllers vis-a-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

(3) Irrespective of the terms of the arrangement referred to in paragraph (1) of this Article, the data subject may exercise his or her rights under this Law in respect of and against each of the controllers.

Representatives of controllers or processors not established in the Republic of North Macedonia

Article 31

(1) Where paragraph (2) of Article 3 of this Law applies, the controller or the processor shall designate in writing an authorised representative in the Republic of North Macedonia. (2) The obligation laid down in paragraph (1) of this Article shall not apply to:

(a) the processing which is occasional, and does not include, on a large scale, processing of special categories of data as referred to in Article 13 paragraph (1) of this Law or processing of personal data relating to criminal convictions and offences referred to in Article 14, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

(b) a state administration authorities or other body.

(3) The personal data subjects and the Agency may, in addition or instead of the controller or processor, address the authorised representative on all issues related to processing, for the purposes of ensuring compliance with this Law.

(4) The designation of an authorised representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Processor

Article 32

(1) Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Law and ensure the protection of the rights of the data subject.

(2) The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the engagement or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

(3) Processing by a processor shall be governed by a contract or other legal act compliant with the law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required

to do so by law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 36 of this Law;

(d) respects the conditions referred to in paragraphs 2 and 4 of this Article for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of this Law; (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 36 to 40 of this Law, taking into account the nature of processing and the information available to the processor; (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless the law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of this paragraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this law or other regulations pertaining to personal data protection provisions.

(4) Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph (3) of this Article, shall be imposed on that other processor by way of a contract or other legal act in compliance with the law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Law. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

(5) Adherence of a processor to an approved code of conduct as referred to in Article 44 of this Law or approved certification mechanism as referred to in Article 46 of this Law may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs (1) and (4) of this Article.

(6) The contract or the other legal act referred to in paragraphs (3) and (4) of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraph (7) of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 46 and 47 of this Law, without prejudice to the individual contract between the controller and the processor.

(7) The Agency may lay down standard contractual clauses for the matters referred to in paragraphs (3) and (4) of this Article.

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

(9) If a processor infringes this Law by determining the purposes and means of processing, that processor shall be considered to be a controller in respect of that processing, without prejudice to Article 101 and provisions of Chapter IX of this Law.

Processing under the authority of the controller or processor

Article 33

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so under this of another law.

Records of processing activities

Article 34

(1) Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall, in particular, contain all of the following information:

(a) the name, that is first and last name and contact details of the controller and, where applicable, of all joint controllers, the controller's authorised 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 third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 53 paragraph (1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of personal data; (g) where possible, a general description of the technical and organisational security measures referred to in Article 36, paragraph (1) of this Law.

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

(a) the name, that is first and last name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's authorised representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;
(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in Article 53 paragraph (1), second subparagraph of this Law, the documentation of suitable safeguards;
(d) where possible, a general description of the technical and organisational security measures referred to in Article 36, paragraph (1) of this Law.

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

(4) The controller or the processor and, where applicable, their authorised representatives, shall make the records referred to in paragraphs (1) and (2) of this Article available to the Agency, upon its request.

(5) The obligations referred to in paragraphs (1) and (2) of this Article shall not apply to an enterprise or an organisation employing fewer than 50 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 13 paragraph (1) of this Law or personal data relating to criminal convictions and offences referred to in Article 14 paragraph (1) of this Law.

Cooperation with the Agency
Article 35

The controller and the processor and, where applicable, their representatives, shall cooperate, at the request of the Agency, for the fulfilment of their tasks.

2. Security of personal data

Security of processing

Article 36

(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 risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
(a) the 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 physical or technical incidents;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

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

(3) Adherence to an approved code of conduct as referred to in Article 44 of this Law or an approved certification mechanism as referred to in Article 46 of this Law may be used as an element by which to demonstrate compliance with the requirements set out in paragraph (1) of this Article.

(4) The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by law.

(5) The controller and processor are obliged to demonstrate the implementation of the measures in accordance with the requirements of paragraph (1) of this Article.

Notification of a personal data breach to the Agency

Article 37

(1) In the event of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Agency unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Agency is not made within 72 hours, it shall be accompanied by reasons for the delay.

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

(3) The notification referred to in paragraph (1) of this Article shall, at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of filing systems concerned;

(b) communicate the first and last name, and contact details of the data protection officer or other contact point where more information can be obtained;

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

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(4) Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

(5) The controller shall document any personal data breaches, including the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Agency to verify compliance with this Article.

Communication of a personal data breach to the data subject

Article 38

(1) When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

(2) The communication to the data subject referred to in paragraph (1) of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in Article 37 paragraph (3) points (b), (c) and (d) of this Law.

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

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as the encryption;

(b) the 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) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner. (4) If the controller has not already communicated the personal data breach to the data subject, the Agency, having considered the 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 Law are met.

3. Data protection impact assessment and prior consultation

Data protection impact assessment

Article 39

(1) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights

and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

(2) The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

(3) A data protection impact assessment referred to in paragraph (1) of this Article shall in particular be required 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 on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
(b) processing of a large scale of special categories of data referred to in Article 13 paragraph (1) of this Law, or of personal data relating to criminal convictions and offences referred to in Article 14 of this Law; or
(c) a systematic monitoring of a publicly accessible area on a large scale.
(4) The Agency shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph (1) of this Article. (5) The Agency may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required.
(6) The assessment shall contain 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 controller;
b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

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

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

(7) Compliance with approved codes of conduct referred to in Article 44 of this Law by relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

(8) Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

(9) Where necessary, the controller is obliged to carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk caused by processing operations.

Prior consultation

Article 40

(1) The controller shall consult the Agency prior to processing where a data protection impact assessment under Article 39 of this Law indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

(2) Where the Agency is of the opinion that the intended processing referred to in paragraph (1) of this Article would infringe this Law, in particular where the controller has insufficiently identified or mitigated the risk, the Agency shall, within period of up to 60 days of receipt of the request for consultation, provide written advice to the controller and, where applicable, to the processor, and may use any of its powers referred to in Article 66 of this Law. That period may be extended by 40 days, taking into account the complexity of the intended processing. The Agency shall, within 30 days of the receipt of the request for consultation, inform the controller, and, where applicable, the processor, of any such extension, including reasons for the delay. Those periods may be suspended until the Agency has obtained all information it has requested for the purposes of the consultation.

(3) When consulting the Agency pursuant to paragraph (1) of this Article, the controller shall provide the Agency with the following information:

(a) where applicable, data on respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
(b) the purposes and means of the intended processing;
(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Law;
(d) where applicable, the contact details of the data protection officer;
(e) the data protection impact assessment provided for in Article 39 of this Law; and
(f) any other information requested by the Agency.

(4) State administration bodies shall consult the Agency during the preparation of a proposal for a legislative measure to be adopted by the Parliament of the Republic of North Macedonia, or of a regulatory measure based on such a legislative measure, which relates to processing.

(5) Notwithstanding paragraph (1) of this Article, during the consultation process of controllers with the Agency, controllers shall seek prior authorisation from the Agency in relation to processing by a

controller for the performance of tasks in the public interest, including processing in relation to social protection and public health.

(6) The authorisation referred to in paragraph (5) of this Article shall in particular be required in the case of:

(a) the core activities of the controller consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale;

(b) the core activities of the controller consist of processing on a large scale of special categories of data pursuant to Article 13 of this Law and personal data relating to criminal convictions and offences referred to in Article 14 of this Law, or

(c) a systematic monitoring of areas on a large scale.

4. Data protection officer

Designation of the data protection officer

Article 41

(1) The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a state administration body, except for courts acting in their judicial capacity, which designated officer for other processing of personal data conducted in accordance with the law;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 13 of this Law and personal data relating to criminal convictions and offences referred to in Article 14 of this Law.

(2) A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment, the Agency and the data subjects.

(3) Where the controller or the processor is a state administration body, a single data protection officer may be designated for several such bodies, taking account of their organisational structure and size.

(4) In cases other than those referred to in paragraph (1) of this Article, the controller or processor or associations and other bodies representing categories of controllers or processors shall designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

(5) The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of personal data protection law and practices and the ability to fulfil the tasks referred to in Article 43 of this Law.

A person may be designated a data protection officer if he/she is:

- meets the conditions for employment determined by this and other law,
- in active command of the Macedonian language,
- at the time of designation does have imposed on him/her a conviction by a final court judgement or misdemeanour sanction with a prohibition to act in his/her profession, activity or duty,
- has at least 240 credits under the ECTS or completed VII/1 level of education, and
- has acquired knowledge and skills regarding the practices and regulations for personal data protection, in accordance with the provisions of this Law.

(6) The data protection officer may be a staff member of the controller or processor, or fulfil the tasks based on a service contract.

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

Position of the data protection officer

Article 42

(1) The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

(2) The controller and processor shall support the data protection officer in performing the tasks referred to in Article 43 of this Law by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

(3) The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. The data protection officer shall not be dismissed or penalised by the controller or the processor for performing his/her tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

(4) Data subjects may contact the data protection officer regarding all issues related to processing of their personal data and to the exercise of their rights under this Law.

(5) The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with the Law.

(6) The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Tasks of the data protection officer

Article 43

(1) The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing in accordance with their obligations pursuant to data protection regulations;

(b) to monitor compliance with this Law, with other regulations pertaining to personal data protection in the Republic of North Macedonia and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, as well as to conduct audit of personal data protection;

(c) where necessary, to provide advice on data protection impact assessment and to monitor its performance pursuant to Article 39 of this Law;

(d) to cooperate with the Agency;

(e) to act as the contact point for the Agency on issues relating to processing, including the prior consultation referred to in Article 40 of this Law, and to consult, where appropriate, regarding any other matters.

(2) The data protection officer shall, in the performance of his or her tasks, have due regard to the risk associated with processing operations, considering the nature, scope, context and purposes of processing.

5. Codes of conduct and certification

Codes of conduct

Article 44

(1) Having regard to the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises, with the goal of contributing to the proper application of this Law, the associations and other bodies representing the categories of controllers or processors may prepare codes of conduct, amend or extend them in order to better specify this Law and its application with regard to:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;
(h) the measures and procedures referred to in Articles 28 and 29 of this Law, and the measures to ensure security of processing referred to in Article 36 of this Law;
(i) the notification of personal data breaches to the Agency and the communication of such personal data breaches to data subjects;
(j) the transfer of personal data to third countries or international organisations; or
(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 97 and 99 of this Law.

