

DATA PROTECTION LAWS OF THE WORLD

Armenia



Downloaded: 29 April 2024

ARMENIA



Last modified 17 January 2024

LAW

Personal Data Protection Law as of 18.05.2015, number 1344-1365-49-1350;

DEFINITIONS

Personal Data is defined as *any information related to an individual that allows or may allow directly or indirectly identifying a person.*

Definition of Sensitive Personal Data

Special Category is defined as any information related to a person's

- race;
- nationality or ethnicity;
- political views;
- religious or philosophical beliefs;
- membership in a professional union;
- health status; and
- sexual life.

Definition of Personal Life Data

Data on personal life is defined as any information on a person's

- personal life;
- family life;
- the physical, physiological, mental, or social condition of a person; or
- other similar information.

Definition of Biometric Personal Data

Biometric personal data is defined as any information characterizing person's

- the physical characteristics;
- physiological characteristics; and / or
- biological characteristics of a person.

Definition of Publicly Available Personal Data

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 a certain scope of persons or the public at large, as well as information, which is provided for by law as publicly available information.

NATIONAL DATA PROTECTION AUTHORITY

Based on Decision N 573-A of the RA Prime Minister as of July 3, 2015, the Personal Data Protection Agency of the RA Ministry of Justice was appointed as the authorized body for personal data protection.

REGISTRATION

Registration is voluntary unless otherwise specified by the authorized body. Processing of personal data may be carried out by state administration or local self-government bodies, state or municipal institutions or organizations, legal or natural persons, which organize and / or carry out the processing of personal data.

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

At the request of the authorized body, the processor shall be obliged to send a notification to the authorized body.

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

The notification shall include the following information:

- name (surname, name, patronymic) of the processor or his or her authorised person (if any), registered office or place of registration (actual residence);
- purpose and legal grounds for processing personal data;
- scope of personal data;
- scope of data subjects;
- list of operations performed upon personal data, general description of the ways of processing personal data by the processor;
- description of measures which the processor is obliged to undertake for ensuring security of processing personal data;
- date of starting the processing of personal data;
- time limits and conditions for completing the processing of personal data.

The authorized body for the protection of personal data shall enter the information mentioned in the notification, 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.

In case when information submitted by the processor, provided for by the mentioned notification, is incomplete or inaccurate, the authorized 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.

DATA PROTECTION OFFICERS

No requirement to appoint a data protection officer.

COLLECTION & PROCESSING

- By and large, the entities must obtain prior express consent from data subjects to lawfully collect and process personal data; The consent is not necessary in the cases directly provided by the legislation or if the data is being collected from public sources.

- 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.
- The data subject's consent shall be considered to be given and the processor shall have the right to process, where:
 - 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;
 - 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;
 - the data subject, voluntarily, for use purposes, verbally transfers information on his or her personal data to the processor.
- Personal data may be processed without the data subject's consent, where the processing of data is directly provided for by law.
- 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.
- 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.

The processor of personal data for obtaining the data subject's consent notifies of the intention to process the data. The notification shall include:

- surname, name, patronymic of the data subject;
- legal grounds and purpose of the processing of personal data;
- list of personal data subject to processing;
- list of operations to be performed upon personal data for which the subject's consent is requested;
- scope of persons to whom personal data may be transferred;
- 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);
- 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;
- validity of the consent requested, as well as the procedure and consequences of withdrawing the consent.

Characteristics for processing publicly available personal data

- 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.
- Information on the data subject, except for information provided for by previous clause, may be removed from publicly available sources of personal data at the request of data subject or through judicial procedure.
- 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.

Characteristics for processing sensitive personal data

- 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.
- The processing of personal data provided for by the previous clause shall immediately be terminated, where the grounds and purpose of the processing of data were eliminated.

Characteristics for processing personal data of persons with incapacity or limited capacity and minors under the age of 16

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 / parent of the data subject

Characteristics for processing biometric personal data

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.

