DRAFT

LAW OF THE REPUBLIC OF ARMENIA
ON THE PROTECTION OF PERSONAL DATA

CHAPTER 1.
GENERAL PROVISIONS

Article 1. Object of Regulation and Objective of the Law

1. This Law shall regulate relations pertaining to the processing of personal data by state and local self-governance bodies, state or community institutions, legal entities or natural persons.

2. This Law shall not apply to relations pertaining to the processing of personal data that constitute state classified information, the processing of personal data by data subjects for personal, family and similar purposes, nor to relations regulated by the legislation of the Republic of Armenia concerning archival management.

3. The objective of this Law shall be to ensure the protection of human and citizen's rights in the context of personal data protection, including the protection of the right to personal and family privacy.

Article 2. Legislation of the Republic of Armenia on Personal Data

1. The legislation of the Republic of Armenia on personal data consists of the Constitution of the Republic of Armenia, this Law and other legislative acts that regulate the processing of personal data.

2. In the event an international treaty, to which the Republic of Armenia is a party, provides otherwise than this Law, the provisions of the international treaty shall apply.

Article 3. Basic Terms Used by the Law

As used by this Law, the following terms shall mean:

1) personal data: information on facts, events, circumstances that concerns a natural person where presented in a form that allows or may allow to directly or indirectly identify the natural person in question;

2) data subject: the natural person whom the personal data concern;

3) personal data processing: any act or sequence of acts that concern personal data collection, input, organization, modification, dissemination (including transmission), storage, rectification, access blockage, anonymization, destruction and use, performed by automated means or without thereof;

4) data processor: state or local self-governance body, state or community institutions, legal entity or natural person that organizes and/or implements personal data processing;

5) personal data base (hereinafter referred to as “database”): a collection of personal data organized by certain attributes;

6) personal data information system (hereinafter referred to as “information system”): a set of information technologies and technical means used for automated or non-automated processing of personal data included in a database;

7) personal data anonymization: acts resulting in the impossibility of identification of the subject of the given set of data;

8) personal data dissemination: acts aimed at the transmission of personal data to a restricted audience or the sharing of personal data with an unrestricted audience, including the publicizing of personal data by mass media, the posting of personal data in information communication networks, or making personal data otherwise accessible;

9) personal data use: acts by data processor aimed at making decisions or performing acts resulting in the occurrence of legal consequences for the data subject or otherwise affecting the data subject's rights and freedoms;

10) personal data access blockage: temporary suspension of the possibility to collect, input, organize, disseminate (including transmission) and use personal data;

11) personal data destruction: acts resulting in non-restorable loss of personal data in an information system or in the destruction of physical information carriers;

12) biometric personal data: information on an individual's physiological characteristics allowing to identify the individual in question;

13) special category personal data: personal data concerning an individual's racial or ethnic origin, political views, religious or philosophical convictions, membership in specialized organizations, health status and intimate life;

14) confidential information: information, access to which is restricted by law;

15) consent of the data subject: unequivocal voluntary permission by the data subject for the processing of his/her personal data, given in any form;

16) third party (customer): any entity or individual that is not a data subject or data processor;

17) publicly accessible personal data: personal data that, with the consent of the data subject, have been made accessible to everyone, as well as personal data the access to which is not restricted by law.

CHAPTER 2.
PERSONAL DATA PROCESSING

Article 4. General Principles of Personal Data Processing

1. Personal data shall be collected and processed lawfully.

2. Personal data shall be collected for clearly specified or declared legitimate purposes and shall not be used for other purposes.

3. Collection and processing of personal data that is not necessary for the achievement of the purposes of processing shall be prohibited.

4. Volume and nature of personal data, as well as their processing mode, shall be proportional to the purpose of processing.

5. Personal data shall be accurate and sufficient for the achievement of the purposes of processing.

6. In the event of personal data being inaccurate or insufficient, well-reasoned steps shall be taken to rectify or destroy the personal data.

7. Personal data shall be preserved for no longer than is required for the purpose the personal data have been collected and processed, unless the law provides otherwise.

Article 5. Lawfulness of Personal Data Processing

1. Personal data processing shall be found lawful if:

1) personal data are processed with the data subject’s consent;

2) personal data processing is provided for by a law that determines the purpose of such processing, conditions for personal data collection, and data subjects;

3) personal data processing is implemented as part of a contract to which the data subject is a party;

4) personal data processing is implemented for statistical or other scientific purposes, provided that the condition of data anonymization is complied with;

5) personal data processing is implemented with the purpose of protecting the data subject's life, health or other vital interests, in the event of impossibility of obtaining the data subject's consent;

6) personal data processing is implemented as part of a journalist's professional activities;

7) personal data processing is implemented with the purpose of protecting state security and public safety from an immediate threat;

2. Specifics of special category and biometric personal data processing shall be described in Articles 9 and 10 of this Law.