(2) The code of conduct from paragraph (1) of this Article shall contain mechanisms which enable the monitoring body from Article 45 of this Law to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of the Agency pursuant to Articles 64 and 65 of this Law.

(3) Associations and other bodies referred to in paragraph (1) of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the Agency. The Agency shall provide an opinion on whether the draft code, its amendment or extension complies with this Law and shall also approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

(4) Where the draft code, or amendment or extension is approved in accordance with paragraph (3) of this Article, the Agency shall register and publish the code.

(5) The Agency shall keep a register of all approved codes of conduct, amendments and extensions and shall make them publicly available by way of appropriate means.

(6) The form, content and manner of keeping the register referred to in paragraph (5) of this Article shall be adopted by the Director of the Agency.

Monitoring of approved codes of conduct

Article 45

(1) Without prejudice to the tasks and powers of the Agency under Articles 65 and 66 of this Law, the monitoring of compliance with a code of conduct pursuant to Article 44 of this Law may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the Agency.

(2) The body as referred to in paragraph (1) of this Article may be accredited to monitor compliance with a code of conduct where the body has:

(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the Agency;

(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) demonstrated to the satisfaction of the Agency that its tasks and duties do not result in a conflict of interests.

(3) The director of the Agency shall determine the criteria for accreditation of the body referred to in paragraph (1) of this Article.

(4) Without prejudice to the tasks and powers of the Agency and the provisions of Chapter VIII and IX of this Law, the body as referred to in paragraph (1) of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. The body from paragraph (1) of this Article shall inform the Agency of such actions and the reasons for taking them.

(5) The Agency shall revoke the accreditation of a body as referred to in paragraph (1) of this Article if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Law.

(6) Provisions of this Article shall not apply to processing carried out by state administration bodies and authorities.

Certification

Article 46

(1) The Agency shall encourage the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Law of processing operations by controllers and processors, taking into account the specific characteristics of different sectors for personal data processing and the specific needs of micro, small and medium-sized enterprises in order to contribute to the proper implementation of this Law.

(2) The certification shall be voluntary and available via a process that is transparent.

(3) The certification pursuant to this Article shall not reduce the responsibility of the controller or the processor for compliance with this Law and is without prejudice to the tasks and powers of the Agency pursuant to Article 64 or 65 of this Law.
(4) The certification pursuant to this Article shall be issued by the Agency or by the certification bodies referred to in Article 47 of this Law, based on criteria approved by the Director of the Agency.
(5) The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 47 of this Law, with all information and access to its processing activities which are necessary to conduct the certification procedure.
(6) Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements reffered to in paragraph (4) continue to be fulfilled. The certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 47 of this Law or by the Agency, where the requirements for the certification are not or are no longer being fulfilled.
(7) The Agency shall keep a register of all certification mechanisms and data protection seals and marks and shall make them publicly available by any appropriate means.
(8) The form, content and manner of keeping the register referred to in paragraph (7) of this Article shall be adopted by the Director of the Agency.

Certification bodies

Article 47

(1) Without prejudice to the tasks and powers of the Agency under Articles 65 and 66 of this Law, the certification bodies which have an appropriate level of expertise in relation to data protection, having previously notified the Agency in order to receive approval for using their authorisation, for which, if necessary, the Agency shall issue and renew certification in compliance with Article 66 paragraph (2) item (h) of this Law.

(2) The certification bodies referred to in paragraph (1) of this Article performing certification under the provisions of this Law, shall be accredited by the Institute for Accreditation of the Republic of North Macedonia (hereinafter: the Institute), in accordance with the accreditation regulations. The certification bodies from this paragraph shall only be accredited provided that: (a) they demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the Institute;

(b) undertaken to respect the specification criteria pursuant to Article 46 paragraph (4) of this Law; (c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;
(d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(e) demonstrated, to the satisfaction of the Institute, that their tasks and duties do not result in a conflict of interests.

(3) The accreditation of certification bodies as referred to in paragraph (1) of this Article shall take place on the basis of criteria prescribed by the Director of the Agency.

(4) The certification bodies referred to in paragraph (1) of this Article shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Law. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body still meets the requirements set out in this Article.

(5) The certification bodies referred to in paragraph (1) of this Article shall provide the Agency the requested data and/or documents with the reasons for granting or withdrawing the requested certification. (6) The Institute shall revoke an accreditation of a certification body pursuant to paragraph (1) of this Article, where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Law.

(7) The Director of the Agency shall adopt technical standards for the data protection certification mechanisms and the seals and marks for personal data protection as well as the mechanisms for promotion and recognition of certification mechanisms, seals and marks.

(8) The provisions of this Article shall also apply to the certification of bodies for conducting trainings in the field of personal data protection in accordance with the provisions of this Law.

V. TRANSFER OF PERSONAL DATA

General principle for transfers

Article 48

(1) Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if the conditions laid down in this Law are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Law is not undermined.

(2) Provisions of this Chapter shall not apply for transfer of personal data from paragraph (1) of this Article from the Republic of North Macedonia to a Member State or member of the European Economic Area.

(3) The controller or processor shall notify the Agency in case of transfer of personal data to a Member State or member of the European Economic Area.

Transfer of personal data to third countries or international organisations

Article 49

(1) A transfer of personal data to a third country or an international organisation may take place where the Agency has decided that the third country or the international organisation in question ensures an adequate level of protection.

(2) When assessing the adequacy of the level of protection, the Agency shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable judgements applied to data subject and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

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

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

(3) In case when a third country or international organisation to which personal data are to be transferred ensures adequate level of data protection pursuant to paragraph (2) of this Article, then the controller or processor may conduct data transfer based on an adequacy decision made by the Agency.

(4) In case when the third country or international organisations to which personal data are to be transferred does not ensure adequate level of data protection, the controller or processor shall not conduct personal data transfer.

Transfers subject to appropriate safeguards

Article 50

(1) In the absence of a decision pursuant to Article 49 paragraph (3) of this Law, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

(2) When no decision referred to in Article 49 paragraph (3) of this Law has been made, appropriate safeguards referred to in paragraph (1) of this Article may be provided for, without requiring any specific authorisation from the Agency, by:

(a) a legally binding and enforceable instruments between public authorities or bodies;
(b) binding corporate rules in accordance with Article 51 of this Law;
(c) standard data protection clauses adopted by the Agency or approved by the European Commission;
(d) an approved code of conduct pursuant to Article 44 of this LAw together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
(f) an approved certification mechanism pursuant to Article 46 of this Law together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

(3) Subject to the authorisation from the Agency, the appropriate safeguards referred to in paragraph (1) of this Article may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

Binding corporate rules

Article 51

(1) The Agency shall approve binding corporate rules provided that they:

(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees; (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

(c) fulfil the requirements laid down in paragraph (2) of this Article.

(2) The binding corporate rules referred to in paragraph (1) of this Article shall specify at least: (a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;
(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules; (e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 26 of this Law, the right to lodge a request with the Agency and before the competent courts in accordance with law, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of the Republic of North Macedonia of liability for any breaches of the binding corporate rules by any member concerned not established in the Republic of North Macedonia. The controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 17 and

18 of this Law;

(h) the tasks of any data protection officer designated in accordance with Article 41 of this Law or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(i) the complaint procedures;

(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) of this paragraph and to the senior management of the controlling legal entity in the group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request of the Agency;

(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 any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the Agency the results of verifications of the measures referred to in point (j);

(m) the mechanisms for reporting to the Agency any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

Transfers or disclosures of personal data based on an international agreement

Article 52

Any judgment of a court or any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the third country where the controller is established of the processor has made the request and the Republic of North Macedonia, without prejudice to other grounds for transfer pursuant to this Chapter.

Derogations for a specific situation

Article 53

(1) In the absence of an adequacy decision pursuant to Article 49 paragraph (3) of this Law, or of appropriate safeguards pursuant to Article 50 of this Law, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; (c) the transfer is necessary for the conclusion or performance of a contract concluded in the

interest of the data subject between the controller and another natural or legal person;

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

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

(f) the transfer is necessary in order to protect the vital 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 law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 49 or 50 of this Law, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and

the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the Agency of the transfer. The controller shall, in addition to providing the information referred to in Articles 17 and 18 of this Law, inform the data subject of the transfer and on the compelling legitimate interests pursued.

(2) A transfer pursuant to point (g) of the first subparagraph 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 at the request of those persons or if they are to be the recipients.

(3) Points (a), (b) and (c) of the first subparagraph of paragraph (1) of this Article and the second subparagraph of paragraph (1) of this Article shall not apply to activities carried out by state administration bodies in the exercise of their public powers.

(4) The public interest referred to in point (d) of the first subparagraph of paragraph (1) of this Article shall be recognised by law to which the controller is subject.

(5) In the absence of an adequacy decision, the law of the Republic of North Macedonia may, for important reasons of public interest, expressly set limits to the transfer of special categories of personal data to a third country or an international organisation.

(6) The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph (1) of this Article in the records referred to in Article 34 of this Law.

International cooperation for the protection of personal data

Article 54

In relation to third countries and international organisations, the Agency shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

Decision-making of the Agency

Article 55

(1) In cases referred to in Article 49 paragraph (3), Article 50 paragraph (3) and Article 51 of this Law, the Agency shall issue a decision within 90 of the receipt of the request.

(2) The decision of the Agency from paragraph (1) of this Article may be appealed before competent court by initiating administrative dispute, within 30 days of receipt of the decision.

By-laws of the Agency

Article 56

The Director of the Agency shall stipulate the manner of reporting on personal data transfer to a Member State or Member of the European Economic Area, the form and content of the template of the request for obtaining approval for transfer for cases referred to in Article 49 paragraph (3), Article 50 paragraph (3) and Article 51 of this Law, as well as the form and content of the template for recording the personal data transfer to third countries and international organisations, the European Union and the European Economic Area and the manner of record-keeping.

VI. THE PERSONAL DATA PROTECTION AGENCY

1. Independent status

Supervisory authority

Article 57

(1) The Agency is an independent and autonomous state administration body responsible for monitoring the lawfulness of activities taken when processing personal data on the territory of the Republic of North Macedonia, as well as for protection of the fundamental rights and freedoms of natural persons in relation to processing of their personal data.
(2) The Agency shall be held accountable for its work before the Parliament of the Republic of North Macedonia.
(3) The Agency shall have a status of a legal entity.
(4) The seat of the Agency shall be in Skopje.

