THOMSON REUTERS
PRACTICAL LAW™

Data protection in Armenia: overview

by Narine Beglaryan, Concern Dialog law firm

Status: **Law stated as of 18-Sep-2019** | Jurisdiction: **Armenia**

This document is published by Practical Law and can be found at: **uk.practicallaw.tr.com/w-015-7912**
Request a free trial and demonstration at: **uk.practicallaw.tr.com/about/freetrial**

A Q&A guide to data protection in Armenia.

This Q&A guide gives a high-level overview of data protection rules and principles, including obligations on the data controller and the consent of data subjects, rights to access personal data or object to its collection, and security requirements. It also covers cookies and spam, data processing by third parties, and the international transfer of data. This Q&A also details the national regulator, its enforcement powers, and sanctions and remedies.

To compare answers across multiple jurisdictions, visit the Data Protection Country Q&A Tool.

Regulation

Legislation

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

General laws

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) is not applicable in Armenia. However, Armenian data protection legislation reflects most of GDPR's main principles and rules.

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 applies to personal data protection in Armenia.

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 specifies that the following matters are regulated by other laws:

- State and official secrets.
- Banking, notarial, and insurance secrecy.
- Legal professional privilege.
- Personal data use during operations concerning national security or defence.
- Personal data use in preventing and detecting money laundering, 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 connection with money laundering and terrorism financing prevention.
- 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 Labor Code of Armenia, which protects employees' personal data.
- The Law of Armenia on electronic communications, which protects electronic communications service providers' clients' data.
- The Code on Administrative Offenses of Armenia (in Armenian), which imposes administrative liability

for violating the general rules on personal data protection and processing and defines the relevant administrative offenses.

- The Criminal Code of Armenia, which imposes criminal liability for violating the general rules on personal data protection and processing and defines the relevant criminal offenses.

Scope of legislation

2. To whom do the laws apply?

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

For more on the definition of personal data, see Question 3. For more on data processing operations, see Question 4.

Personal data processor

The Data Protection Law defines a personal data processor as a person who organises or carries out personal data processing (Article 3(2), Data Protection Law). The following can act as personal data processors:

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

Personal data processors must comply with the Data Protection Law.

Authorized person

The Data Protection Law defines an authorized person as a person that a data processor authorizes to collect, input, organize, or otherwise process personal data in cases prescribed by law or under an agreement (Article 3(16), Data Protection Law).

Authorized persons must comply with the Data Protection Law.

3. What data is regulated?

The Law of Armenia on protection of personal data (Data Protection Law) broadly defines personal data to include any information relating to a natural person that allows or may allow that person to be identified directly or indirectly (Article 3(1), Data Protection Law).

The Data Protection Law does not guarantee publicly available personal data to be protected, such as information that either:

- Becomes publicly available to certain persons or the public either:
  - with the data subject's consent (Article 8(1), Data Protection Law); or
  - through the data subject's conscious actions to make the information public (Article 11, Data Protection Law).
- Constitutes publicly available information by law (such as a person's name, surname, year, month and day of birth, and place of birth) (Article 3(15), Data Protection Law).

For information on processing personal data, see Question 4.

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 (Article 3(14), Data Protection Law). For information on processing special category personal data, see Question 11.

The Data Protection Law also defines biometric personal data as information relating to a person's physical, physiological, and biological characteristics (Article 3(13), Data Protection Law).

4. What acts are regulated?

The Law of Armenia on protection of personal data (Data Protection Law) covers personal data processing. Processing includes any operation or set of operations, regardless of the form and mode of implementation (automated, with or without use of technical means), related to personal data including:

- Collection.
- Input.
- Systematization.
- Organization.
- Storage.
- Use.
- Alteration.
- Restoration.
- Transfer.

- Rectification.
- Blocking.
- Deletion.

(Article 3(2), Data Protection Law.)

The Data Protection Law also regulates personal data use, defined to include any operation performed on personal data that both:

- Gives rise or may give rise to legal consequences for the data subject or third parties, or is otherwise related to these persons' rights and freedoms.
- 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.

(Article 3 (4), Data Protection Law.)

5. What is the jurisdictional scope of the rules?

The Law of Armenia on protection of personal data (Data Protection Law) does not clearly specify its jurisdictional scope.

