Practical Law™
GLOBAL GUIDE 2018
DATA PROTECTION

Data protection in Armenia: overview

Narine Beglaryan
Concern Dialog law firm

global.practicallaw.com/w-015-7912

REGULATION
Legislation

1. What national laws regulate the collection and use of personal data?

General laws

Directive 95/46/EC on data protection (Data Protection Directive) is not applicable in Armenia. However, Armenian data protection legislation reflects the main principles and rules of the Data Protection Directive. From May 2018, the Data Protection Directive has been replaced by Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (GDPR).

Armenia has ratified the Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (European Convention on Human Rights). Therefore, Article 8 of the European Convention on Human Rights apply to cases involving the protection of personal data.

The Constitution of Armenia protects the right to protection of personal data. General rules concerning the processing of personal data are set out in the Law of Armenia on protection of personal data (Data Protection Law), which was adopted in 2015.

Sectoral laws

There are several sectoral laws that impose an obligation on processors of certain categories of personal data to treat such data as confidential and guarantee a certain level of protection of personal data.

The Data Protection Law provides that the following matters are regulated by other laws:

- State and official secrets.
- Banking, notarial, and insurance secrecy.
- Legal professional privilege.
- Use of personal data during operations concerning national security or defence.
- Use of personal data in the fight against money laundering and terrorism financing, and operational intelligence activities and proceedings.

Relevant sectoral laws include the following:

- The Law of Armenia on banking secrecy, which aims to protect data collected by banks.
- The Law of Armenia on insurance and insurance activity, which protects data transferred to insurance companies and intermediaries.
- The Law of Armenia on combating money laundering and terrorism financing, which regulates data protection issues in the area of combating money laundering and terrorism financing.
- The Law of Armenia on circulation of credit information and activities of credit bureaus, which defines special rules for the collection, processing, registration, maintenance and use of credit information in Armenia.
- The Labour Code of Armenia, which protects personal data of employees.
- The Law of Armenia on electronic communications, which guarantees the protection of data of clients of electronic communications service providers.
- The Code on Administrative Offences of Armenia, which imposes administrative liability for breach of the general rules on the protection and processing of personal data and defines the relevant administrative offences.
- The Criminal Code of Armenia, which imposes criminal liability for breach of the general rules on the protection and processing of personal data and defines the relevant criminal offences.

Scope of legislation

2. To whom do the laws apply?

The Armenian Data Protection Law guarantees the rights of natural persons (data subjects) and imposes mandatory requirements on processors of personal data, authorised persons and third parties. The Law does not use the term "controller", but uses the terms "processor" and "authorised persons" instead.

Personal data processor

A personal data processor is defined as a person who organises and/or carries out the processing of personal data. The following can act as personal data processors:

- The state.
- State administrations.
- Local self-government bodies.
- State and community institutions.
- State or community organisations.
- Legal entities.
- Natural persons.

Personal data processors must comply with the Data Protection Law.

Authorised person

An authorised person is a person that is authorised by the data processor to collect, input, organise or otherwise process personal data in cases prescribed by law or under an agreement. Authorised persons must comply with the Data Protection Law.

3. What data is regulated?

The Data Protection Law provides a broad definition of "personal data". Personal data includes any information relating to a natural person that allows or may allow for the direct or indirect identification of that person's identity.

The Data Protection Law does not guarantee the protection of publicly available personal data, that is, information that either:

- Becomes publicly available to certain persons or the general public with the data subject's consent or through conscious actions of the data subject aimed at making his or her personal data publicly available.
- Constitutes publicly available information by law (such as a person's name, surname, year, month and day of birth, and place of birth).

The Data Protection Law defines "special category personal data" as information relating to a person's race, national identity or ethnic origin, political views, religious or philosophical beliefs, trade union membership, health, and sex life.

The Data Protection Law also defines "biometric personal data" as information relating to the physical, physiological and biological characteristics of a person.