(5) The Agency has a Secretariat that performs professional, normative-legal, administrative, administrative - supervisory, supervisory, material - financial, accounting, information and other matters within the competence of the Agency (hereinafter: Secretariat).
(6) The Secretariat is headed by the secretary general.

Independence

Article 58

(1) The Agency shall be completely politically, financially and functionally independent in performing its tasks and exercising powers in accordance with this Law.

(2) The Agency, its director, deputy director and employees shall not take or request instructions from public authorities, municipal administration bodies or administration bodies of the city of Skopje or any other legal and/or natural persons.

(3) The director, deputy director and the employees of the Agency in the performance of their function and tasks are obliged to pay attention to possible conflict of interests and in the performance of public authorities and duties must not be guided by personal, family, religious, political and ethnic interests, nor from pressures and promises from a superior or other person.

(4) The independence of the Agency shall be respected at all times, and no body and/or person from paragraph (2) of this Article shall influence the director, deputy director or staff at the Agency during their exercise of powers, tasks, nor shall influence the exercise of the Agency's powers.

(5) The director, deputy director and employees of the Agency shall, in the exercise of their responsibilities and/or in their decision-making:

1) act professionally, impartially and objectively, free of any influence of controllers and processors as well as of any other interested party;
2) shall not be guided by personal, business or financial interests;
3) shall not misuse their powers and status at the Agency or as Agency staff, and 4) shall protect the reputation of the Agency.

Director and deputy director

Article 59

(1) The Agency shall be managed by a director, appointed and dismissed by the Parliament of the Republic of North Macedonia upon nomination of the Elections and Appointments Committee of the Parliament of the Republic of North Macedonia (hereinafter: the Committee).

(2) A public announcement shall be announced for election of director, published in at least two daily newspapers with national circulation, one of which is issued in a language spoken by at least 20% citizens speaking in official language different from the Macedonian.

(3) The term of office of the director of the Agency shall be five years, which may be renewable twice. (4) The director of the Agency shall have a deputy elected and dismissed by the Parliament of the Republic of North Macedonia upon nomination of the Committee with a term of office of five years, which may be renewable twice.

(5) A public announcement shall be announced for election of deputy director, published in at least two daily newspapers with national circulation, one of which is issued in a language spoken by at least 20% citizens speaking in official language different from the Macedonian.

(6) The Committee is obliged to check whether the candidates who have applied for the public announcement for director, ie deputy director meet the conditions for applying for the public announcement determined in this law.

(7) The Committee is obliged within one month after the end of the public announcement to organize a public hearing for the candidates for director or deputy director that fulfill the conditions set out in this law. (8) After the public hearing, the Committee compiles the proposed list of candidates for director or deputy director. The final draft list of candidates for director or deputy director, the Committee decides in accordance with the Rules of Procedure of the Assembly of the Republic of North Macedonia.

(9) The deputy director shall replace the director in cases of absence or in case, due to illness or other reasons, he/she is unable to execute his/her function, with all his/her management authorities and responsibilities.

(10) In coordination with the director of the Agency, the deputy director shall fulfil tasks and responsibilities assigned by the director.

(11) The director and deputy director shall be liable for their work and the performances of the Agency before the Parliament of the Republic of North Macedonia

Conditions for appointment or dismissal

Article 60

(1) A person meeting the following conditions may be eligible for director:

1) to be citizen of the Republic of North Macedonia;
2) at the time of appointing shall not have imposed on him/her conviction by a final court judgement or misdemeanour sanction with a prohibition to act in his/her profession, activity or duty;

3) has at least 240 credits under the ECTS or a completed VII/1 degree of higher education in the area of law;
4) is not member of any political party body;
5) has at least ten years of work experience following completion of higher education;
6) has at least five years of work experience, as well as professional qualifications and skills in the field of personal data protection;
7) holds a certificate of knowledge of computer programs for office work and
8) has at least one of the following internationally recognized certificates or diplomas for active command of the English language, not older than five years:

- TOEFL IBT – at least 74 points,
- IELTS – at least 6 points,
- ILEC (Cambridge English: Legal) – at least B2 level,
- FCE (Cambridge English: First) – passed,
- BULATS at least 60 points or
- APTIS – at least level B2.

(2) A person fulfilling the conditions laid down in paragraph (1) of this Article may be elected deputy director of the Agency.

(3) The term of office of the director and/or deputy director, may cease before the expiration of the mandate, in the following cases:

- if he/she resigns,
- if he/she permanently loses the ability to perform the function, as stated by the Assembly of the Republic of North Macedonia
- if he/she meets the requirements for old-age pension,
- in case of death,
- if elected or appointed to another public office or
- if he/she is dismissed from office before the end of his/her term.

(4) The function director and/or deputy director shall be terminated only on the following grounds:

- at his/her request,
- if convicted with a final court judgement for criminal offence and unconditionally sentenced to imprisonment for at least six months,
- due to misuse of personal data ascertained by the Assembly of the Republic of North Macedonia, and
- if he/she ceases to meet any of the conditions laid down in paragraph (1) lines 1, 2 and 4 of this Article ascertained by the Assembly of the Republic of North Macedonia.

(5) The Assembly of the Republic of North Macedonia in the cases referred to in paragraphs (3) and
(4) of this Article shall conclude termination of the function.

(6) The Assembly of the Republic of North Macedonia dismisses the director and/or deputy director of the Agency upon the proposal of the Committee, if one of the following conditions is met:

- it is determined that he/she does not meet the conditions referred to in paragraph (1) of this Article,

- is unjustifiably absent from work of the Agency for more than six months,
- due to misuse of personal data or
- obviously violated the rules for conflict of interest, ie exemption in situations in which the director and/or the deputy director knew or should have known about the existence of one of the grounds for conflict of interest, ie exemption provided by law.

(7) In case of termination of the function or dismissal of the director of the Agency, until the election of a new director of the Agency, the function of director of the Agency is performed by the deputy director of the Agency, with all rights, duties and authorities that the director had.

(8) In case of dismissal and/or termination of the function of the director and/or deputy director of the Agency before the expiration of the mandate, the Assembly of the Republic of North Macedonia within ten days at the latest starts a procedure for election of a new director and/or deputy director of the Agency.

Solemn statement

Article 61

Prior to assuming office, the director and/or deputy director shall declare and sign an official oath before the Parliament of the Republic of North Macedonia, stating as follows:

"I solemnly declare that I shall perform the rights and duties of the office director and/or deputy director diligently, impartially and responsibly, and in doing so I shall respect the law on protection of personal data and shall adhere to the Constitution and laws of the Republic of North Macedonia".

Incompatibility of office and confidentiality

Article 62

(1) The office of director and/or deputy director shall be incompatible with other public functions as well as with the exercise of function in a political party or workplace.

(2) The director and deputy director shall be subject to a duty of professional secrecy both during and after their term of office, with regard to any personal or confidential information which has come to their knowledge while discharging their tasks or exercising their powers, in accordance with law. The director and deputy director shall keep as professional secret in particular the information received by natural persons of infringements of provisions of this Law.

Competences of the director of the Agency

Article 63

(1) Director of the Agency:

- shall represent and act on behalf of the Agency before competent institutions, except for property rights and interests for which it is represented before courts and other institutions by the State Attorney of the Republic of North Macedonia,
- take all legal actions on behalf and for the account of the Agency,
- shall organize and ensure lawful, effective and efficient exercise of tasks and responsibilities at the Agency,
- shall decide on issues regarding rights and responsibilities of the staff of the Agency, in compliance with the Law,
- shall adopt all internal organisation and job systematisation acts of the Agency,
- shall adopt financial, that is, strategic documents and annual working program of the Agency, and shall organise their enforcement,
- shall adopt decisions in compliance with the law;
- shall adopt regulations and other acts within his/her authority, in compliance with the Law,
- shall provide for the publicity of the Agency's operations, and
- shall perform other tasks within the competence of the Agency, in compliance with the law.

(2) The by-laws, adopted by the director of the Agency, are published in the "Official Gazette of the Republic of North Macedonia".

2. Competence, tasks, powers of the Agency

Competence

Article 64

(1) The Agency shall be competent for the performance of tasks and powers assigned in accordance with the law.

(2) The Agency shall not be competent to supervise processing operations of courts acting in their judicial capacity, with the exception for supervision of lawfulness of actions taken during other personal data processing actions done by the courts, in accordance with the law.

Tasks

Article 65

(1) Without prejudice to other tasks set out under this Law, the Agency shall, on its territory:

(a) monitor and enforce the application of this Law;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing, and specifically for activities targeting children;

(c) advise, in accordance with the law, the Parliament of the Republic of North Macedonia, the Government of the Republic of North Macedonia and other institutions and bodies on the

legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Law;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Law and, if appropriate, cooperate with other supervisory authorities for personal data protection, to that end;

(f) handle requests submitted by a data subject, or by a citizen association in accordance with this Law, and investigate, to the extent appropriate, the subject matter of the requests and inform the requesting party of the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g) cooperate with, including sharing information and providing mutual assistance to, other supervisory authorities with a view to ensuring safeguards for the rights and freedoms of physical persons with regard to personal data processing;

(h) conduct investigations on the application of this Law, including on the basis of information received from another supervisory authority or other public authority;

(i) 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;

(j) adopt standard contractual clauses referred to in Article 32 paragraph (7) and Article 50, paragraph (2) point (c) of this Law;

(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 39 paragraph (4) of this Law;

(l) give advice on the processing operations referred to in Article 40 paragraph (2) of this Law; (m) encourage the drawing up of codes of conduct pursuant to Article 44 of this Law and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 44 paragraph (3) of this Law;

(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 46 of this Law;

(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 46 paragraph (6) of this Law;

(p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 45 of this Law and of the certification body pursuant to Article 47 of this Law; (q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 45 of this Law;

(r) authorise contractual clauses and provisions referred to in Article 50 paragraph (3) of this Law;

(s) approve binding corporate rules pursuant to Article 51 of this Law;

(t) establishes and maintains records of infringements of this Law and of measures taken in accordance with Article 66 paragraph (2) of this Law; and

(u) conducts training on personal data protection and

(v) fulfil any other tasks related to personal data protection, in accordance with the Law.

