LAW

OF THE REPUBLIC OF ARMENIA

Adopted on 18 May 2015

ON PROTECTION OF PERSONAL DATA

CHAPTER 1

GENERAL PROVISIONS

Article 1. Subject matter of the Law

1. This Law shall regulate the procedure and conditions for processing personal data, exercising state control over them by state administration or local self-government bodies, state or community institutions or organisations, legal or natural persons.

2. Characteristics pertaining to personal data constituting state and official, banking, notarial, insurance secrecy, legal professional privilege, those used in the course of operations concerning national security or defence, as well as those used in the fight against money laundering and terrorism, operational-intelligence activity and proceedings shall be regulated by other laws.

3. The restrictions of processing of personal data prescribed by this Law shall not cover the personal data being processed exclusively for journalism, literary and artistic purposes.

4. Characteristics for processing of, exercising control over personal data may be prescribed by other laws. In case a body exercising control is prescribed by other laws, the authorised body shall exercise its powers as prescribed by this Law.

Article 2. Legislation of the Republic of Armenia on personal data

1. Relations pertaining to the processing of personal data shall be regulated by the Constitution of the Republic of Armenia, international treaties of the Republic of Armenia, this Law, and other laws.

Article 3. Main concepts of the Law

1. The following main concepts shall be used in this Law:

(1) **"personal data"** shall mean any information relating to a natural person, which allows or may allow for direct or indirect identification of a person's identity;

(2) **"processing of personal data"** shall mean any operation or set of operations, irrespective of the form and mode of implementation (including automated, with or without use of any technical means) thereof, which is related to the collection either stipulation or input or systematisation or organisation or storage or use or alteration or restoration or transfer or rectification or blocking or destruction of personal data or to carrying out other operations;

(3) **"transfer of personal data to third parties"** shall mean an operation aimed at transferring personal data to certain scope of persons or public at large or at familiarising with them, including disclosure of personal data through the mass media, posting in information communication networks or otherwise making personal data available to other person;

(4) **"use of personal data"** shall mean an operation performed upon personal data, which may be directly or indirectly aimed at delivering decisions or forming opinions or acquiring rights or granting rights or privileges or restricting or depriving of rights or achieving other purpose, which give rise or may give rise to legal consequences for the data subject or third parties or otherwise relate to the rights and freedoms thereof;

(5) **"processor of personal data"** shall mean a state administration or local self-government body, state or community institution or organisation, legal or natural person, which organise and/or carries out processing of personal data;

(6) **"data subject"** shall mean a natural person to whom the personal data relate;

(7) **"database"** shall mean a set of personal data systematised by certain features;

(8) **"information system"** shall mean a set of personal data included in the database, set of information technologies or technical means used for their processing by electronic or non-electronic mode;

(9) **"depersonalisation of personal data"** shall mean operations, which render it impossible to identify the data subject to whom they belong;

(10) **"blocking of personal data"** shall mean temporary suspension of the possibility to collect or fix or systematise or transfer or use personal data;

(11) **"destruction of personal data"** shall mean an operation, which renders the restoration of the content of personal data contained in an information system impossible;

(12) **"data on personal life"** shall mean information on personal life, family life, physical, physiological, mental, social condition of a person or other similar information;

(13) **"biometric personal data"** shall mean information characterising the physical, physiological and biological characteristics of a person;

(14) **"special category personal data"** shall mean information relating to race, national identity or ethnic origin, political views, religious or philosophical beliefs, a trade-union membership, health and sex life of a person;

(15) **"publicly available personal data"** shall mean information, which, by the data subject's consent or by conscious operations aimed at making his or her personal data publicly available, becomes publicly available for certain scope of persons or public at large, as well as information, which is provided for by law as publicly available information;

(16) **"authorised person"** shall mean a legal or natural person, state administration or local self-government body, state or community institution or organisation, which was assigned by the data processor to collect, input, systematise or otherwise process personal data in cases prescribed by law or on the basis of an agreement;

(17) **"third party"** shall mean any person, body, institution or organisation other than the data subject, processor of personal data or authorised person and whose rights or legitimate interests are affected or may be affected due to the processing of personal data.