For example, the law does not specify which rules apply to a foreign company's collection and transfer of Armenian citizens' or foreign citizens' personal data outside Armenia, or to an Armenian company that uses collection and processing technology located outside Armenia.

The law's jurisdictional scope should be further clarified through case law and amendments to the Data Protection Law. However, a person who collects and processes personal data in Armenia, and transfers that data outside Armenia, likely must meet the law's requirements.

Armenia does not require an organization to appoint a designated individual, such as a data protection or privacy officer, to oversee the organization's compliance with legal obligations.

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

Personal data that relates to state and official secrets, banking, notarial, and insurance secrecy, legal professional privilege, anti-money laundering, and so on, are governed by special laws (Article 1(2), Law of Armenia on protection of personal data (Data Protection Law); see Sectoral laws).

The Data Protection Law also does not apply to personal data processing exclusively for journalism, literary and artistic purposes (Article 1(3), Data Protection Law).

Notification

7. Is notification or registration required before processing data?

Generally, yes. The Law of Armenia on protection of personal data (Data Protection Law) requires the data subject's consent for lawful processing, except where the personal data is publicly available (Article 8, Data Protection Law; see Question 3).

To obtain the data subject's written consent before processing personal data, a processor or authorized person must notify the data subject of its intention to process the subject's data (Article 9(6), Data Protection Law; see Question 12). The data subject notification must include:

- The data subject's surname, name, and patronymic.
- The legal grounds and purpose of the processing.
- A list of personal data subject to processing.
- A list of operations the processor will perform on the data.
- The scope of recipients to whom the processor may transfer the data.
- The processor's or its representative's surname, name, patronymic, and position.
- A request for the data subject's consent, and their registered office or actual residence.
- Information on correcting or deleting the personal data and terminating the data processing or any other operation relating to the processing.
- The procedure to withdraw consent, and the consequences of withdrawal.

(Article 10(2), Data Protection Law.) For more on individual notice requirements, see Question 12.

Before processing personal data, the data processor may notify the Armenian Personal Data Protection Agency (PDPA) of its intention to process data (Article 23(1), Data Protection Law). A processor must notify the PDPA if:

- The PDPA requests notice (Article 23(2), Data Protection Law.)
- The processor intends to process biometric or special category personal data (Article 23(3), Data Protection Law; see Question 3).

Any notification to the PDPA must include the following information:

- The processor's name or the authorized person's name (if any), as well as their registered office or place of registration (actual residence).

- The processing's purpose and legal grounds.
- The processing's scope.
- The number and scope of affected data subjects.
- A list of operations the processor performs on the personal data and a general description of the processor's processing methods.
- A description of the measures that the processor must undertake to ensure the processing's security.
- The processing's start date.
- The time limits and conditions for completing the processing.

(Article 23(4), Data Protection Law.)

The PDPA must enter the above information and notification's date in the register of processors (Article 23(5), Data Protection Law). The PDPA can request additional information if the information submitted is incomplete or inaccurate (Article 23(7), Data Protection Law). When there are changes to registered information, the processor must notify the PDPA within ten working days after the changes occur (Article 23(8), Data Protection Law). For the PDPA's contact information, see Regulator details.

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?

Under the Law of Armenia on protection of personal data (Data Protection Law), a processor must:

- Provide the data subject or Personal Data Protection Agency (PDPA) with information about the personal data processing on request (Articles 18(1) and 23, Data Protection Law).
- 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 that is unnecessary to achieve the processing's purposes (Article 18(2), Data Protection Law).
- Delete or block personal data that is not necessary for achieving the processing's legitimate purposes (Article 19(1), Data Protection Law).
- Use encryption keys and other appropriate technical and organizational measures (Articles 19(2) and 19(3), Data Protection Law).
- Prevent unauthorized access to processing technologies and ensure that only lawful users access processed data (Article 19(3), Data Protection Law).
- Maintain the confidentiality of personal data processed to perform official or employment duties, including after processing is complete (Article 19(7), Data Protection Law).
- Block personal data until control activities are complete, if the data subject or the PDPA challenge the processing's reliability or lawfulness (Article 21(1), Data Protection Law).
- Correct personal data and unblock it in accordance with information the data subject or PDPA submits, if it is confirmed that personal data is inaccurate (Article 21(2), Data Protection Law).
- Address and correct data protection rule violations if unlawful processing operations are revealed or delete unlawfully processed personal data if it is impossible to correct violations (Article 21(3), Data Protection Law).
- Terminate personal data processing when the processing's purpose is achieved, unless otherwise required by law (Article 21(5), Data Protection Law).