(2) The Agency shall facilitate the submission of request referred to in point (f) of paragraph (1) of this Article by measures such as: a template for submission of request, which can also be filled in electronically, in accordance with the law, without excluding other means of communication.

(3) The performance of the tasks referred to in paragraph (1) of this Article shall be free of charge for the data subject and, where applicable, for the data protection officer.

(4) Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the Agency may charge a reasonable fee based on administrative costs, or to refuse to act on the request. The Agency authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request. The Agency determines the fee with a decision based on the scope, time and complexity of providing the information.

(5) In addition to the tasks referred to in paragraph (1) of this Article, the Agency may:

- initiates amendments to laws and other by-laws for their harmonization with the provisions of this Law, as well as with international agreements ratified in accordance with the Constitution of the Republic of North Macedonia,

- submit proposals to the Constitutional Court of the Republic of North Macedonia for assessment of the constitutionality of the laws and the constitutionality and legality of other regulations or general acts related to the protection of personal data.

Powers

Article 66

(1) The Agency shall have the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's authorised representative, to provide any information it requires for the performance of its tasks;

(b) to carry out supervisions in accordance with this Law;

(c) to carry out a review on certifications issued pursuant to Article 46 paragraph (6) of this Law;

(d) to notify the controller or the processor of an alleged infringement of this Law;

(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with law.

(2) The Agency shall have the following corrective powers:

(a) to issue warnings to a controller or processor that intended personal data processing operations are likely to infringe provisions of this Law;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Law;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Law;

(d) to order the controller or processor to bring processing operations into compliance with provisions of this Law, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;
(f) to impose a temporary or definitive limitation including a ban on processing;
(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 20, 21 and 22 of this Law, and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 21 paragraph (2) and Article 23 of this Law; (h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 46 and 47 of this Law, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
(i) to initiate misdemeanour proceedings pursuant to this Law, together with the measures or instead of the measures listed in this paragraph, and depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in another country or to an international organisation.

(3) The Agency shall have the following powers in relation to issuing approvals or opinions:
(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 40 of this Law;
(b) to issue, on its own initiative or on request, opinions to the Parliament of the Republic of Norht Macedonia, the Government of the Republic of North Macedonia, or, in accordance with the law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;
(c) to authorise processing referred to in Article 40 paragraph (5) of this Law;
(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40 paragraph (3) of this Law;
(e) to approve criteria of certification in accordance with Article 46 paragraph (4) of this Law; (f) to issue a positive or negative opinion on the fulfilment of criteria for issuance of certificates, pursuant to Article 47 of this Law;
(g) to adopt standard data protection clauses referred to in Article 32 paragraph (7) and Article 50 paragraph (2) point (c) of this Law;

(h) to authorise contractual clauses referred to in Article 50, paragraph (3), point (a) of this Law; (i) to authorise administrative arrangements referred to in Article 50, paragraph (3), point (b) of this Law;

(j) to approve binding corporate rules pursuant to Article 51 of this Law.
(4) The exercise of the powers by the Agency pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, in accordance with the law.

(5) The Agency shall have the power to bring infringements of this Law to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Law.

(6) The Director of the Agency shall adopt guidances for actions of the controllers and processors during the processing of personal data in accordance with this Law.

(7) When using technologies for some type of processing, taking into account the nature, scope, context and purposes of data processing, it is likely the same to cause a high risk to the rights and freedoms of individuals, the Agency may publish issued decisions, opinions and indications on its website.

(8) The decisions, opinions and indications referred to in paragraph (7) of this Article shall be anonymized or pseudonymized.

Cooperation of the Agency with state administration bodies

Article 67

(1) State administration bodies shall notify the Agency of all measures taken with the goal of implementing its request, proposals, opinions, or notifications within the deadline specified by the Agency, but no later than 30 days upon receipt of the request submitted to the Agency.

(2) In case the state administration body fails to notify the Agency in accordance with paragraph (1) of this Article or only partially accepts its requests, proposals, opinions, recommendations or notifications or fails to act accordingly, the Agency shall inform of this the direct superior body, the managing official of that body of the Parliament of the Republic of North Macedonia, that is, the Government of the Republic of North Macedonia.

(3) The Parliament of the Republic of North Macedonia, that is, the Government of the Republic of North Macedonia, upon receiving the special report on the nonfeasance and failure to implement the requests, proposals, opinions, recommendations or notifications of the Agency, shall deliberate and take a position on a session mandatorily attended by the official managing the state administration body referred to in the special report, by proposing provisional measures, and shall notify the Agency of the measures taken within the deadline specified in the special report.

Record of data protection officers

Article 68

(1) The Agency shall keep records of data protection officers reffered to in Article 41 paragraph (7) which it shall publish on its webpage.
(2) The records referred to in paragraph (1) of this Article shall contain the following information:
- name and establishment of the controller, that is the processor;
- first and last name of the data protection officer;
- contact data of the data protection officer (e-mail and phone number).

Data protection training

Article 69

(1) The Agency shall prepare and carry out training for employees of the controllers and/or processors as well as for data protection officers, upon which it shall issue certificates of accomplished training, and shall keep record thereof.

(2) The purpose of the trainings is that employees of the controllers and/or processors gain knowledge in the pertinent area and so that data protection officers gain knowledge and skills about practices and regulations in the field of data protection and develop their ability to perform tasks referred to in Article 43 of this Law.

(3) The training schedule from paragraph (1) of this Article shall be published on the webpage of the Agency.

(4) Training costs referred to in paragraph (1) of this Article shall be borne by the controller and/or processor, that is, the natural person, and are in relation to the costs incurred for conducting the training.

(5) The controller and/or processor, the natural person and the data protection officer who attended the training shall be issued by the Agency a certificate of training with a validity of three years from the date of issue.

(6) The director of the Agency shall stipulate the manner in which the training is conducted referred to in this Article, the program of the data protection training, the form and content of the template of the training certificate and the manner of record-keeping of issued training certificates

(7) The training from this Article is conducted by the employees of the Agency determined by the director of the Agency.

Annual report of the Agency

Article 70

(1) The Agency shall draw up an annual report of its work, which may incorporate the list of breaches of which it was notified as well as the types of measures taken in accordance with Article 66 paragraph (2) of this Law.
(2) The Agency shall submit to the Parliament of the Republic of North Macedonia the annual report referred to in paragraph (1) of this Article for the previous calendar year the latest by March of the running year.

(3) The Agency shall publish its annual report referred to in paragraph (1) of this Article on its webpage.
(4) The Agency may also issue additional reports, upon need and at the request of the Parliament of the Republic of North Macedonia.

Notification for high-risk data processing

Article 71

(1) The controller shall notify the Agency in the event when, during use of new technologies for some type of processing, having regard to the nature, scope, context and goals of the personal data processing, possibility arises of it posing high risk for the rights and freedoms of physical persons, and in function of Article 9 paragraph (2) of this Law.
(2) The notification referred to in paragraph (1) of this Article shall contain:
1) title of the filing system;
2) name, that is, first and last name and contact data of the controller, if applicable of all joint controllers, of the authorised representative of the controller, if any, and of the data protection officer;
3) purpose or purposes of processing;
4) legal basis for establishing a filing system;
5) description of categories of data subjects and the categories of personal data pertaining to them;
6) categories of recipients to whom personal data are or will be revealed, including recipients in third countries or international organisations;
7) duration of storage of personal data, that is, stipulated deadlines for erasure of different categories of personal data;
8) transfer of personal data to a third country or international organisation; and
9) general description of implemented technical and organisational measures according to Article 36 of this Law.

(3) The Agency shall keep electronic record of high-risk filing systems which contain data from notifications received in accordance with this Article.
(4) The director of the Agency shall prescribe the form and content of the notification template, the manner of notification referred to in paragraph (1) of this Article, as well as the form and content of the record referred to in paragraph (3) of this Article.

3. Cooperation and international legal aid

Cooperation

Article 72

(1) The Agency shall cooperate with other supervisory authorities for data protection in accordance with this Law with the purpose of ensuring protection of rights and freedoms of natural persons concerning personal data processing. The Agency and the supervisory authorities concerned shall exchange all relevant information with each other by electronic means, not excluding other means of correspondence, using adequate technical and organisational measures of ensuring secrecy and data protection.

(2) The Agency may request, at any time, that other supervisory authorities concerned provide mutual assistance pursuant to Article 73 of this Law, and may conduct joint operations pursuant to Article 74 of this Law, in particular for carrying out investigations or for monitoring the implementation of measures concerning a controller or processor established outside of the Republic of North Macedonia.

Mutual assistance

Article 73

(1) The Agency and other supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Law in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

(2) The Agency shall take all appropriate measures required to reply to a request of another supervisory authority for data protection, without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

(3) Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

(4) The Agency, if requested, shall not refuse to comply with the request for mutual assistance unless:

(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or

(b) compliance with the request would infringe this Law.

(5) The Agency shall inform the requesting supervisory authority for data protection of the results or, as the case may be, of the progress of the measures taken in order to respond to the request.

The Agency shall provide reasons for any refusal to comply with a request pursuant to paragraph (4) of this Article.

(6) The Agency shall, as a rule, supply the information requested by other supervisory authorities by electronic means, not excluding other means of correspondence, using adequate technical and organisational measures of ensuring secrecy and data protection of the processing.

(7) The Agency shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. The Agency and supervisory authorities may reach agreement on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

Joint operations

Article 74

(1) The Agency may conduct joint operations with other supervisory authorities for data protection, including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities are involved in joint operations.

(2) The Agency may confer powers, including investigative powers on members or staff of the supervisory authority concerned, involved in joint operations, in accordance with the Law. Such investigative powers may be exercised only under the guidance and in the presence of Agency staff. The members or staff of the supervisory authority concerned, that are involved in the joint operations, shall be subject to the law of the Republic of North Macedonia.

(3) For the purpose of conducting joint operations with other supervisory authorities for data protection, the Agency may sign memorandum of cooperation for implementation of provisions of this Law.

Urgent procedure

Article 75

In exceptional circumstances, where the Agency deems that an urgent need has arisen to act in order to protect the rights and freedoms of data subjects, it may immediately adopt provisional measures intended to produce legal effects on the territory of the Republic of North Macedonia with a specified period of validity which shall not exceed three months, counting from the day of adoption of the provisional measures. The Agency shall, without delay, communicate the provisional measures taken and the reasons for adopting them to the other supervisory authorities concerned.