CHAPTER 2

BASIC PRINCIPLES FOR PROCESSING PERSONAL DATA

Article 4. Principle of lawfulness

1. The processor of personal data shall be obliged to follow and ensure that the data are processed in observance of the requirements of the law.

2. Personal data shall be processed for legitimate and specified purposes and may not be used for other purposes without the data subject's consent.

Article 5. Principle of proportionality

1. The processing of data must pursue a legitimate purpose, measures to achieve it must be suitable, necessary and moderate.

2. The processor of personal data shall be obliged to process the minimum volume of personal data that are necessary for achieving legitimate purposes.

3. The processing of personal data that are not necessary for the purpose of processing of data or are incompatible with it shall be prohibited.

4. The processing of personal data shall be prohibited where the purpose of processing of data is possible to achieve in a depersonalised manner.

5. Personal data must be stored in such a way as to exclude the identification thereof with the data subject for a period longer than is necessary for achieving predetermined purposes.

Article 6. Principle of reliability

1. The personal data being processed must be complete, accurate, simple and, where necessary, kept up to date.

Article 7. Principle of minimum engagement of subjects

1. The processing of personal data shall be carried out under the principle of minimum engagement of subjects.

2. Where the state administration or local self-government body, the notary are able to obtain the personal data from other body through a uniform electronic information system, personal data subject shall not be required to submit personal data necessary for certain operations.

3. In case of a written consent of the personal data subject, natural or legal persons considered as a processor of personal data may obtain from a state or local self-government body personal data necessary for a certain operation and directly specified in the written consent of a personal data subject.

4. The procedure for the transfer of personal data through an electronic information system shall be prescribed by the Government of the Republic of Armenia.

CHAPTER 3

PROCESSING OF PERSONAL DATA

Article 8. Lawfulness of processing personal data

1. The processing of personal data shall be lawful, where:

(1) the data have been processed in observance of the requirements of the law and the data subject has given his or her consent, except for cases directly provided for by this Law or other laws; or

(2) the data being processed have been obtained from publicly available sources of personal data.

Article 9. Data subject's consent

1. The data subject may give his or her consent in person or through the representative, where the power of attorney specifically provides for such a power.

2. The data being processed on the basis of consent shall be stored for the period objectively necessary for implementing the purposes of processing data or for the period prescribed by the consent.

3. The data subject shall have the right to withdraw his or her consent in cases and as prescribed by this Law, as well as other laws.

4. The data subject's consent shall be considered to be given and the processor shall have the right to process, where:

(1) personal data are indicated in a document addressed to the processor and signed by the data subject, except for the cases when the document, by its content, is an objection against processing of personal data;

(2) the processor has obtained data on the basis of an agreement concluded with the data subject and uses it for the purposes of operations prescribed by this Agreement;

(3) the data subject, voluntarily, for use purposes, verbally transfers information on his or her personal data to the processor.

5. Personal data may be processed without the data subject's consent, where the processing of data is directly provided for by law.

6. The processor of personal data or the authorised person, for obtaining the data subject's written consent, shall notify the data subject of the intention to process the data.

7. The data subject shall give his or her consent in writing or electronically, validated by electronic digital signature; in case of an oral consent — by means of such reliable operations which will obviously attest the consent of the data subject on using the personal data.

8. The burden of proving the fact of obtaining data subject's consent and, in case of processing publicly available personal data, the fact that the data are publicly available shall lie upon the processor.

9. In case of incapacity or limited capacity of the data subject or of being a minor under the age of 16, consent for processing his or her personal data shall be given by a legal representative of the data subject.

10. In case of death of the data subject or declaring him or her dead by a judgement of the court, the consent to process his or her personal data shall be given by all legal heirs of the data subject, in case of not having heirs, the head of the community of the place of opening the succession, whereas in case of declaring him or her as missing, the trust manager of the property of the person declared as missing, where the data subject has not given such consent before that.

11. In case of death of the data subject, his or her personal data may be processed without consent, where data being processed are the name, gender, year, month and day of birth and death of the deceased person. In case of death of a figure in the fields of culture, arts, science, education, sport, religion and in other public field, data on his personal life may be processed without consent, where 50 years have elapsed from the day of death.

Article 10. Notification to the data subject for obtaining consent to process personal data

1. The processor of personal data or the authorised person provided for in Article 14 of this Law shall, for obtaining the data subject's consent, notifies of the intention to process the data.