Article 6. Confidentiality of Personal Data

1. Personal data administered by a data processor shall be confidential information.

2. The confidentiality condition shall not apply where personal data have been anonymized or are publicly accessible.

Article 7. Publicly Accessible Sources of Personal Data

1. With data subject's consent or in cases established by law, personal data may be made publicly accessible (telephone directories, address books, biographic directories, personal ads, income declarations, etc). With data subject's written consent, publicly accessible sources of data may include data subject's last name, first name and patronymic, year, month and day of birth, place of birth, address, information about his/her occupation and other personal data provided by the data subject.

4. Information on data subject may be removed from public sources of personal data at any time by data subject's request or by decision of a court or any other competent state body.

Article 8. Consent of Data Subject

1. Personal data processing shall be done with the data subject's consent, except in cases described in paragraph 2 of this Article. A data subject may always withdraw his/her consent.

2. Data subject shall be required to provide his/her personal data for the purposes of protecting the foundations of the constitutional order, health, morality or rights and liberties of other people, national and public security.

3. The responsibility to prove the fact of obtaining data subject's consent, as well as to prove the fact that data is publicly accessible in the case if publicly available personal data is processed, shall lie with the data processor.

4. In cases described by this Law, personal data shall be processed exclusively on the basis of data subject's written consent.

5. Data subject's written consent shall contain the following:

1¤ data subject's last name, first name, patronymic, series and number of personal identification document, data of issue and by whom it was issued,

2¤ name (last name, first name, patronymic) and address of the data processor obtaining data subject's consent,

3¤ purpose of personal data processing,

4¤ list of personal data to be processed for which data subject is giving his/her consent,

5¤ list of activities carried out with personal data for which data subject is giving his/her consent, as well as a general description of personal data processing methods used by processor,

6¤ period of time for which data subject's consent is valid, as well as procedures for withdrawing data subject's consent.

6. In the case if data subject is incapacitated, written consent for the processing of his/her personal data shall be given by his/her legal representative.

7. In the case of data subject's death, written consent for the processing of his/her personal data shall be given by his/her heirs, unless data subject had given such consent before his/her death.

Article 9. Special Category Personal Data

1. Processing of special category personal data shall be prohibited, except in cases described in paragraph 2 of this Article.

2. Special category personal data shall be processed in the following cases:

1¤ there is a written consent by data subject,

2¤ personal data is publicly accessible,

3¤ personal data is related to data subject's health condition, and its processing is necessary for the protection of his/her or other people's lives, health or other vital interests, and it is not possible to get data subject's consent,

4¤ personal data processing is done for medical/preventive reasons, for medical diagnosis and provision of medical and medical/social services, provided that personal data is processed in

accordance with procedures established by law and it is done by persons providing medical assistance and services,

5¤ personal data of members of non-governmental or religious organizations is processed in order to achieve the objectives of such non-governmental or religious organizations operating in accordance with procedures described by legislation, which are stated in their founding documents, provided that personal data is not disseminated without data subject's written consent,

6¤ personal data processing is necessary in order to exercise justice,

7¤ personal data is processed in accordance with legislation on operative-investigative activities.

3. In cases described in paragraph 2 of this Article, special category personal data processing shall stop immediately, as soon as the reasons for data processing are no longer there.

Article 10. Biometric Personal Data

1. Biometric personal data shall be processed exclusively on the basis of data subject's written consent, except in cases described in paragraph 2 of this Article.

2. Biometric personal data may be processed without data subject's consent for the purposes of exercising justice, as well as in accordance with the Republic of Armenia legislation on operative-investigative activities and on issues related to leaving the Republic of Armenia and returning to the Republic of Armenia.

Article 11. Personal Data Processing by State and Local Self-Governance Bodies, and State or Community Institutions

1. State and local self-governance bodies, and state or community institutions shall be authorized to process personal data only in cases described by law.

2. State and local self-governance bodies, and state or community institutions shall be required to ensure the accuracy of personal data processed by them.

Article 12. Personal Data Processing at a Third Party (Customer) Request

1. Personal data may also be processed by request from a third party (customer). The request shall be made in writing, and it shall contain the legal grounds and conditions for personal

data processing, the list of personal data to be processed, the range of data subjects involved, potential range of dissemination of personal data, technical and organizations means of personal data protection, and other required information.