For more on personal data processing, see Question 4. For information on special category personal data processing, see Question 11.

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

In Armenia, personal data processing is deemed lawful under the Law of Armenia on protection of personal data (Data Protection Law) if either:

- The data subject has consented to the processing, except in cases provided by law, (Article 8(1), Data Protection Law).
- The processed data is obtained from a publicly available source ((Article 8(2), Data Protection Law).

The data subject can give consent in person or through a representative with power of attorney (Article 9 (1), Data Protection Law).

The data subject can withdraw consent in cases prescribed by the Data Protection Law (Article 9(3), Data Protection Law) or other laws, such as the Labor Code, if the personal data processing would violate a law's requirements, for example, non-compliance with the processing's purpose or a breach of data transfer rules.

The data subject must in principle give consent in writing or electronically, validated by an electronic digital signature. Verbal consent may suffice if it obviously attests to the data subject's consent to the use of the subject's personal data. (Article 9(7), Data Protection Law.)

A data subject's consent is deemed to be given, affording the processor the right to process personal data, in the following situations:

- Personal data is included in a document addressed to the processor and signed by the data subject, unless the data subject objects to the personal data processing in the document.
- The processor has obtained personal data under an agreement with the data subject and uses the data to implement that agreement.
- The data subject voluntarily and verbally provides information about their personal data to the processor for the processor to use.

(Article 9(4), Data Protection Law.)

If a data subject is incapacitated or has limited capacity, or is a minor under the age of 16, the subject's legal representative, such as their parent or custodian, must give consent (Article 9(9), Data Protection Law).

Consent to process a deceased data subject's personal data must be given by all legal heirs of the data subject or, if there are no legal heirs, by the head of the community of testator's last place of residence. If the data subject is declared missing, consent must be given by the trust manager of the data subject's property consent (Article 9(10), Data Protection Law).

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

Under the Law of Armenia on protection of personal data (Data Protection Law), personal data processing is lawful without consent in the following cases:

- The processed data is obtained from a publicly available source consent (Article 8(2), Data Protection Law).
- The data subject has died and the data being processed is the deceased's name and gender, and the year, month, and day of their birth and death (Article 9(11), Data Protection Law).
- The processed data concerns the personal life of a deceased public figure in the culture, arts, science, education, sport, religion, or other public field, and 50 years have elapsed since the subject died (Article 9(11), Data Protection Law).
- Other cases provided by law.

Special rules

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

Under Articles 12 and 13 of the Law of Armenia on protection of personal data (Data Protection Law, special category and biometric personal data (*see* Question 3) cannot generally be processed without the data subject's consent. Processors must stop processing special category data when the processing's purpose and the legal basis for processing no longer exist (Articles 12(1) and 13, Data Protection Law).

A processor may process special category and biometric personal data without the data subject's consent only if:

- Directly permitted by law, for special category data (Article 12(1), Data Protection Law).
- Directly permitted by law that requires processing to implement the law's purpose, for biometric data (Article 13, Data Protection Law).

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 that law or agreement directly provides for:
  - the information's transfer; and
  - an adequate level of protection.
- In exceptional cases provided for by law.
- To protect the data subject's life, health, or freedom.

(Article 23, Data Protection Law.)

There are additional technical requirements to protect biometric personal data. For example, biometric personal data use and storage 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. (Article 19(6), Data Protection Law.)

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:

- The data subject's first name and surname.
- The legal basis for the processing and its purpose.
- A list of personal data that will be processed.
- A list of operations the processor will perform using personal data that requires the subject's consent.
- The persons to whom the processor may transfer the personal data.
- The requesting processor's or authorized person's surname, first name, patronymic name, and position, 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.
- The consent terms requested and the procedure for, and consequences of, withdrawing consent.

(Article 10(2), the Law of Armenia on protection of personal data.)