2. The notification shall include:

(1) surname, name, patronymic of the data subject;

(2) legal grounds and purpose of the processing of personal data;

(3) list of personal data subject to processing;

(4) list of operations to be performed upon personal data for which the subject's consent is requested;

(5) scope of persons to whom personal data may be transferred;

(6) name (surname, name, patronymic, position) of the processor or his or her representative requesting the data subject's consent and registered office or place of registration (actual residence);

(7) information on requiring by the data subject rectification, destruction of personal data, terminating the processing of data or on carrying out other operation relating to the processing;

(8) validity of the consent requested, as well as the procedure and consequences of withdrawing the consent.

Article 11. Publicly available personal data

1. A regime of publicly available information of personal data (phone directories, address books, biographical directories, private announcements, declaration of income, etc.) may be established by the data subject's consent or in cases provided for by law. The name, surname, year, month and day of birth, place of birth, place of death, year, month and day of death, as well as the personal data which by conscious operations carried out by the data subject aimed at making publicly available becomes publicly available for certain scope of persons or public at large, shall be considered as publicly available.

2. Information on the data subject, except for information provided for by part 1 of this Article, may be removed from publicly available sources of personal data at the request of data subject or through judicial procedure.

3. The data being processed on the basis of an agreement may be removed from publicly available sources of personal data by mutual consent or through judicial procedure.

Article 12. Characteristics for processing special category personal data

1. The processing of special category personal data without the person's consent shall be prohibited, except when the processing of data is directly provided for by law.

2. The processing of personal data provided for by part 1 of this Article shall immediately be terminated, where the grounds and purpose of processing of data were eliminated.

Article 13. Characteristics for processing biometric personal data

1. Biometric personal data shall be processed only by the data subject's consent, except for cases provided for by law and where the purpose pursued by law is possible to implement only through processing of these biometric data.

Article 14. Processing of personal data by authorised person assigned by processor of data

1. Personal data may also be processed by an authorised person assigned by the processor.

2. The assignment shall be in writing, which includes legal grounds and conditions for, purpose of the processing of personal data, the list of personal data subject to processing, the scope of data subjects, the scope of persons to whom personal data may be transferred, technical and organisational measures for the protection of personal data and other necessary information.

3. Personal data shall be processed only within the scope of the assignment. The processor of data shall be responsible for processing of personal data within scope of the assignment. Where the assignment does not comply with the requirements of the Law, the authorised person must inform in writing thereon to the processor of data and refuse the processing.

4. Personal data assigned by state administration or local self-government bodies, state or community institutions or organisations shall be processed in observance of the requirements of this Law.

5. Characteristics for processing personal data by the authorised person may be prescribed by other laws or by agreements concluded between the processor of data and authorised person, which may not affect the rights and responsibilities of other persons.

CHAPTER 4

RIGHTS OF DATA SUBJECT

Article 15. Right of data subject to information on his or her personal data

1. The data subject shall have the right to information on his or her personal data, processing of data, grounds and purposes for processing, processor of data, the registered office thereof, as well as the scope of persons to whom personal data may be transferred.

2. The data subject shall have the right to get familiarised with his or her personal data, require from the processor to rectify, block or destruct his or her personal data, where the personal data are not complete or accurate or are outdated or has been obtained unlawfully or are not necessary for achieving the purposes of the processing.

3. In case of doubts with regard to the rectification, blocking or destruction of personal data by the processor, the data subject shall have the right to apply to the authorised body for the protection of personal data to make clear the fact of his or her personal data being rectified, blocked or destructed and by the request to be provided with information.

4. Information on personal data shall be provided by the processor to the data subject in an accessible manner and must not contain personal data on other data subject.

5. Data subject shall be provided with personal data based on a written request of the data subject or a representative acting by virtue of a power of attorney, or of a legal representative. The request may be filed electronically validated by an electronic digital signature.

6. The data subject shall have the right to information on the processing of his or her personal data, including on:

(1) confirming the fact of processing personal data and on the purpose of the processing;

(2) ways of processing personal data;

(3) subjects to whom personal data have been provided or may be provided;

(4) list of personal data being processed and the source from which it has been obtained;

(5) time limits for processing personal data;

(6) potential legal consequences for the data subject due to processing personal data.