4. What acts are regulated?

The Data Protection Law covers personal data processing, that is, any operation or set of operations, regardless of the form and mode of implementation (automated, with or without use of technical means), related to the collection, input, systematisation, organisation, storage, use, alteration, restoration, transfer, rectification, blocking, or deletion of personal data, and any other operations involving personal data.

"Use of personal data" is defined as any operation performed on personal data that gives rise or may give rise to legal consequences for the data subject or third parties, or is otherwise related to the rights and freedoms of such persons, and which may be directly or indirectly aimed at issuing decisions or forming opinions, acquiring rights, granting rights or privileges, restricting or depriving of rights, or achieving any other purpose (*Data Protection Law*).

5. What is the jurisdictional scope of the rules?

The Data Protection Law imposes mandatory rules on the processing of personal data in Armenia.

However, the Data Protection Law does not clearly specify its jurisdictional scope. For example, the law does not specify which rules apply to the collection and transfer of Armenian citizens' or foreign citizens' personal data outside Armenia by a foreign company, or which law applies to an Armenian company that uses collection and processing technology located outside Armenia. The author believes that the jurisdictional scope of the law should be further clarified through case law and/or amendments to the Data Protection Law. However, the author is of the opinion that a person who collects and processes personal data in Armenia, and transfers such data outside Armenia, must meet the requirements of the Armenian Data Protection Law.

6. What are the main exemptions (if any)?

Personal data that relate to state and official secrets, banking, notarial, and insurance secrecy, legal professional privilege, anti-money laundering, and so on, are governed by special laws (*see Question 1, Sectoral laws*).

Additionally, publicly available data is not protected by the Data Protection Law (*see Question 3*).

Notification

7. Is notification or registration required before processing data?

To obtain the data subject's written consent before processing personal data, a processor or authorised person must notify the data subject of its intention to process his or her data (*see Question 12*).

Before processing personal data, the data processor can notify the Personal Data Protection Agency (PDPA) of its intention to process data. On request of the PDPA, a data processor must also notify the PDPA of any processing of personal data. A processor that intends to process biometric or special category personal data (*see Question 3*) must notify the PDPA before such processing. \Any notification to the PDPA must include the following information:

- Name of the processor or authorised person (if any), as well as their registered office or place of registration (actual residence).
- Purpose and legal grounds of the processing.
- Scope of personal data being processed.
- Scope of data subjects.
- List of operations performed on personal data and general description of the processing methods used by the processor.
- Description of measures that the processor must undertake to ensure the security of the processing.
- Start date of the processing.
- Time limits and conditions for completing the processing.

The PDPA must enter the above information and date of notification in the register of processors. The PDPA can request additional information if the information submitted is incomplete or inaccurate. When there are changes to registered information, the processor must notify the PDPA within ten working days after the changes occur.

MAIN DATA PROTECTION RULES AND PRINCIPLES

Main obligations and processing requirements

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

The processor must:

- Provide the data subject or Personal Data Protection Agency (PDPA) with information about the processing of personal data on request.
- Carry out necessary operations for making personal data complete, keeping up to date, rectifying or deleting incomplete, inaccurate, outdated, or unlawfully obtained personal data or data unnecessary for achieving the purposes of the processing.
- Delete or block personal data that are not necessary for achieving the legitimate purposes of the processing.

- Use encryption keys.
- Prevent access to process technologies by unauthorised persons and ensure that processed data are only accessed by lawful users.
- Maintain the confidentiality of personal data processed for the performance of official or employment duties, including after completion of the processing.
- Block personal data until the completion of control activities, if the reliability or lawfulness of the processing are challenged by the data subject or the PDPA.
- Rectify personal data and unblock them in accordance with information submitted by the data subject or PDPA, if it is confirmed that personal data are inaccurate.
- Correct violations of data protection rules if unlawful processing operations are revealed, or delete unlawfully processed personal data if it is impossible to correct violations.
- Terminate the processing of personal data when the purpose of the processing is achieved, unless otherwise required by law.