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

The Law of Armenia on protection of personal data (Data Protection Law) recognizes a data subject's right to:

- Obtain information on their personal data, the processing of that data, the processing's legal basis and purpose, the data processor and its registered office, and the persons to whom personal data may be transferred (Article 15(1) and (6), Data Protection Law).
- Be familiarised with their personal data (Article 15(2), Data Protection Law).
- Request that the processor rectify, block, or delete their personal data in certain cases (*see* Question 14) (Article 15(2), Data Protection Law).
- Apply to the Personal Data Protection Agency (PDPA) to request that their personal data be rectified, blocked, or deleted, and request information on the processor's rectification, blocking or deletion (Article 15(3), Data Protection Law).
- Challenge the processor's actions or inactions before the PDPA or through judicial proceedings, including claiming compensation for damages based on violations of the data subject's constitutional rights (Article 17, Data Protection Law).

Data subjects may exercise these rights by submitting a written request (Article 15(5), Data Protection Law). Processors must provide requested information free of charge (Article 15(7), Data Protection Law).

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

Yes. Data subjects may request that processors delete their personal data if the data:

- Is incomplete.
- Is inaccurate.
- Is outdated.
- Has been obtained unlawfully.
- Is not necessary to achieve the processing's purposes.

(Articles 15(2), 18(2), and 19(1), Law of Armenia on protection of personal data (Data Protection Law)). When it destroys a data subject's personal data because it is inaccurate, the processor must inform the data subject within three days (Article 20(2), Data Protection Law). A processor must respond to a data subject's written deletion request within five days. If it will not comply with the request, the processor's response must include a reasoned explanation referencing the relevant sections of the Data Protection Law justifying the processor's decision not to delete the data. (Article 20(5), Data Protection Law.)

Processors must also delete personal data when a data subject withdraws consent, unless otherwise provided by law or agreed between the data subject and the processor (Article 9(3), Data Protection Law).

Security requirements

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

There are no specific regulations relating to personal data security, except for data processors' general obligations set out in the Law of Armenia on protection of personal data (Data Protection Law), such as:

- Using encryption keys.
- Preventing unlawful access.
- Keeping data confidential.

(Article 19, Data Protection Law; see Question 8.) There are specific provisions on securing special category and biometrical personal data (see Question 7 and Question 11).

The Resolution 1175-N of Government of Armenia on 15.10.2015 (Requirements on Issues of Domestic Personal Data and Technologies for Keeping Personal Data Out of Information Systems) (in Armenian)

(Resolution) stipulates specific rules for secure biometric personal data processing. Among other requirements, the Resolution:

- Requires tangible media to prohibit copying the information in the tangible media.
- Allows state authorities and processors to the data thereon.
- Provides the possibility to identify the information within the information system. The processor should register the tangible media used. The tangible media should have unique identification number.

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

Data processors must notify data subjects or their representatives and the Personal Data Protection Agency (PDPA), if the request was received from the PDPA, when it has stopped illegal processing or deleted illegally processed personal data (Article 23(5), the Law of Armenia on protection of personal data (Data Protection Law)).

When personal data is illegally extracted from electronic systems, the processor must:

- Make an immediate public announcement.
- Report the incident to the police.
- Notify the PDPA.

(Article 23(4), Data Protection Law.) The Data Protection Law is silent on the timing to comply with these requirements.

These requirements apply even if no harm results from the breach.

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 authorized third party must process personal data under an assignment from the primary processor and may process data only within the assignment's scope. The third-party processor is responsible for ensuring that the personal data processing remains within the processing assignment's scope. If the assignment does not comply with the Law of Armenia on protection of personal data (Data Protection Law), the third-party processor must notify the data processor in writing and refuse to carry out the processing. (Article 14(3), Data Protection Law).

The assignment must be in writing and include:

- The legal grounds and conditions for the processing and the processing's purpose.
- A list of personal data subject to processing.
- The scope of data subjects.
- The persons to whom the third party may transfer personal data.
- The required technical and organizational measures to protect the personal data.
- Any other necessary information,

(Article 14(2), Data Protection Law.) Failing to include these in the assignment subjects authorized parties to liability under the Code on Administrative Offenses of Armenia (Article 189.17, Code on Administrative Offenses of Armenia).