2. Personal data shall be processed within the scope of the request only. The requester shall be responsible for personal data processing within the scope of the request. If the request does not meet the requirements of this Law and other legislative acts regulating personal data processing, then personal data processor shall notify the third person (customer) and refuse to process the data.

3. Personal data processing at the request of state and local self-governance bodies, state or community institutions shall be done in accordance with procedures described in Article 11 of this Law.

CHAPTER 3.
RIGHTS OF DATA SUBJECT

Article 13. The Right of Data Subject to Obtain Information on His/Her Own Personal Data

1. Data subject shall have the right to receive information about data processor, data processor's location and his/her possession of data subject's personal data, as well as the right to access the said personal data, except in cases described in paragraph 6 of this Article. Data subject shall have the right to request the processor to modify his/her data, block access to it or destroy it, if the personal data are not complete, are inaccurate, outdated, acquired by illegal means or are not necessary to achieve the goals of processing.

2. Processor shall provide information about the existence of personal data to data subject in an accessible form, and this information shall not contain personal data on other subjects.

3. Information about personal data shall be provided to data subject on the basis of his/her or her legal representative's written request. The request shall include the series and number of data subject's or his/her legal representative's personal identification document, its date of issuance and by whom it was issued, as well as data subject's or his/her legal representative's signature. The request may be submitted in electronic form, validated by an electronic signature.

4. Data subject shall have the right to receive information about the processing of his/her personal data, including information on the following:

1¤ confirming the fact of personal data is being processed and goals of such processing,

2¤ ways of personal data processing,

3¤ subjects who have received or may receive personal data,

4¤ list of personal data being processed and sources from which such data was obtained,

5¤ time periods for the processing and storing of personal data,

6¤ potential legal consequences of personal data processing for data subject.

5. Information shall be provided to data subject free of charge, unless stated otherwise by law.

6. Data subject's right to receive information about his/her personal data may be limited, if

1¤ personal data processing, including processing of data acquired as a result of operative-investigative activities, is done for the purposing of protecting the state, national security and legal order,

2¤ personal data processing is done by a state body that has arrested the data subject on suspicion of having committed a crime, or data subject has been charged in a criminal case, or data subject has been subjected to a means of prevention before being charged with a crime, except in cases, when the suspect or the accused has the right to have access to these personal data under criminal procedure laws,

3¤ provision of personal data violates other person's constitutional rights and liberties.

Article 14. The Rights of the Data Subject with Respect to Decisions Made on the Basis of Automated Personal Data Processing

1. It shall be prohibited to reach decisions on the basis of automated personal data processing, if such decisions have legal consequences for data subject or are related in any way to his/her rights and legal interests, except in cases described in paragraph 2 of this Article.

2. Decisions that have legal consequences for data subject or are related in any way to his/her rights or legal interests may be reached on the basis of automated personal data processing only if there is data subject's consent or in other cases described by law, provided that the protection of data subject's rights and legal interests is guaranteed.

3. Processor shall be required to explain to data subject the process by which decisions are made on the basis of automated personal data processing and the possible legal consequences of such a decision, and to give data subject a possibility to appeal against any such decision, as well as to explain to data subject the procedures for protecting his/her rights and legal interests.

4. Processor shall be required to review the complaints mentioned in paragraph 3 of this Article within seven working days of receiving it and notify data subject about the results of such a review.

Article 15. The Right to Appeal against Actions or Inaction by Data Processor

1. If data subject thinks that processor is processing his/her personal data in violation of this Law or is violating his/her rights and liberties in any other way, then he/she shall have the right to appeal against processor's actions or inaction to a state body authorized for the protection of personal data or to a court of law.

2. Data subject shall have the right to compensation for damages.

CHAPTER 4.
RIGHTS OF THE PROCESSOR

Article 16. Processor's Responsibilities during Personal Data Collection

1. During personal data collection, processor shall be required to provide data subject with information described in paragraph 4, Article 13 of this Law, upon data subject's request.

2. If the obligation to provide personal data to processor is prescribed by law, then processor shall be required to explain to data subject the legal consequences of the latter's refusal to provide personal data.

3. If personal data were received not from data subject, except the data provided to processor on the basis of the law, as well as publicly accessible data, then processor shall be required to provide the following information to data subject prior to processing such data:

1¤ name of the processor or its legal representative (last name, first name and patronymic) and address,

2¤ purpose and legal grounds for personal data processing,

3¤ suggested users of personal data,

4¤ rights of data subject prescribed by this Law.

Article 17. Means to Ensure Security of Personal Data Processing

1. While processing personal data, processor shall be required to take relevant organizational and technical measures, including encoding, to protect information systems containing personal data from accidental loss, unauthorized access, unauthorized use, destruction, modification, blocking, copying, dissemination and other unlawful activity.