9. Is the consent of data subjects required before processing personal data?

In Armenia, the processing of personal data is deemed to be lawful if either:

- The data subject has given his or her consent to the processing (except in cases provided by law).
- The processed data is obtained from a publicly available source.

The data subject can give his or her consent in person or through a representative if a power of attorney specifically provides for such power.

The data subject can withdraw his or her consent in cases prescribed by the Data Protection Law and other laws.

The data subject must in principle give his or her consent in writing or electronically (validated by an electronic digital signature). Oral consent can be given if it obviously attests to the data subject's consent to the use of his or her personal data.

The data subject's consent is deemed to be given and the processor has the right to process personal data where any of the following applies:

- Personal data are included in a document addressed to the processor and signed by the data subject, except when the document objects to the processing of such personal data.
- The processor has obtained personal data under an agreement concluded with the data subject and uses such data for the purposes of implementing that agreement.
- The data subject voluntarily provides information orally on his or her personal data to the processor for use purposes.

In the case of incapacity or limited capacity of the data subject, or if the data subject is under the age of 16, consent must be given by their legal representative (for example, a parent, custodian, and so on).

In the case of death of the data subject or a court judgment declaring him or her dead, consent to process his or her personal data must be given by all his/her legal heirs or the head of the community of the place of opening of the succession (if there are no legal heirs). If the data subject is declared missing, consent must be given by the trust manager of the data subject's property.

10. If consent is not given, on what other grounds (if any) can processing be justified?

If consent is not given, the processing of personal data is deemed to be lawful in the following cases:

- The processed data is obtained from a publicly available source.
- The data subject has died and the data being processed are his or her name, gender, year, month and day of birth and death.
- The processed data concerns the personal life of a deceased public figure in the fields of culture, arts, science, education, sport, religion or other public field, and 50 years have elapsed since the day of that person's death.
- Other cases provided by law.

Special rules

11. Do special rules apply for certain types of personal data, such as sensitive data?

Special category and biometric personal data (*see Question 3*) cannot generally be processed without the consent of the data subject (*Data Protection Law*). The processing of special category personal data must be terminated when the purpose and grounds of the processing no longer exists.

The Data Protection Law and other laws list the cases in which special category and biometric personal data can be processed without the data subject's consent.

The processor can transfer special category personal data to third parties or grant access to data without the personal data subject's consent in the following circumstances:

- The data processor is considered a processor of special category personal data under the law or an interstate agreement, and the transfer of such information is directly provided for by law and provides for an adequate level of protection.
- In exceptional cases provided for by law, to protect the life, health or freedom of the data subject.

There are additional technical requirements for the protection of biometric personal data. For example, the use and storage of biometric personal data on information systems can only be carried out through tangible media and technology that ensure protection from unauthorised access, unlawful use, destruction, alteration, blocking, copying, dissemination, and so on.

RIGHTS OF INDIVIDUALS

12. What information should be provided to data subjects at the point of collection of the personal data?

The notification addressed to the data subject before processing their personal data (*see Question 7*) must include the following information:

- First name and patronymic name of the data subject.
- Legal grounds and purpose of the processing.
- List of personal data subject to the processing.
- List of operations to be performed using personal data for which the subject's consent is required.
- Persons to whom personal data may be transferred.

- Surname, first name, patronymic name, and position of the processor or authorised person requesting the data subject's consent, and their registered office or place of registration (actual residence).
- Information on the data subject's right to request the rectification or deletion of personal data, and termination of the processing or other operation relating to the processing.
- Term of consent requested and procedure for, and consequences of, withdrawing consent.

13. What other specific rights are granted to data subjects?

A data subject has the right to:

- Obtain information on his or her personal data, the processing of such data, the grounds and purposes of the processing, the data processor and its registered office, and the persons to whom personal data may be transferred.
- Be familiarised with his or her personal data rights.
- Request the processor to rectify, block or delete his or her personal data in certain cases (*see Question 14*).
- Apply to the Personal Data Protection Agency (PDPA) to request the rectification, blocking or deletion of his or her personal data, and in the case of doubt, request information on any rectification, blocking or deletion of personal data by the processor.
- Challenge the actions or inactions of the processor before the PDPA or through judicial proceedings, including claiming compensation of damages.