4. Secretariat

Article 76

(1) All professional, normative and legal, administrative and supervisory, material and financial, accounting, information and other matters of the Agency shall be discharged by the Agency Secretariat.

(2) The director of the Agency shall adopt the internal organisation acts and job systematisation of the Secretariat in accordance with the regulations for employees in the public sector, in which the jobs are defined, the job description and the job tasks, the total number of employees and conditions for each job.

(3) The secretary general and the employees of the Secretariat, except for maintenance and technical staff shall have the status of administrative employees.

(4) The Secretariat is headed by the secretary general of the Agency, who is elected in accordance with the regulations for administrative officials.

(5) About the issues related to the employment of the staff of the Agency, the provisions of the Law on Administrative Officials, the general regulations on labor relations and this Law are applied.

(6) The Secretariat shall act independently and impartially when performing its tasks, adhering to procedures laid down by this Law and regulations adopted thereinafter.

(7) Procedures for filling vacancies (employment, promotion and mobility through deployment or takeover) are carried out in accordance with the regulations for the administrative officials, regulations for employees in the public sector and the general regulations for labor relations, within the provided financial means in the Budget section of the Republic of North Macedonia designated for the Agency.

Salary and rewards of the employees of the Secretariat of the Agency

Article 77

Employees of the Secretariat of the Agency are entitled to monthly salary, allowances and rewards in accordance with the regulations for administrative officials and the provisions of this Law.

Confidentiality

Article 78

Agency staff shall keep as secret any personal data which has come to their knowledge in the course of the performance of their tasks for the duration of their employment with the Agency and after, which represent personal or classified information in accordance with law. Agency staff shall keep as a secret in particular the information of natural persons of infringements of provisions of this Law.

5. Funding of the Agency

Operating assets

Article 79

(1) The funds for work of the Agency shall be provided from the Budget of the Republic of North Macedonia, own revenues from fees, donations and other sources, in accordance with law.

(2) The fees collected by the Agency are:

- accreditation of body for monitoring the compliance with the Code of Conduct according to Article 45 of this Law,
- issuance of certifications according to Article 46 of this Law;
- issuing opinion for fulfilment of criteria for issuing accreditation, under Article 47 of this Law;
- fees for organized trainings under Article 69 of this Law and
- other revenues accrued by the Agency during its operations according to law.

(3) The Agency shall determine the fees referred to in paragraph (2) of this Article with a decision based on the scope and complexity for performing the authorizations determined by this Law.

(4) Own revenues referred to in paragraphs (1) and (2) of this Article shall be used for covering daily operations costs, professional development, training and other staff costs, as well as the performance of other activities, in accordance with the Law. The distribution of own revenues is done through financial plan adopted by the Director of the Agency.

(5) Auditing of the material and financial operations of the Agency shall be conducted by the State Audit Office, in accordance with law.

Budget

Article 80

(1) The means to perform the function of the Agency shall be provided from the Budget of the Republic of North Macedonia.

(2) In order to provide the funds for the work of the Agency from the Budget of the Republic of North Macedonia according to Article 79 of this Law, the Agency prepares a proposal which it submits to the Ministry of Finance in accordance with the Law on Budgets.

(3) The Director of the Agency, and in his absence the deputy director of the Agency, participates in the sessions of the working bodies of the Assembly of the Republic of North Macedonia, where the proposal for the Budget of the Republic of North Macedonia is considered, to present and explain the needs for the funds referred to in paragraph (1) of this Article.

VII. SPECIFIC OPERATIONS RELATING TO PERSONAL DATA PROCESSING

Processing and freedom of expression and information

Article 81

(1) For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, exemptions or derogations may be allowed from Chapter II (Principles), Chapter III (Rights of the data subject), Chapter IV (Controller and processor), Chapter V (Transfer of personal data), Chapter VI (Personal Data Protection Agency), as well as from provisions of this Chapter of this Law, if they are necessary to reconcile the right to protection of personal data with the freedom of expression and information

(2) Provision of paragraph (1) of this Article, shall apply in particular to the processing of personal data in the audio-visual field and in news archives and press libraries.

(3) Provisions of this Law shall not apply on processing carried out for journalistic purposes only in cases when public interest overrides the personal interest of the personal data subject.

(4) The following criteria shall apply when reconciling the right to personal data protection with the freedom of expression and information:

- the nature of personal data;
- circumstances in which data are obtained;
- impact of the published information on the discussion on public interest;
- how renowned is the physical person concerned and the subject-matter of the information;
- prior conduct of the physical person concerned;
- prior consent of the physical person concerned;
- content, form and consequences of publishing of this information.

Processing and public access to official documents

Article 82

Personal data in official documents held by a state administration body, state authorities or a legal entity exercising public authorisations may be disclosed by the authority or body in order to fulfil a task in the public interest in accordance with Law, thus reconciling public access to official documents with the right to the protection of personal data pursuant to this Law.

Processing citizen’s national identification number

Article 83

(1) The national identification number of a citizen shall be processed only:

- upon prior consent of the data subject according to Article 11 of this Law;
- for the exercise of legally binding rights or responsibilities of the data subject and the controller, and
- in other cases stipulated by law.

(2) Only after previously obtained approval by the Agency shall a systematic and extensive processing of the national identification number of the citizen be performed, according to line 1 paragraph (1) of this Article.

(3) For the cases referred to in lines 2 and 3 from paragraph (1) of this Article, the law must contain safeguards and other measures for protection of the rights and freedoms of data subjects in accordance with the provisions of this Law.

(4) For the cases referred to in paragraph (2) of this Article, the Agency shall decide with a decision within 90 days from the day of receipt of the request for obtaining approval.

(5) Against the decision of the Agency referred to in paragraph (4) of this Article, lawsuit for initiating an administrative dispute may be filed to the competent court, within 30 days from the receipt of the decision.

(6) The controller and processor shall ensure that the citizen's national identification number is not unduly made visible, printed or extracted from a filing system.

Prior approval

Article 84

(1) Processing of the following personal data shall be conducted only with prior approval of the Agency:

- data concerning health;
- genetic data, unless processing is conducted by experts for the needs of preventive medicine, medical diagnostics or care and treatment of data subject, and - biometric data.

(2) The approval referred to in paragraph (1) of this Article shall also be obtained if processing is carried out after the data subject has given explicit consent to the processing in accordance with Article 13 paragraph (2) point 1) of this Law.

(3) The approval referred to in paragraph (1) of this Article is not required in case when the processing of personal data is determined by a law which contains safeguards and other measures for protection of the rights and freedoms of data subjects in accordance with the provisions of this Law.

(4) For cases referred to in paragraph (1) of this Article, the Agency shall issue a decision within 90 days from receipt of the request for issuance of approval.

(5) The decision of the Agency referred to in paragraph (4) of this Article may be appealed before a competent court by initiating administrative dispute within 30 days from receipt of the decision.

Processing in the context of employment

Article 85

(1) The state may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the employment contract, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

(2) Rules from paragraph (1) of this Article shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity.

(3) The Agency shall issue opinion whether the specific rules referred to in paragraph (1) of this Law, provided for in the law and collective agreements, are in conformity with this Law.

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Article 86

(1) When processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, the controller shall be subject to appropriate safeguards, in accordance with this Law, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

(2) Where personal data are processed for scientific or historical research purposes or statistical purposes, the law may provide for derogations from the rights referred to in Articles 19, 20, 22 and 25 of this Law, subject to the conditions and safeguards referred to in paragraph (1) of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

(3) Where personal data are processed for archiving purposes in the public interest, the law may provide for derogations from the rights referred to in Articles 19, 20, 22, 23, 24 and 25 subject to the conditions and safeguards referred to in paragraph (1) of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

(4) Where 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 paragraphs (2) and (3) of this Article.

Processing of personal data by churches, religious communities or religious groups

Article 87

(1) Churches, religious communities or religious groups shall apply safeguarding measures when processing personal data of natural persons, in accordance with provisions of this Law.

Processing data of deceased persons

Article 88

(1) The controller may provide personal data of deceased persons only to recipients who, in accordance with the law are authorised to process these personal data.

(2) Notwithstanding Paragraph (1) of this Article, the controller shall make available data on deceased person to the person's lawful successor, with a view to fulfilling the legitimate interests in accordance with the law, provided the deceased has not prohibited the provision of such personal data in writing.

(3) The controller may provide data referred to in paragraph (2) of this Article to any other person which will process the data for scientific or historic researches or for statistical purposes, provided the deceased has not prohibited the provision of such personal data in writing, unless otherwise provided for by law.

(4) In case the deceased has not prohibited the provision of personal data referred to in paragraph (3) of this Article, the persons who are the person's legal successors may prohibit the provision of the person's data in writing, unless otherwise provided for by law.

Video surveillance

Article 89

(1) Provisions of this Law shall also apply to the processing of personal data by performing video surveillance, unless otherwise provided for by another law.

(2) The provisions of this Law shall not apply to the processing of personal data by performing video surveillance by natural persons solely for the purpose of domestic activities.

(3) The controller performing video surveillance shall publish a notice to that effect. Such notice must be clear, visible, and made public in a way that enables data subjects become informed of the video surveillance in place.

(4) The notification referred to in paragraph (3) of this Article shall contain information:

- that video surveillance is in place;
- the name/title of the controller implementing the video surveillance, and
- of the manner in which information can be obtained about the place and duration of storage of the recordings from the video surveillance system.

(5) The data subject shall be informed of the personal data processing in accordance with Articles 17 and 18 of this Law, in case a notice has been displayed in accordance with paragraphs (3) and (4) of this Article.

(6) The controller may perform video surveillance only on the area sufficient for fulfilling the goals for which it has been installed.

(7) The controller shall notify employees of the video surveillance in official or business premises.

(8) The video surveillance recordings shall be stored until the goals of surveillance are fulfilled, but for no longer than 30 days, unless another law provides for a longer period containing safeguards and other measures for protection of the rights and freedoms of data subjects in accordance with the provisions of this Law.

(9) In case of installation of cameras contrary to the provisions of this Law, the owner of the video surveillance system shall undertake measures for their removal, at his/her own expense.