7. Information shall be provided to the data subject free of charge, unless otherwise provided for by law.

Article 16. Rights of data subject when delivering decisions based on processing personal data

1. It shall be prohibited to deliver decisions not stemming from the purposes of processing personal data, which give rise to legal consequences for the data subject or otherwise affect his or her rights and legitimate interests, except for cases provided for by part 2 of this Article.

2. Decisions giving rise to legal consequences for the data subject or otherwise affecting his or her rights and legitimate interests based on processing of personal data may be delivered by the data subject's consent or in cases provided for by law.

Article 17. Right to appeal actions or inaction of processor

1. Where the data subject considers that the processing of his or her personal data is carried out in violation of the requirements of this Law or otherwise violates his or her rights and freedoms, he or she shall have the right to appeal actions or inaction of the processor before an authorised state body for the protection of personal data or through judicial procedure.

2. The data subject shall have the right to compensation of damage as prescribed by law.

CHAPTER 5

RESPONSIBILITIES OF PROCESSOR OF PERSONAL DATA

Article 18. Responsibilities of processor of personal data in the course of collecting personal data

1. In the course of processing personal data the processor shall be obliged to provide information provided for by Article 15 of this Law to the data subject at the request of the data subject.

2. In case of incomplete, inaccurate, outdated, unlawfully obtained personal data or those unnecessary for achieving the purposes of the processing, the processor of personal data

shall be obliged to carry out necessary operations for making them complete, keeping up to date, rectifying or destructing.

3. The processor shall be obliged to explain to the data subject in writing the consequences for failure to provide personal data, including the rights of personal data subject.

4. Where the personal data have been obtained not from the data subject, except for cases provided for by law, as well as publicly available data, the processor, before processing such personal data, shall be obliged to provide the data subject with the following information:

(1) name (surname, name, patronymic) of the processor or his or her authorised person (if any) and registered office or place of registration (actual residence);

(2) purpose and the legal ground for processing personal data, the list of data being processed;

(3) scope of potential users of personal data;

(4) rights of the data subject prescribed by this Law.

Article 19. Security measures for processing personal data and responsibilities of processor

1. The processor shall be obliged to destruct or block personal data that are not necessary for achieving the legitimate purpose.

2. In the course of processing personal data the processor shall be obliged to use encryption keys to ensure the protection of information systems containing personal data against accidental loss, unauthorised access to information systems, unlawful use,

recording, destructing, altering, blocking, copying, disseminating personal data and other interference.

3. The processor shall be obliged to prevent the access of appropriate technologies for processing personal data for persons not having a right thereto and ensure that only data, subject to processing by him or her, are accessed by the lawful user of these systems and the data which are allowed to be used.

4. The requirements for ensuring security of processing of personal data in information systems, the requirements for tangible media of biometric personal data and technologies for storage of these personal data out of information systems shall be prescribed by the Decision of the Government of the Republic of Armenia.

5. In case other body exercising control is prescribed by law, this body, within the scope of powers reserved to it by law, may prescribe higher requirements other than that provided for by part 4 of this Article, prescribed by the Decision of the Government of the Republic of Armenia.

6. Use and storage of biometric personal data out of information systems may be carried out only through such tangible media, application of such technologies or forms, which ensure the protection of these data from the unauthorised access thereof, unlawful use, destruction, alteration, blocking, copying, dissemination of the personal data, etc.

7. Processors of personal data or other persons provided for by this Law shall be obliged to maintain confidentiality both in the course of performing official or employment duties concerning the processing of personal data and after completing thereof.

8. The control over the fulfilment of the requirements of this Article shall be exercised by the authorised body for the protection of personal data without the right to process personal data being processed in the information systems.

9. Legal persons processing personal data, for having recognised electronic systems for processing of personal data under their possession as having an adequate level of protection and including them in the register, may apply to the authorised body for the protection of personal data.

Article 20. Responsibilities of processor of personal data in cases of written request of data subject or authorised body, familiarisation with personal data, revelation of violations by processor or authorised person

1. The processor shall be obliged to provide information to the data subject and authorised body as prescribed by Article 15 of this Law on the availability of personal data on the data subject, or to provide an opportunity to get familiarised with them within five working days upon receipt of the written request.