14. Do data subjects have a right to request the deletion of their data?

Data subjects are entitled to request the deletion of their personal data if such data:

- Is incomplete.
- Is not accurate.
- Is outdated.
- Has been obtained unlawfully.
- Is not necessary to achieve the purposes of the processing.

Personal data must also be deleted when the data subject withdraws his or her consent, unless otherwise provided by law or agreed between the data subject and the processor.

SECURITY REQUIREMENTS

15. What security requirements are imposed in relation to personal data?

There are no specific regulations relating to security of personal data, except for the general obligations of data processors set out in the Data Protection Law (such as the use of encryption keys, prevention of unlawful access, keeping data confidential, and so on) (*see Question 8*).

16. Is there a requirement to notify personal data security breaches to data subjects or the national regulator?

The data processor must notify the data subject or his or her representative and the Personal Data Protection Agency (PDPA) (if the request was received from the PDPA) of the cessation of illegal processing or deletion of illegally processed personal data.

When personal data is illegally extracted from electronic systems, the processor must make an immediate public announcement, report to the police and notify the PDPA.

PROCESSING BY THIRD PARTIES

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

An authorised person must process personal data within the scope of its assignment. If the assignment does not comply with the Data Protection Law, the authorised person must notify the data processor in writing and refuse to carry out the processing.

ELECTRONIC COMMUNICATIONS

18. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

There are no special rules on cookies and equivalent devices.

19. What requirements are imposed on the sending of unsolicited electronic commercial communications (spam)?

There are no special rules on unsolicited electronic commercial communications (spam).

However, the Personal Data Protection Agency has issued a recommendation on direct marketing stating that providers and operators of electronic communications services should act on the basis and within the scope of data subjects' consent through providing opt-in and opt-out mechanisms.

INTERNATIONAL TRANSFER OF DATA

Transfer of data outside the jurisdiction

20. What rules regulate the transfer of data outside your jurisdiction?

The Data Protection Law allows the transfer of personal data to third countries where either:

- The data subject has given his or her consent to the transfer.
- The transfer stems from the purposes of the processing or is necessary for the implementation of these purposes.

To transfer personal data to a third country, the permission of the Personal Data Protection Agency (PDPA) is required. The PDPA will grant permission if it considers that the data transfer agreement ensures an adequate protection of personal data.

The PDPA's permission is not required if personal data is transferred to a country that ensures an adequate level of protection of personal data. An adequate level of protection is presumed where either:

- Personal data are transferred in compliance with international agreements.
- Personal data are transferred to a country included in a list officially published by the PDPA.

The Data Protection Law does not distinguish between transfers of data abroad within the same group of companies or to a third company. Therefore, the above rules apply in both scenarios.

Personal data held by state bodies can only be transferred to foreign state bodies under interstate agreements. Transfers to foreign non-state bodies must comply with the above rules.

21. Is there a requirement to store any type of personal data inside the jurisdiction?

There is no requirement to store any type of personal data inside Armenia.

Data transfer agreements

22. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

A data processor and an authorised person must enter into a data transfer agreement. Agreements for the transfer of data abroad must ensure an adequate level of protection of personal data (*see Question 20*).

A data transfer agreement between a processor and an authorised person must include the following information:

- Legal grounds and conditions for the processing.
- Purpose(s) of the processing.
- List of processed personal data.
- Data subjects concerned by the processing.
- Persons to whom personal data can be transferred.
- Technical and organisational measures for the protection of personal data.
- Any other necessary information.

There are no special content requirements for international data transfer agreements.

No standard forms or precedents have been approved by national authorities.

23. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

A data transfer agreement is not sufficient to legitimise transfer, unless the law allows transfer without the data subject's consent and the agreement provides an adequate level of protection.