Personal data processing through video surveillance system

Article 90

(1) The controller may conduct video surveillance of official or business premises if deemed necessary for:

- protection of lives or health of people;
- protection of ownership;

- protection of lives and health of employees, due to the nature of work, or - controlling the movement in and out of official or business premises.

(2) The controller shall regulate the manner of video surveillance by means of a special act.

(3) Video surveillance in changing rooms, dressing rooms, toilets and similar rooms shall be prohibited.

(4) The director of the Agency shall stipulate the form and content of the act referred to in paragraph (2) of this Article.

Video surveillance in single unit and multi-unit residential buildings

Article 91

(1) The written consent of at least 70% of the owners, that is, tenants of the housing units shall be required for the introduction of video surveillance in single-unit and multi-unit residential buildings.

(2) After providing the consent referred to in paragraph (1) of this Article, it is necessary for the owners, that is, tenants of the apartments to be informed about the start of the functioning of the video surveillance system.

(3) It shall be prohibited to transmit recordings of the video surveillance system of the single unit and multi-unit residential buildings through cable television (public or internal network), through the Internet or other electronic means of data transmission.

(4) It shall be prohibited to record entrances to individual apartments of other owners or tenants.

Analysis and periodical assessment

Article 92

(1) The controller shall perform analysis of the goal, that is, goals of the video surveillance prior to the installation process, unless otherwise provided for by law.

(2) The analysis referred to in paragraph (1) of this Article shall indicate the reasons of the video surveillance explaining the reasons for fulfilment of the goal, that is, goals, in accordance with provisions of Article 90 paragraph (1) of this Law, as well as a description of movable and immovable assets, that is of the premises which will be protected by installing the video surveillance.

(3) The controller shall conduct periodic assessment of results achieved with the video surveillance system every two years, focusing in particular on:

- the further need for use of the video surveillance system;

- the goal, that is, goals of video surveillance, and
- feasible technical solutions for replacing the video surveillance system.

(4) As part of the assessment from paragraph (3) of this Article, the controller shall prepare report as integral part of the documentation for establishing video surveillance system.

(5) The report referred to in paragraph (4) of this Article shall include, as a rule, statistical indicators on the access to the recordings made during the video surveillance, as well as the purpose of the recordings.

(6) The form and content of the analysis referred to in paragraph (1) of this Article and the report on the periodic assessment of the results achieved with the video surveillance system shall be prescribed by the director of the Agency.

Request for confirming violation of the right of personal data protection related to processing of personal data involving video surveillance

Article 93

(1) In cases when a natural person submits a request for confirming a violation of the right of personal data protection related to processing of personal data involving video surveillance in single unit and multi-unit residential buildings, the requesting party shall indicate data of the natural person who is subject of the request, in particular the person's first and last name and address, that is, the legal entity's name and establishment.

(2) In case of absence of data referred to in paragraph (1) of this Article from the request, the requesting party shall, upon request of the supervisors, submit the requested data within eight days from receipt of the request.

(3) In case of failure to submit data in accordance with paragraph (1) of this Article, that is, failure to supplement the request within the specified deadline, resulting in failure to act upon it, it shall be deemed that no request has been submitted, of which the supervisor shall issue a decision to reject the request that does not contain legal remedy.

(4) In case a request was submitted in reference to paragraph (1) of this Article, the natural person, that is, the legal entity against whom the request was submitted shall, upon the request of the supervisor, submit evidence related to the request, and in particular:

- a print screen of the monitor showing video surveillance cameras, along with photographs of the position of the surveillance cameras, or

- a sworn notary statement that no video surveillance is performed on premises which are owned or are in possession of the requesting party, in relation to which the request was made, or

- an oral statement that no video surveillance is performed on premises which are owned or are in possession of the requesting party, in relation to which the request was made, which shall be recorded in the minutes prepared by the supervisor.

(5) Upon submission of evidence referred to in paragraph (4) of this Article, the supervisor shall conduct supervision in accordance with provisions of this Law.

Providing personal data to recipients

Article 94

(1) The controller shall make available personal data to recipients, based on a written request of the recipient, in case the recipient is authorised to process that personal data, in accordance with the Law.

(2) In case the obligation for providing personal data to a recipient is laid down by law and takes place with the planned dynamics, the recipient shall not submit a written request to the controller in accordance to the provisions of this Law.

(3) The written request referred to in paragraph (1) of this Article shall include the reasons, legal grounds for use of personal data, category of data subjects and categories of personal data requested.

(4) The request from paragraph (1) of this Article may be submitted electronically in accordance with the law.

(5) It shall be prohibited to make available personal data to recipients whose processing, that is use, cannot be conducted in accordance with provisions of Articles 10 and 13 of this Law and if the purpose for which personal data are requested is in breach of Article 9 paragraph (1) line 2 of this Law.

(6) Personal data processed for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes shall not be disclosed to a recipient in a form which permits the identification of the data subject.

(7) In cases referred to in paragraphs (1) and (2) of this Article, the controller shall keep separate record of personal data provided, the data recipient, the category of data subjects, and the legal grounds and reason for which the personal data have been disclosed to the recipient.

(8) Personal data from this Article may be used only for the duration necessary for fulfilment of the specified purpose provided for by law.

(9) Upon expiry of the deadlines referred to in paragraph (8) of this Article, personal data shall be erased, unless otherwise provided for by law.

Exchange of personal data

Article 95

Provisions of Article 94 of this Law for providing personal data for use also pertain to exchange of personal data between state administration bodies and authorities, unless otherwise provided for by law.

Direct marketing

Article 96

The processing of personal data for the purposes of direct marketing, which includes profiling to the extent that it is related to direct marketing, is allowed only if the personal data are processed after the data subject has given explicit consent in accordance with Article 11 of this Law.

VIII. JUDICIAL REMEDY AND LIABILITY

Right to file request to the Agency

Article 97

(1) Every data subject shall have the right to file a request with the Agency if the data subject considers that the processing of personal data relating to him or her infringes provisions of this Law, without prejudice to any other administrative or judicial remedy.

(2) The Agency shall inform the complaining party of the progress and outcome of the procedure, including the possibility of a judicial remedy pursuant to Article 98 of this Law.

(3) The form and content of the request template referred to in Article (1) of this Law shall be presribed by the director of the Agency.

(4) The Agency shall decide whether to reveal, during the procedure, personal data of the complaining party, to the contesting party as well as to the witness.

(5) The Agency shall initiate supervision in accordance with provisions of this Law for the filed request referred to in paragraph (1) of this Article.

Right to effective judicial remedy against decisions of the Agency

Article 98

(1) Each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them, without prejudice to any other administrative or non-judicial remedy.

(2) Without prejudice to any other administrative or non-judicial remedy, every data subject has the right to effective judicial protection, when the Agency in accordance with the competencies determined in Articles 65 and 66 of this Law has not acted upon the request or has not

informed the personal data subject within three months for the outcome of the procedure upon the submitted request according to Article 97 of this Law.

Right to an effective judicial remedy against a controller or processor

Article 99

(1) Without prejudice to any available administrative or non-judicial remedy, including the right to submit a request to the Agency in accordance with Article 97 of this Law, every data subject shall have the right to effective judicial protection when it considers that his/her rights determined by this Law have been violated, as a result of the processing of his/her personal data contrary to this Law.

(2) The data subject shall exercise its right referred to in paragraph (1) of this Article by filing a lawsuit to the competent court in accordance with law.

Representation of data subjects

Article 100

(1) The data subject shall have the right to mandate a citizen association to lodge the request on his or her behalf in relation to personal data protection, in order to exercise the rights referred to in Articles 97, 98 and 99 of this Law, and, if provided for by law, to exercise the right to compensation referred to in Article 98 of this Law.

(2) The statute of the citizen association referred to in paragraph (1) of this Article established in accordance with law, shall mandatorily indicate their goals which serve the public interest, its nonprofit character, as well as that the association is active in the field of data protection and protection of the rights and freedoms of data subjects.

Right to compensation and liability

Article 101

(1) Any person who has suffered material or non-material damage as a result of an infringement of this Law is entitled to compensation from the controller or processor for the damage suffered.

(2) Any controller involved in the data processing shall be liable for the damage caused by processing which infringes this Law. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Law specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

(3) A controller or processor shall be exempt from liability under paragraph (2) of this Article if it proves that it is not in any way responsible for the event giving rise to the damage.

(4) Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs (2) and (3) of this Law, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

(5) Where a controller or processor has, in accordance with paragraph (4) of this Article, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions stipulated by paragraph (2) of this Article.

(6) Court proceedings for exercising the right to receive compensation shall be brought before a competent court in accordance with the law.

IX. SUPERVISION OVER DATA PROTECTION

Domain and authorisation for supervision

Article 102

(1) Supervision of data protection within the meaning of this Law is a systematic and independent oversight over the lawfulness of activities taken when processing personal data and their protection in application of this Law and regulations pursuant to this Law, which in particular includes investigation, verification, giving guidelines and prevention of controllers and processors (hereinafter: supervision).

(2) The supervision shall be conducted by the Agency via the data protection supervisors (hereinafter: supervisors).

(3) The supervisors performing supervision, in addition to the general conditions established for employment in accordance with the regulations for administrative officials, shall also have higher education in the field of law on information science.

(4) The supervisors are administrative officials.

Official ID

Article 103

(1) The Agency shall issue the supervisor an official ID which shall prove its official capacity which the supervisor shall present when conducting supervision.

(2) The form and content of the official ID referred to in paragraph (2) of this Article and the procedure of its issuance and revocation shall be prescribed by the director of the Agency.

Types of supervision

Article 104

(1) A supervisor may conduct the following types of supervision:
- regular supervision,
- irregular supervision, and - control supervision.

(2) Regular supervision is conducted with prior announcement in accordance with annual supervision program adopted by the director of the Agency the latest by the end of the calendar year, for the following year.

(3) Irregular supervision, as a rule, is an unannounced supervision and is performed in the case of a filed request in accordance with provisions of Articles 93, 97 and 100 of this Law, upon an initiative submitted by a state administration body, legal or natural person, ex officio or in case of suspicion of the supervisor of infringement of provisions of this Law.

(4) Control supervision may be conducted by the supervisor no later than six month upon expiry of the final deadline set for removal of observed infringements referred to in the decision from article 107 paragraph (4) of this Law.

(5) The supervision referred to in paragraph (1) of this Article, based on the method and means employed, may be conducted electronically.