2. The processor shall be obliged to inform the data subject on the destruction of personal data within three working days upon destruction. The processor shall be obliged to provide an opportunity to the data subject to get familiarised with personal data relating to the data subject free of charge. In case personal data of the data subject is not complete or accurate or outdated or has been obtained unlawfully or is not necessary for achieving the purposes of the processing, the processor shall — after it is revealed by the processor or the authorised person or an application is received from the data subject or legal representative (or authorised person) — be obliged to immediately or, where there is no such an opportunity, within three working days, carry out necessary operations for completing, updating, rectifying, blocking or destructing them.

3. The processor shall be obliged to provide — on the basis of the written request of the authorised body for the protection of personal data — information necessary for the activities thereof within five working days upon receipt of the request.

4. Where the provision, rectification, blocking or destruction of personal data of the data subject on the basis of the written request of the data subject is rejected, the processor shall be obliged to provide the data subject and the authorised body — within five days following the receipt of the request — with a written reasoned decision by making a reference to the provisions of the Law which served as a ground for delivering a decision.

5. Where the authorised body considers the grounds for rejecting the provision, rectification, blocking or destruction of personal data unjustified, the processor shall be obliged to immediately provide, rectify, block or destruct personal data of the data subject or appeal the decision of the authorised body through judicial procedure.

Article 21. Responsibilities of processor while eliminating violations of legislation committed in the course of processing personal data, rectifying, blocking or destructing personal data

1. In case the reliability or lawfulness of processing of personal data are challenged on the basis of the request of the data subject or the authorised body for the protection of personal data, the processor shall be obliged to block personal data concerning the data subject upon receipt of the request until the completion of control activities.

2. In case it is confirmed that personal data are inaccurate the processor shall be obliged to rectify personal data and unblock them on the basis of documents or other necessary documents submitted by the data subject or the authorised body for the protection of personal data.

3. In case unlawful operations performed upon personal data are revealed, the processor shall be obliged to immediately, but not later than within three working days eliminate the committed violations. In case it is impossible to eliminate the violations, the processor shall be obliged to immediately destruct personal data. The processor shall be obliged to inform the data subject or his or her representative on the elimination of violations or the destruction of personal data within three working days, and where the request is received from the authorised body for the protection of personal data — also this body.

4. In case of outflow of personal data from electronic systems the processor shall be obliged to immediately publish an announcement thereon, meanwhile reporting on the outflow the Police of the Republic of Armenia and authorised body for the protection of personal data.

5. In case the purpose of the processing of personal data is achieved, the processor shall be obliged to immediately terminate the processing of data, unless otherwise provided for by law.

6. In case of withdrawal of the data subject's consent given in writing, validated by signature, or electronically, validated by electronic digital signature, the processor shall be obliged to terminate the processing of personal data and destruct the data within ten working days following the receipt of the withdrawal, unless otherwise provided for by mutual consent of the data subject and the processor or by law. The processor shall be obliged to inform the data subject on the destruction of personal data within three working days upon destruction.

Article 22. Procedure for exercise powers of authorised body through other body exercising control

1. In case other body exercising control is prescribed by law, this body exercising control shall provide the authorised body with the opinion on recognising electronic systems for processing of personal data of legal persons as having an adequate level of protection.

2. In case other body exercising control is prescribed by law, the authorised body shall transfer the applications on the protection of personal data, as well as information on the protection of personal data.

3. Other body exercising control shall, within the short time limit, forward its decisions delivered in the field of personal data protection or information on operations carried out for the protection of personal data to the authorised body.

4. Decisions, actions and inaction of other body exercising control may be appealed through judicial procedure.

Article 23. Notification to the authorised body of processing of personal data

1. The processor, prior to the processing of personal data, shall have the right to notify the authorised body for the protection of personal data of the intention to process data.

2. At the request of the authorised body the processor shall be obliged to send notification to the authorised body.

3. The processor, prior to the processing of biometric or special category personal data, shall be obliged to notify the authorised body for the protection of personal data of the intention to process data.

4. The notification shall include the following information:

(1) name (surname, name, patronymic) of the processor or his or her authorised person (if any), registered office or place of registration (actual residence);

(2) purpose and legal grounds for processing personal data;

(3) scope of personal data;

(4) scope of data subjects;

(5) list of operations performed upon personal data, general description of the ways of processing personal data by the processor;

(6) description of measures which the processor is obliged to undertake for ensuring security of processing personal data;

(7) date of starting the processing of personal data;

(8) time limits and conditions for completing the processing of personal data.