When data is transferred to a country that does not ensure an adequate level of data protection, permission from the Personal Data Protection Agency is required for the transfer, based on an analysis of the data transfer agreement (*see Question 20*).

24. Does the relevant national regulator need to approve the data transfer agreement?

The Personal Data Protection Agency (PDPA) does not need to approve data transfer agreements, but must approve transfers to countries that are not on the list approved by the PDPA.

ENFORCEMENT AND SANCTIONS

25. What are the enforcement powers of the national regulator?

The Personal Data Protection Agency is entitled to:

- Verify compliance of personal data processing with the Data Protection Law.
- Impose administrative sanctions for violations of the Data Protection Law.
- Require the blocking, suspension or termination of personal data processing violating the Data Protection Law.
- Require data processors to rectify, modify, block or delete personal data on the grounds set out in the Data Protection Law.
- Prohibit fully or partially the processing of personal data following examination of the notification submitted by a data processor.
- Recognise electronic systems used for processing personal data as ensuring an adequate level of protection and include them in a register.
- Check devices and documents used for processing data, including existing data and computer software.
- Ensure the protection of data subjects' rights.
- Consider applications brought by natural persons regarding the processing of personal data and issue decisions within the scope of its powers.
- Conduct research and provide advice on data processing on request or on its own initiative, and inform on best practices for the processing of personal data.
- Report violations of a criminal nature identified in the course of its activities to law enforcement bodies.
- Exercise other powers as prescribed by law.

26. What are the sanctions and remedies for non-compliance with data protection laws?

Non-compliance with data protection laws may lead to either:

- Administrative sanctions, for infringements that are not subject to criminal liability. Fines vary depending on the rule violated. The highest fine is AMD500,000 (about USD1,000).
- Criminal sanctions, including:
  - monetary penalties from AMD200,000 to AMD500,000; or
  - imprisonment for one to two months.

REGULATOR DETAILS

Personal Data Protection Agency (PDPA), Ministry of Justice of Armenia,

W *www.moj.am* (*www.moj.am/en/structures/view/structure/32*)

Main areas of responsibility. The PDPA ensures the:

- Protection of the rights of data subjects.
- Lawful processing of personal data, within the scope of its powers.
- Maintenance of the registry of personal data processors.

ONLINE RESOURCES

Armenian Legal Information System

W *www.arlis.am*

Description. The Armenian Legal Information System provides access to Armenian legislation and is supported by the Public Bulletin CJSC (the official up-to-date source of legislation). This website does not contain translations of legal acts and regulations.

Ministry of Justice of Armenia

W *www.moj.am*

Description. The official website of the Ministry of Justice of Armenia provides access to decisions of the Personal Data Protection Agency (*www.moj.am/page/587*).

Translation Centre of the Ministry of justice

W *http://translation-centre.am*

Description. This website publishes translations of legal acts. At the time of writing, there is no English translation of the Law of Armenia on protection of personal data.

Practical Law **Contributor profile**

Narine Beglaryan, Partner, Attorney

Concern Dialog law firm

T +374 99 353452
F +374 60 278888
E narine.beglaryan@dialog.am
W www.dialog.am

Professional qualifications. Republic of Armenia, Attorney, 2007

Areas of practice. Banking; capital markets; anti-money laundering and counter-terrorism financing.

Languages. Armenian, English, Russian

Professional associations/memberships. Chamber of the Advocates of the Republic of Armenia (since 2012).

Publications

- Authored the article *"Warranty: a Rescue or a Trap?", AmCham Business Magazine Spring-summer 2014.*
- Authored *"Analysis of the Company Law", International Trust Laws and Analysis, Supplement 2018.*
- Co-authored the article *"Doing business in Armenia", Practical Law Global Guide 2016/17.*
- Co-authored the article *"Mergers and Acquisitions 2016", International Comparative Legal Guide.*
- Co-authored the article *"Litigation and Dispute Resolution 2017", Global Legal Insights.*
- Expert contributor, *Data Protection in the Financial Sector Guidance: Data Guidance, the global privacy platform, 2017.*