2. The security requirement for personal data processing in information systems, as well as the requirements for material carriers for personal biometric data and personal data storage technologies outside of information systems shall be set by the Republic of Armenia government.

3. Compliance with the requirements described in paragraph 2 of this Article shall be controlled by the authorized state body for the protection of personal data, without the right of access to the personal data being processed in information systems.

4. Biometric personal data may be used and stored outside of information systems only by means of material carriers and technologies that ensure data protection from illegal access, illegal use of personal data, destruction, modification, blocking, copying, dissemination and other unlawful activity.

Article 18. Processor's Responsibilities in the Case of Receiving Written Requests from Data Subject or His/Her Legal Representative, as well as from the Authorized State Body for the Protection of Personal Data

1. Processor shall be required to provide data subject or his/her legal representative with information about the existence of his/her personal data, in accordance with procedures described in Article 13 of this Law, as well as to provide an opportunity to get access to this data within 10 working days of receiving data subject's or his legal representative's written request.

2. In the case of refusing to provide information about the existence of personal data or to give access to such data on the basis of data subject's or his/her legal representative's written request, processor shall be required to provide a justified written decision on refusal within 7 working days of receiving data subject's or his/her legal representative's request; this written decision shall contain a reference to paragraph 6 of Article 13 of this Law or to any other legal provision the refusal is based on.

3. Processor shall be required to provide data subject or his/her legal representative with free access to personal data on data subject, and to modify the data as needed, destroy or block the data, if data subject or his/her legal representative provide information to prove that personal data is not complete or is inaccurate, has been acquired by illegal means or is not necessary to achieve the stated goal of processing. Processor shall be required to notify data subject or his/her legal representative and third persons, to whom data subject's personal data has been forwarded, about the modifications and other measures taken.

4. Processor shall be required to provide the authorized state body for the protection of personal data with information that is necessary for the latter's activities within 7 working days of receiving a written request for information from that body.

Article 19. Processor's Responsibilities When Rectifying Violations of the Law Committed While Processing Personal Data, as well as When Correcting, Blocking and Destroying Personal Data

1. If the accuracy of personal data or legality of personal data processing is questioned on the basis of a request by data subject or his/her legal representative or authorized state body for the protection of personal data, then processor shall be required to block personal data on the data subject in question from the moment the request is received until the completion of the checking activities.

2. If the inaccuracy of personal data is confirmed, processor shall be required to correct the personal data on the basis of documents provided by data subject or his/her legal representative or authorized state body for the protection of personal data or other relevant documents, and then unblock it.

3. If unlawful use of personal data is discovered, processor shall be required to rectify the situation within 3 working days. If it is impossible to rectify the situation, processor shall be required to destroy the personal data within 3 working days of discovering unlawful use of personal data. Processor shall be required to notify data subject or his/her legal representative about rectifying the situation or destroying personal data; in the case if the request was received from the authorized state body for the protection of personal data, then that body shall also be notified.

4. When the goal of personal data processing is reached, processor shall immediately stop data processing and destroy the personal data within 3 working days, unless stated otherwise by law, and notify data subject or his/her legal representative about this; in the case if the request was received from the authorized state body for the protection of personal data, then that body shall also be notified.

5. If data subject withdraws his/her consent, then processor shall stop personal data processing and destroy the personal data within 3 working days following the withdrawal, unless stated otherwise in the mutual agreement between data subject and processor. Processor shall be required to notify data subject about destroying the personal data.

Article 20. Notification about Personal Data Processing

1. Before starting personal data processing, processor shall notify the authorized state body for the protection of personal data about his/her intention to process personal data, except in cases described in paragraph 2 of this Article.

2. Processor shall have the right to process the following personal data without notifying the authorized state body for the protection of personal data:

1¤ data on subjects who have a work relationship with processor,

2¤ data received by processor in connection with signing an agreement, one of the parties to which is the data subject, provided that personal data is not disseminated or provided to third parties without data subject's consent and is used by processor exclusively for the purpose of enforcing the said agreement or signing other agreements with the data subject,

3¤ data on members of non-governmental or religious organizations, which is processed for achieving the goals of the said organizations as stated in their founding documents, provided that personal data is not disseminated without data subject's written consent,

4¤ data that is publicly accessible,

5¤ data that includes data subjects' last names, first names and patronymics only,

6¤ data that is required for granting data subject a one-time access to data processor's premises,

7¤ data that is included in state information systems established for the purpose of protecting state and public security,

8¤ data processed without automated means and in accordance with laws and other normative acts containing requirements for the security of personal data processing and for the protection of data subjects' rights.