(6) The supervision referred to in paragraph (1) of this Article shall take place on premises of the controller, that is, processor where personal data are processed, or/and on premises of the Agency.

(7) The director of the Agency shall prescribe the supervision procedure referred to in paragraph (1) of this Article, also the form, content and manner of keeping records of performed supervisions.

Rights of the supervisor
Article 105

In exercising supervision, the supervisor may:

- review general and individual acts, files, documents, computer records, information and other large-scale evidence, according to the subject of supervision, and to seek and keep copies of them in paper or electronic form, free of charge;
- control business premises and other facilities where personal data are processed and conduct an inquiry in their processing;
- request for an inquiry in the personal identification documentation in order to verify their identity in accordance with the Law;
- request for written or oral explanation from the controller i.e. processor in relation to issues related to the supervision;
- request to prepare an expert analysis and opinion related to the conducted supervision;
- use technical equipment intended for taking photographs and to provide video records which may be used in the supervision;
- examine the equipment for data processing and the equipment where personal data are stored, as well as examine the information system and information infrastructure within which personal data are processed, with an authorized representative of the controller, i.e. processor;
- use the communication devices of the controller, i.e. processor in order to fulfil the goals of the supervision, and

- provide other necessary evidence according to the supervision subject.

Responsibilities of the controller and processor during supervision

Article 106

The controller, that is, processor, shall make the supervision fully available to the supervisor, and shall in particular:

- make visually available all documents, data and information (in hard copy or electronic form) necessary for the supervision, and to ensure a copy of them if necessary;
- enable the presence of all responsible, that is, authorised persons necessary for the supervision to be conducted;
- provide proper work conditions for undisturbed work and to establish the factual state, and
- enable access to premises and equipment where personal data are processed or are related to data processing and are subject to supervision.

Minutes and measures in case of infringement of regulations

Article 107

(1) The supervisor, within 30 days from the day when the supervision is finalised, shall prepare minutes of the conducted regular or irregular supervision indicating the factual state and found infringements, which he/she shall deliver to the controller, that is, processor.

(2) If no infringement of data protection regulations is found during supervision or the infringement has been removed in the course of supervision or until the adoption of decision for removal of the infringements found during supervision, the supervisor shall adopt a decision for suspension of the procedure, subject to complaint by a dissatisfied party by initiating administrative dispute to the competent court within 30 days upon receipt of the decision.

(3) Notwithstanding paragraph (2) of this Article, in case of supervision conducted in accordance with Articles 97 and 100 of this Law, infringements are found of personal data protection regulations which are removed in the course of supervision or until the adoption of decision for removal of the infringements found during supervision, the supervisor, instead of a decision for suspension of the procedure referred to in paragraph (2) of this Article, shall adopt a decision acknowledging the request referred to in Articles 97 and 100 of this Law and shall establish an infringement of data protection regulations, subject to complaint by a dissatisfied party by initiating administrative dispute to the competent court within 30 days upon receipt of the decision.

(4) With the purpose of removal of the identified infringements, the supervisor shall adopt a decision which shall, in particular stipulate the following measures:

- completion, update, correction, disclosure or provision of personal data secrecy;
- implementation of additional technical and organizational measures for ensuring secrecy and protection of data processing;

- prohibition for further data processing;
- freezing of the data transfer in other countries or international organizations;
- provision of data and their transfer to other entities,
- blocking, deletion or annihilation of the personal data,
- disassembly, transfer or removal of equipment, devices, installations and systems used for data processing,
- deadline for adoption of documentation i.e. regulations in accordance with the provisions of this Law, and
- deadline for removal of infringements or
- other measures according to Article 66 paragraph (2) of this Law.

(5) If the decision referred to in paragraph (4) of this Article determines a deadline for the controller or processor to take appropriate action in accordance with this Law, he/she shall notify the Agency of the action taken, upon expiry of the stipulated deadline, and to provide appropriate evidence.

(6) The decision referred to in paragraph (4) of this Article may be subject to complaint by initiating administrative dispute to the competent court within 30 days upon receipt of the decision.

(7) Provisions of this Article shall apply also for the filed request in accordance with Article 93 of this Law.

Minutes of control supervision

Article 108

(1) Minutes shall be prepared of the conducted control supervision in which the supervisor shall note that the controller, that is, processor, acted wholly or partially or did not act upon a decision from the conducted regular or irregular supervision.

(2) In case of partial or absence of action upon a decision, the supervisor shall initiate misdemeanour procedure in accordance with this Law and the Law on Misdemeanours.

Initiating misdemeanour procedure

Article 109

(1) If during conduction of the supervision, the supervisor establishes infringement of this Law, he/she shall submit a request for initiating misdemeanour procedure to the Misdemeanor commission, in accordance with this Law and the Law on Misdemeanours.

(2) If, in the course of regular supervision, the inspector establishes an infringement of this or another law, by decision referred to in Article 107, paragraph (4) of this Law, he/she shall stipulate a deadline for removal of the infringement. After the expiry of the deadline laid down in the decision, the supervisor may enforce control supervision, in accordance with this Law.

X. MISDEMEANOUR PROVISIONS

Misdemeanours of category I

Article 110

(1) A fine amounting up to 2% of the total annual turnover of the controller or processor - legal entity, (in the absolute amount) accrued in the business year preceding the year when the misdemeanour was committed or of the total revenue accrued for a period shorter than a year preceding the year when the misdemeanour was committed in case the legal entity started to operate during that year, shall be imposed for misdemeanour on the legal entity, in case it:

1) does not provide conditions for verification that consent is given by the holder of parental responsibility over the child in relation to the services of the information society according to the provisions of Article 12 of this Law;

2) performs processing for which the identification of the data subject is not required contrary to the provisions of Article 15 of this Law;

3) does not apply data protection by design and by default according to the provisions of Article 29 of this Law;

4) does not fulfill the obligations regarding the actions of joint controllers according to the provisions of Article 30 of this Law;

5) does not appoint an authorized representative of a controller or processor not established in the Republic of North Macedonia according to the provisions of Article 31 of this Law;

6) when hiring processors, acts in a manner contrary to the provisions of Article 32 of this Law;

7) performs processing without given instructions by the controller contrary to the provisions of Article 33 of this Law;

8) does not keep records of processing activities according to the provisions of Article 34 of this Law;

9) does not cooperate with the Agency at its request according to the provisions of Article 35 of this Law;

10) does not fulfill the obligation for security of processing according to the provisions of Article 36 of this Law;

11) does not fulfill the obligation to notify the personal data breach according to the provisions of Article 37 of this Law;

12) does not fulfill the obligations to communicate the personal data breach to the data subject according to the provisions of article 38 of this Law;

13) does not carry out data protection impact assessment according to the provisions of Article
39 of this Law;

14) does not perform prior consultation according to the provisions of Article 40 of this Law;

15) does not fulfill the obligation to appoint a data protection officer according to the provisions of Article 41 of this Law;

16) does not fulfill the obligations for securing the position of the data protection officer according to the provisions of Article 42 of this Law;

17) does not provide conditions for performing the activities of the data protection officer according to the provisions of Article 43 of this Law;

18) does not fulfill the obligation regarding the provision of personal data to recipients in accordance with the provisions of Article 94 of this Law;

19) processes personal data for the purposes of direct marketing contrary to the provisions of
Article 96 of this Law and

20) does not allow for supervision to be performed under the provisions of Article 106 of this Law.

(2) A fine in the amount of 300 to 500 euros in mkd equivalent shall be imposed on the responsible person at the legal entity for the misdemeanor referred to in paragraph (1) of this Article.

(3) A fine in the amount of 100 to 500 euros in mkd equivalent shall be imposed on an official in the state administration body for a misdemeanour referred to in paragraph (1) of this Article.

(4) A fine in the amount of 100 to 250 euros in mkd equivalent shall be imposed on a natural person-controller or processor for a misdemeanour referred to in paragraph (1) of this Article.

(5) A fine amounting up to 2% of the total annual revenue of a code of conduct compliance monitoring body (in the absolute amount) accrued in the business year preceding the year when the misdemeanour was committed or of the total revenue accrued for a period shorter than a year preceding the year when the misdemeanour was committed in case the body started to operate during that year, shall be imposed for misdemeanour if it acts in a manner which infringes provisions of Article 45 paragraph (4) of this Law.

(6) A fine in the amount of up to 2% of the total annual revenue of the certification body (in the absolute amount) accrued in the business year preceding the year when the misdemeanour was committed or of the total revenue accrued for a period shorter than a year preceding the year when the misdemeanour was committed in case the body started to operate during that year, shall be imposed for misdemeanour if it acts in a manner which infringes provisions of Article 46 and 47 of this Law.

(7) A fine in the amount of 300 to 500 euros in mkd equivalent shall be imposed on the responsible person at the certification body, that is, on the responsible person within the body which implements monitoring of compliance with the code of conduct referred to in paragraphs (5) and (6) of this Article.