Processing of personal data by an authorized person assigned by the processor of data

Personal data may also be processed by an authorized person assigned by the processor. The assignment shall be in writing, which shall include

- legal grounds and conditions;
- the 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 organizational measures for the protection of personal data and other necessary information.

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

Blocking or destruction of personal data

The data subject shall have the right to get familiarized with his or her personal data, and require 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.

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 authorized 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.

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.

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

TRANSFER

Transfer to third parties shall mean an operation aimed at transferring personal data to a certain scope of persons or the public at large or at familiarizing with them, including disclosure of personal data through the mass media, posting in information communication networks or otherwise making personal data available to another person.

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.

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

- 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;

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

Personal data may be transferred to another country with 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.

Personal data may be transferred to another state without the permission of the authorized 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:

- personal data are transferred in compliance with international agreements;
- personal data are transferred to any of the countries included in the list officially published by the authorized body.

Personal data may be transferred to the territory of the State not ensuring an adequate level of protection only by the permission of the authorized 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 authorized body as ensuring adequate protection.

In cases referred to in the previous paragraph the processor of personal data shall be obliged to: prior to the transfer of data to another country; to apply to the authorized 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), the description (content) of personal data, the purpose of processing and transferring personal data, agreement or the draft thereof. The authorized body shall be obliged to permit or reject the application within 30 days. The authorized 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 authorized 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.

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 provided above.

SECURITY

The processor has an obligation to destruct or block personal data that are not necessary for achieving the legitimate purpose.

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, unauthorized access to information system, unlawful use, recording, destructing, altering, blocking, copying, and disseminating personal data and other interference.

The processor is 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.

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. In case another 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 those provided above.

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 unauthorized access thereof, unlawful use, destruction, alteration, blocking, copying, dissemination of the personal data, etc.

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.

The control over the fulfillment of the above-mentioned requirements shall be exercised by the authorized body for the protection of personal data without the right to process personal data being processed in the information systems.

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

BREACH NOTIFICATION

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 authorized body for the protection of personal data — also this body.

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 authorized body for the protection of personal data — also this body.

Mandatory breach notification

In case of an 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 authorized body for the protection of personal data.

ENFORCEMENT

The authorized body for the protection of personal data is entitled to:

- 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;
- apply administrative sanctions prescribed by law in the case of violation of the requirements of this Law;
- require blocking, suspending or terminating the processing of personal data violating the requirements of this Law;
- require from the processor rectification, modification, blocking or destruction of personal data where grounds provided for by this Law exist;
- prohibit completely or partially the processing of personal data as a result of examination of the notification of the processor on processing personal data;
- keep a register of processors of personal data;
- recognize electronic systems for processing of personal data of legal persons as having an adequate level of protection and include them in the register;
- check the devices and documents, including the existing data and computer software used for processing data;
- apply to court in cases provided for by law;
- exercise other powers prescribed by law;
- maintain the confidentiality of personal data entrusted or known to it in the course of its activities;
- ensure the protection of rights of the data subject;
- consider applications of natural persons regarding the processing of personal data and deliver decisions within the scope of its powers;
- 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;
- 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;
- report to law enforcement bodies where doubts arise with regard to violations of criminal law nature in the course of its activities.

ELECTRONIC MARKETING

There is no regulation. However, it is advised to obtain user consent, such as through appropriate disclaimers.

ONLINE PRIVACY

There is no regulation on cookies and location data. However, it is advisable to obtain user consent, such as through appropriate disclaimers.

KEY CONTACTS

LEGELATA Law Firm

legelata.am/



Arthur Buduryan

Partner

LEGELATA Law Firm

T +37495993696

arthur.buduryan@legelata.am



Artyom Poghosyan

Associate

LEGELATA Law Firm

T +37495992636

artyom.poghosyan@legelata.am

DATA PRIVACY TOOL

You may also be interested in our [Data Privacy Scorebox](#) to assess your organization's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.