3. The notification described in paragraph 1 of this Article shall be sent in writing, validated by data subject's or his/her legal representative's signature, or electronically, validated by an electronic signature. The notification shall contain the following information:

1¤ processor's name (last name, first name and patronymic) and address,

2¤ purpose of personal data processing,

3¤ personal data categories,

4¤ categories of data subjects,

5¤ legal grounds for personal data processing,

6¤ list of activities related to personal data, and a general description of ways to process personal data used by processor,

7¤ description of measures to be taken by processor to ensure the security of personal data processing,

8¤ date when personal data processing is to begin,

9¤ date or conditions when personal data processing is to end.

4. Within 30 days of receiving the notification, the authorized state body for the protection of personal data shall enter the information described in paragraph 3 of this Article, as well as the date when the notification was sent, into a data processors' register. Information in the data processors' register shall be publicly accessible, except for information on security measures to protect personal data processing.

5. Costs associated with reviewing the notification on personal data processing by the authorized state body for the protection of personal data, as well as with inputting the information into the data processors' register, may not be placed on the data processor.

6. In the case if the information provided by processor under paragraph 3 of this Article is not complete or accurate, the authorized state body for the protection of personal data shall have the right to ask the processor to clarify the information before entering it into the data processors' register.

7. In the case if information described in paragraph 3 of this Article changes, processor shall be required to notify the authorized state body for the protection of personal data of these changes within 10 working days of them happening.

CHAPTER 5.
CONTROL OVER THE LAWFULNESS OF PERSONAL DATA PROCESSING: LIABILITY FOR BREAKING THIS LAW

Article 21. Authorized State Body for the Protection of Personal Data

1. Control over compliance with the requirements of this Law shall be exercised by the personal data protection inspection, operating within the national executive body system.

2. Personal data protection inspection shall have the right to:

1¤ request information from natural persons and legal entities that is necessary for exercising its powers, and receive that information free of charge,

2¤ Inspect the compliance of personal data processing with the requirements of this Law, in accordance with the Republic of Armenia Law on the Organization and Carrying out of Inspections,

3¤ request processor to correct, block or destroy personal data, if there are legal grounds for doing so,

4¤ go to courts to protect data subjects' rights, and defend their interests in a courts,

5¤ request the state body that had licensed the processor to suspend or terminate the license in accordance with procedures defined by law, if the license required the processor not to provide personal data to third parties without data subject's written consent and if this requirement was not fulfilled,

6¤ turn to preliminary investigation authorities if signs of a crime have been identified, in order to start criminal prosecution of guilty persons,

7¤ provide recommendations to the Republic of Armenia government on improving personal data legislation,

8¤ impose administrative sanctions on persons who have broken the requirements of this Law.

3. Personal data protection inspection shall be required to maintain the confidentiality of personal data that has become available to it in the process of carrying out its duties.

4. Personal data protection inspection shall be required to

1¤ ensure the protection of data subjects' rights,

2¤ review applications by natural persons and legal entities related to personal data processing and adopt decisions within the scope of its authority,

3¤ keep a data processors' register,

4¤ take measures to improve ways of protecting data subjects' rights,

6¤ provide annual reports on the situation with personal data protection to the President, National Assembly and Government of the Republic of Armenia; the reports shall be subject to publication in the mass media.

5. Personal data protection inspection's decisions may be appealed in a court of law.

6. The activities of personal data protection inspection shall be financed from the state budget.

7. Personal data protection inspection may have a consultative body working free of charge; procedures for its formation and operation shall be established by decree of the personal data protection inspection's director.

Article 22. Liability for Breaking This Law

Persons breaking this law shall be subject to disciplinary or administrative sanctions, or criminal prosecution.

CHAPTER 6.

CONCLUSION AND TRANSITION PROVISIONS

Article 23. Conclusion

1. This Law shall enter into effect on the tenth day of its official promulgation.

2. The Republic of Armenia Law HO-422-N of October 8, 2002 "On Personal Data" shall be considered null and void from the moment of this Law entering into effect.

Article 24. Transition Provisions

1. Personal data processing that started before this Law enters into effect shall continue in accordance with procedures defined by this Law, after this Law enters into effect.

2. Personal data information systems shall be brought into compliance with the requirements of this Law by January 1, 2012.

3. Processors, who have started personal data processing before this Law enters into effect and continue to process personal data after this Law enter into effect, shall be required to send notifications described in Article 20 of this Law to the authorized state body for the protection of personal data by January 1, 2010.

Translation arranged by the International Organization for Migration