5. The authorised body for the protection of personal data shall enter the information provided for by part 2 of this Article, as well as the information on the date of sending the given notification into the register of processors within thirty days following the receipt of the given notification.

6. Expenses related to the consideration of the notification on processing personal data by the authorised body for the protection of personal data, as well as to the entry of information into the register of processors may not be imposed on the processor.

7. In case when information submitted by the processor, provided for by part 2 of this Article, is incomplete or inaccurate, the authorised body for the protection of personal data shall have the right to require the processor to specify the submitted information prior to its entry into the register of processors.

8. In case of change of information provided for by part 2 of this Article, the processor shall be obliged to notify the authorised body for the protection of personal data of changes within ten working days after the changes are made.

CHAPTER 6

BASIC PRINCIPLES FOR PROCESSING PERSONAL DATA

Article 24. Authorised body for the protection of personal data

1. The protection of personal data shall be carried out by the authorised body, which operates under the structure prescribed by the Decision of the Government of the Republic of Armenia.

2. The authorised body for the protection of personal data shall operate independently based on the Law and other legal acts.

3. Authorised body for the protection of personal data

(1) check, on its initiative or on the basis of an appropriate application, the compliance of the processing of personal data with the requirements of this Law;

(2) apply administrative sanctions prescribed by law in the case of violation of the requirements of this Law;

(3) require blocking, suspending or terminating the processing of personal data violating the requirements of this Law;

(4) require from the processor rectification, modification, blocking or destruction of personal data where grounds provided for by this Law exist;

(5) prohibit completely or partially the processing of personal data as a result of examination of the notification of the processor on processing personal data;

(6) keep a register of processors of personal data;

(7) recognise electronic systems for processing of personal data of legal persons as having an adequate level of protection and include them in the register;

(8) check the devices and documents, including the existing data and computer software used for processing data;

(9) apply to court in cases provided for by law;

(10) exercise other powers prescribed by law;

(11) maintain the confidentiality of personal data entrusted or known to it in the course of its activities;

(12) ensure the protection of rights of the data subject;

(13) consider applications of natural persons regarding the processing of personal data and deliver decisions within the scope of its powers;

(14) submit, once a year, a public report on the current situation in the field of personal data protection and on the activities of the previous year;

(15) conduct researches and provide advice on processing data on the basis of applications or coverages of processors or inform on best practices on processing of personal data;

(16) report to law enforcement bodies where doubts arise with regard to violations of criminal law nature in the course of its activities.

4. Decisions of the authorised body for the protection of personal data may be appealed through judicial procedure.

5. Activities of the authorised body for the protection of personal data shall be financed at the expense of the funds of the State Budget presented in a separate line.

6. An advisory body may operate on a voluntary basis adjunct to the authorised body for the protection of personal data, the procedure for the formation and activities of which shall be prescribed by the order of the head of the authorised body for the protection of personal data.

Article 25. Appointment of head of authorised body for the protection of personal data, termination of powers and requirements for him or her

1. The head of the authorised body for the protection of personal data shall be appointed for a term of five years, by the Prime Minister of the Republic of Armenia, upon nomination of the Minister of Justice of the Republic of Armenia, on the basis of joint recommendations of at least five non-governmental organisations carrying out law enforcement activities. The candidate for the head of the authorised body nominated by the Minister of Justice of the Republic of Armenia to the Prime Minister of the Republic of Armenia must be from the list of candidacies suggested by non-governmental organisations.

2. The procedure for recommending candidacies by non-governmental organisations shall be prescribed by the Government of the Republic of Armenia.

3. The same person may not be appointed to the position of the head of the authorised body for the protection of personal data for more than two consecutive terms.

4. The head of the authorised body for the protection of personal data shall manage activities of the authorised body for the protection of personal data and be responsible for the exercise of powers of the authorised body for the protection of personal data.

5. The head of the authorised body for the protection of personal data shall have the rights and responsibilities prescribed by law and other legal acts.