Generally, transferring personal data to a third-party processor is lawful if the data subject consents. However, a processor may transfer personal data to third parties or grant access to data without consent where it is provided for by law, for example, if the state cadastre is obliged to provide all requested information to the attorney, prosecutor or court, and has an adequate level of protection. (Article 26(1), Data Protection Law.)

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

- The data processor is considered a special category data processor by law or an interstate agreement, which directly provides for transferring the information, and the processor has an adequate level of protection.
- The law identifies applicable exceptional cases to protect the data subject's life, health, or freedom of the data subject.

(Article 26(2), Data Protection Law.) For the requirements on data transfer inside and outside of Armenia, see Question 20 and Question 23.

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 (in Armenian) 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 Law of Armenia on protection of personal data (Data Protection Law) allows processors to transfer personal data to third countries where either:

- The data subject has consented to the transfer.
- The transfer is necessary to implement the processing's purpose, for example, to perform a contract with the data subject.

(Article 27(1), Data Protection Law.)

To transfer personal data to a third country, the processor must obtain the Personal Data Protection Agency's (PDPA's) permission. The PDPA will grant permission if it considers the data transfer agreement to ensure an adequate protection of personal data. (Article 27(3), Data Protection Law.)

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

- In compliance with international agreements.
- To a country included in a list (in Armenian) officially published by the PDPA.

(Article 27(4) and (5), Data Protection Law.) The Data Protection Law does not distinguish between cross-border data transfers 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 be transferred to foreign state bodies only under interstate agreements. Transfers to foreign non-state bodies must comply with the above rules. (Article 27(6), Data Protection Law).

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

A processor may store personal data for the period:

- Objectively necessary to implement the processing's purposes.
- Prescribed by the data subject's consent.

(Article 9(2), Law of Armenia on protection of personal data (Data Protection Law)). The Data Protection Law does not explicitly require it, but processors storing personal data for an extended period should consider the data subject's consent to the storage length, which may prompt the processor to provide the data subject with notification about further processing.

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 authorized person must enter into a data transfer agreement (see Question 17).

The national authorities have not approved any standard forms or precedents for data transfer agreements. The agreement must be in writing and include:

- The legal grounds and conditions for the processing and the processing's purpose.
- A list of personal data subject to processing.
- The scope of data subjects.
- The persons to whom the third party may transfer personal data.
- The required technical and organisational measures to protect the personal data.
- Any other necessary information,

(Article 14(2), Law of Armenia on protection of personal data.)

Agreements to transfer data abroad must ensure an adequate level of protection of personal data (see Question 20). There are no special content requirements for international data transfer agreements.

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 legitimize transfer, unless the law allows transfer without the data subject's consent and the agreement provides an adequate level of protection (Articles 26 and 27, Law of Armenia on protection of personal data (Data Protection Law)).

When data is transferred to a country that does not ensure an adequate level of data protection, the processor must obtain the Personal Data Protection Agency's (PDPA's) permission based on the PDPA's analysis of the data transfer agreement (see Question 20 and Question 22).

The Data Protection Law does not distinguish between cross-border data transfers within the same group of companies or to a third company. Therefore, the above rules apply in both scenarios. For more on the rules governing data transfers, see Question 20.

For general information on data processing agreements with third parties, see Question 17.

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 a transfer to a country that is not on the list approved by the PDPA (Article 27(3), Law of Armenia on protection of personal data).

For more information on standard contractual clauses, see Question 22.

Enforcement and sanctions

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

The Personal Data Protection Agency is entitled to:

- Verify a processor's personal data processing's compliance with the Law of Armenia on protection of personal data (Data Protection Law).
- Impose administrative sanctions for Data Protection Law violations.
- Require that personal data processing be blocked, suspended, or terminated where the processing violates 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.
- Fully or partially prohibit personal data processing following the PDPA's examination of the notification a data processor submits.
- Recognize 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 that data subjects' rights are protected.
- Consider applications brought by natural persons regarding personal data processing 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 advise on best practices for processing personal data.
- Report criminal violations 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 for violating the rules on destroying or blocking personal data.
- 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 that processors protect data subject rights.
- Ensures that personal data is lawfully processed, within the scope of its powers.
- Maintains the personal data processor registry.

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.

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*.