Misdemeanours of Category II

Article 111

(1) Fine in the amount of up to 4% of the total annual turnover of the controller or processor - legal entity, (in the absolute amount) accrued in the business year preceding the year when the misdemeanour was committed or of the total revenue accrued for a period shorter than a year

preceding the year when the misdemeanour was committed in case the legal entity started to operate during that year, shall be imposed for misdemeanour on the legal person, in case it:

1) does not act according to the principles related to the processing of personal data provided in the provisions of Article 9 of this Law;
2) does not perform lawfull processing according to the provisions of Article 10 of this Law;
3) does not provide the conditions for consent according to the provisions of Article 11 of this Law;
4) performs processing of special categories of personal data contrary to the provisions of Article 13 of this Law;
5) does not fulfill the obligations for exercising the rights of the data subject according to the provisions of Article 16 of this Law;
6) does not provide information to the data subject when collecting his personal data according to the provisions of Article 17 of this Law;
7) does not provide information to the data subject when the personal data are not obtained from him/her according to the provisions of Article 18 of this Law;
8) does not provide access to the data subject according to the provisions of Article 19 of this Law;
9) does not perform rectification of personal data according to the provisions of Article 20 of this Law;
10) does not fulfill the obligations for the right of erasure (right to be forgotten) according to the provisions of Article 21 of this Law;
11) does not enable restriction of processing of personal data according to the provisions of
Article 22 of this Law;
12) does not fulfill the obligation for notification regarding rectification or erasure of personal data or restriction of processing according to the provisions of Article 23 of this Law;
13) does not enable data portability according to the provisions of Article 24 of this Law;
14) does not act upon a submitted objection according to the provisions of Article 25 of this Law;
15) does not fulfill the obligations for regulation of automated individual decision-making, including profiling according to the provisions of article 26 of this law;
16) does not apply appropriate technical and organizational measures according to the provisions of Article 28 of this Law;
17) does not act according to the general principle for transfer of personal data provided in the provisions of Article 48 of this Law;
18) performs transfer of personal data on the basis of an adequacy decision contrary to the provisions of Article 49 of this Law;
19) performs transfer of personal data which is subject to appropriate safeguards contrary to the provisions of Article 50 of this Law;

20) performs transfer of personal data on the basis of binding corporate rules contrary to the provisions of Article 51 of this Law;

21) performs transfer or discloses personal data contrary to the provisions of Article 52 of this Law;

22) performs transfer of personal data for specific situations contrary to the provisions of Article 53 of this Law;

23) does not allow exercise of the investigative powers of the Agency according to the provisions of Article 66 paragraph (1) of this Law;

24) does not act upon the corrective powers of the Agency according to the provisions of Article 66 paragraph (2) of this Law;

25) processes the citizen's national identification number contrary to the provisions of Article 83 of this Law;

26) performs processing of personal data without previously obtained approval from the Agency according to the provisions of Article 84 paragraph (1) of this Law;

27) does not apply safeguards according to the provisions of Article 86 paragraph (1) of this
Law and

28) processes data of deceased persons contrary to the provisions of Article 88 of this Law.

(2) A fine in the amount of 300 to 500 euros in mkd equivalent shall be imposed on the responsible person at the legal entity for misdemeanours referred to in paragraph (1) of this Article.

(3) Fine in the amount of 100 to 500 euros in mkd equivalent shall be imposed on the official person within a state administration body for a misdemeanour referred to in paragraph (1) of this Article.

(4) A fine in the amount of 100 to 250 euros in mkd equivalent shall be imposed on a natural person - controller or processor for misdemeanour referred to in paragraph (1) of this Article.

Misdemeanours – video surveillance

Article 112

(1) Fine in the amount of 1,000 to 10,000 euros in mkd equivalent shall be imposed for misdemeanour on the legal entity-controller, in case it:

1) performs video surveillance contrary to the provisions of Article 89 of this Law;

2) processes personal data through a video surveillance system contrary to the provisions of Article 90 of this Law;

3) performs video surveillance in single-unit and multi-unit residential buildings contrary to the provisions of Article 91 of this Law; and

4) does not perform analysis and periodic assessment according to the provisions of Article 92 of this Law.

(2) A fine in the amount of 100 to 500 euros in mkd equivalent, shall be imposed on the responsible person at the legal entity for misdemeanours referred to in paragraph (1) of this Article.

(3) Fine in the amount of 100 to 500 euros in mkd equivalent, shall be imposed on the official person within a state administration body for a misdemeanour referred to in paragraph (1) of this Article.

(4) Fine in the amount of 100 to 250 euros in mkd equivalent, shall be imposed on the natural person-controller or processor for misdemeanour referred to in paragraph (1) of this Article.

Sentencing fines

Article 113

(1) When sentencing fines, in each specific case the following elements shall be taken into consideration:

a) the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

b) the intentional or negligent character of the infringement;

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

d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 29 and 36 of this Law;

e) any relevant previous infringements by the controller or processor;

f) the degree of cooperation with the Agency, in order to remedy the infringement and mitigate
the possible adverse effects 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 if so to what extent, the controller or processor notified the infringement;

i) where measures referred to in Article 66 paragraph (2) of this Article have previously been issued against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

j) adherence to approved codes of conduct pursuant to Article 44 of this Law or approved certification mechanisms pursuant to Article 46 of this Law; and

k) any other aggravating or mitigating factors applicable to the circumstances of the case, such

as financial benefits gained, or losses avoided, directly or indirectly, from the infringement

(2) If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Law, the total amount of the fine shall not exceed the amount specified for the gravest infringement.

Misdemeanour jurisdiction

Article 114

(1) For misdemeanours referred to in Article 110, 111 and 112 of this Law the misdemeanour procedure shall be initiated and misdemeanour sanction shall be imposed by the Agency (hereinafter: the Misdemeanour body).

(2) The misdemeanour procedure referred to in paragraph (1) of this Article shall be conducted by the Commission for deciding on misdemeanours (hereinafter: Commission for misdemeanours) established by the director of the Agency.

(3) The Commission for misdemeanours shall be comprised of two members and the
Commission president, and their substitutes.

(4) Commission members and substitutes shall have higher education and working experience of at least one year in the subject matter, of which at least one shall be a lawyer with a passed bar exam.

(5) The mandate of Commission members and their substitutes shall be two years with the right to re-election.

(6) In addition to the members and substitutes of the Commission for misdemeanours, the director of the Agency may appoint a secretary of the Commission for misdemeanour, which shall perform administrative matters for the Commission.

(7) The Commission for misdemeanours shall adopt its Rules of procedure.

(8) The Commission for misdemeanour shall have the right to present evidence and collect data necessary for establishing the case related to the misdemeanour, and to perform other tasks and bring actions provided for by this law, the Law on Misdemeanour and/or other laws.

Judicial protection in misdemeanour procedure

Article 115

(1) Against the decision of the Commission for misdemeanours, the use of a legal remedy is allowed in accordance with the Law on Misdemeanors.

Statute of limitation

Article 116

(1) The misdemeanor procedure cannot be initiated or conducted if two years have passed from the day when the violation of a right guaranteed by this law has been committed.

(2) The statute of limitation period shall start from the day when the misdemeanour was committed.

(3) The statute of limitation period shall be ceased for a period during which, according to the law, misdemeanour proceedings cannot be commenced nor continued.

(4) The statute of limitation period shall be ceased with every procedural action taken with the purpose of prosecution of the offender.

(5) The statute of limitation period shall also be ceased if the offender commits an equally serious or graver misdemeanour during the statute of limitation period.

(6) The statute of limitation period shall resume following every cessation.

(7) The statute of limitation period shall stop by all means when, double the time stipulated by
law for duration of the statute of limitation period, has lapsed.

XI. TRANSITIONAL AND FINAL PROVISIONS

Initiated procedures

Article 117

(1) Procedures of inspection supervision, that is, misdemeanour procedures initiated before the entry into force of this Law shall be finalised in accordance with provisions of this Law, in case they are more favourable for the controller, that is, processor.

(2) Administrative procedures initiated before the entry into force of this Law shall be finalized in accordance with provisions of the Law on General Administrative Procedure ("Official Gazette of the Republic of Macedonia" no. 124/15) and the Law on Personal Data Protection ("Official Gazette of the Republic of Macedonia" no.7/2005, 103/2008, 124/10, 135/11, 43/14, 153/15, 99/16 and 64/18), in case they are more favourable for the parties.

(3) The undertaken actions related to the inspection supervisions that started before the day of entry into force of this Law, will be completed in accordance with the provisions of the Law on Personal Data Protection ("Official Gazette of the Republic of Macedonia" No. 7/2005, 103/2008, 124/10, 135/11, 43/14, 153/15, 99/16 and 64/18) and the regulations adopted on the basis of that law.

Transitional regime of the Agency

Article 118

(1) The Directorate for Personal Data Protection, with the entry into force of this Law, shall continue its operations as the Personal Data Protection Agency.

(2) The employees of the Directorate for Personal Data Protection with the day of entry into force of this Law continue to work in the Agency.

(3) On the day this Law enters into force, the Agency shall take over the objects, archives, material, technical, spatial and other means of work necessary for the implementation of this Law from the Directorate for Personal Data Protection.

(4) The Agency shall bring its operation in line with provisions of this Law within 18 months from the day of entry into force of this Law.

(5) The Central register of filing systems of personal data established by the Law on Personal Data Protection ("Official Gazette of the Republic of Macedonia" No. 7/2005, 103/2008, 124/10, 135/11, 43/14, 153/15, 99/16 and 64/18) will continue to function as a record of filing systems of personal data with high risk in accordance with the provisions of this Law, whereby the controllers are obliged within 18 months from the day of entry into force of this Law to submit a notification for the reported filing systems, according to the provisions of Article 71 of this Law. After the accession of the Republic of North Macedonia to the European Union, the provisions of Article 71 of this Law that refer to the keeping of records of filing systems of personal data with high risk shall cease to apply, whereby the data contained in the records shall be permanently stored in accordance with the regulations for archival material.

(6) The director and deputy director of the Agency, with the day of entry into force of this Law, shall continue discharging their responsibilities as director and deputy director of the Personal Data Protection Agency until expiry of their mandate in accordance with the Law on Personal Data Protection ("Official Gazette of the Republic of Macedonia" no.7/2005, 103/2008, 124/10, 135/11, 43/14, 153/15, 99/16 and 64/18).

(7) The Agency is the legal successor of all rights and obligations of the Directorate for Personal Data Protection.

Alignment period

Article 119

Controllers and processors shall bring their operations in line with provisions of this Law within 18 months from the day of entry into force of this Law.

Alignment with the regulations governing the collection, processing, storage, use and submission of personal data

Article 120

The laws and other acts which regulate the collection, processing, storage, use and submission of personal data shall be aligned with provisions of this Law within 18 months from the day of entry into force of this Law.

Period of adoption of by-laws

Article 121

(1) The by-laws pursuant to this Law shall be enacted by the director of the Agency within 18 months from the day of entry into force of this Law.

(2) Until the day of commencement of the application of the regulations referred to in paragraph (1) of this Article, the existing regulations shall be applied if they are not in conflict with the provisions of this Law.

Termination of application

Article 122

The provisions of Chapter II (except Article 12), III, IV (except Articles 46 and 47), V and VIII of this Law shall cease to apply with the accession of the Republic of North Macedonia to the European Union.

Termination of validity

Article 123

The Law on Personal Data Protection ("Official Gazette of the Republic of Macedonia" no.7/2005, 103/2008, 124/10, 135/11, 43/14, 153/15, 99/16 and 64/18) shall be repealed as of the day when this Law enters into force.

Entry into force

Article 124

This Law shall enter into force on the eighth day following its publishing in the "Official Gazette of the Republic of North Macedonia".