6. The head of the authorised body for the protection of personal data:

(1) must have higher education, enjoy a high reputation and have at least five years of professional work experience;

(2) must refrain from any kind of activities casting doubt on his or her ability to act independently and impartially.

7. The head of the authorised body for the protection of personal data shall be removed from office where the following grounds exist:

(1) on the basis of a written application;

(2) he or she has attained the age of 65 (age for holding office) or the term of office has expired;

(3) he or she has been elected or appointed to another position or has took another job incompatible with the position of the head of the authorised body for the protection of personal data;

(4) in case of failure to report to the service for over 120 consecutive days due to temporary incapacity for work or for over 140 consecutive days in the past 12 months, excluding the pregnancy and maternity leave or the leave for taking care of a child;

(5) he or she has not reported to work for more than five consecutive days without a reasonable excuse;

(6) he or she has been declared as incapable or having limited capacity, missing or dead by a judgement of the court entered into legal force;

(7) the judgement of conviction against him or her has entered into legal force.

CHAPTER 4

TRANSFER OF PERSONAL DATA TO THIRD PARTIES AND OTHER STATES

Article 26. Transfer of personal data to third parties

1. The processor may transfer personal data to third parties or grant access to data without the personal data subject's consent, where it is provided for by law and has an adequate level of protection.

2. The processor may transfer special category personal data to third parties or grant access to data without the personal data subject's consent, where:

(1) the data processor is considered as a processor of special category personal data prescribed by law or an interstate agreement, the transfer of such information is directly provided for by law and has an adequate level of protection;

(2) in exceptional cases provided for by law special category personal data may be transferred for protecting life, health or freedom of the data subject.

Article 27. Transfer of personal data to other states

1. Personal data may be transferred to other country by the data subject's consent or where the transfer of data stems from the purposes of processing personal data and/or is necessary for the implementation of these purposes.

2. Personal data may be transferred to other state without the permission of the authorised body, where the given State ensures an adequate level of protection of personal data. An adequate level of protection of personal data shall be considered to be ensured, where:

(1) personal data are transferred in compliance with international agreements;

(2) personal data are transferred to any of the country included in the list officially published by the authorised body.

3. Personal data may be transferred to the territory of the State not ensuring an adequate level of protection only by the permission of the authorised body where personal data are transferred on the basis of an agreement, and the agreement provides for such safeguards with regard to the protection of personal data which were approved by the authorised body as ensuring adequate protection.

4. In cases referred to in part 3 of this Article the processor of personal data shall be obliged — prior to the transfer of data to other country — apply to the authorised body to obtain permission. The processor of personal data shall be obliged to specify in the application the country where personal data are transferred, the description of the recipient of personal data (name, legal form), description (content) of personal data, purpose of processing and transferring personal data, agreement or the draft thereof. The authorised body shall be obliged to permit or reject the application within 30 days. The authorised body may require from the processor of personal data additional information by observing the time limit for the consideration of the application. In case

when the authorised body finds that contractual safeguards are not sufficient, it shall be obliged to specify those necessary changes which will ensure safeguards for the protection of personal data.

5. The authorised body for the protection of personal data, regularly but not less than once in a year, shall be obliged to revise the list of countries ensuring an adequate level of protection of personal data and publish the changes in the official journal and in its official website.

6. Personal data under the disposition of state bodies may be transferred to foreign state bodies only within the scope of interstate agreements, whereas to non-state bodies in accordance with the norms of this Article.

CHAPTER 8

FINAL PART AND TRANSITIONAL PROVISIONS

Article 28. Final part

1. This Law shall enter into force from 1 July 2015.

2. To repeal the Law of the Republic of Armenia HO-422-N of 8 October 2002 "On personal data" upon entry into force of this Law.

3. Article 7 of this Law shall enter into force from 1 January 2019.

Article 29. Transitional provisions

1. After the entry into force of this Law, the processing of personal data being processed prior to the entry into force of this Law shall continue to be carried out as prescribed by this Law.

2. The processors, who processed personal data prior to the entry into force of this Law and continue processing personal data after the entry into force of this Law, shall be obliged to send the mandatory notification provided for by this Law to the authorised body for the protection of personal data by 1 September 2015.

PRESIDENT
OF THE REPUBLIC OF ARMENIA **S. Sargsyan**

13 June 2015

Yerevan

HO-49-N