COUNTRY COMPARATIVE GUIDES 2024

The Legal 500 Country Comparative Guides

Armenia

DATA PROTECTION & CYBERSECURITY

Contributor

Concern Dialog Law Firm

Narine Beglaryan

Senior Partner, Attorney | narine.beglaryan@dialog.am

Ani Mkrtumyan

Associate, attorney | ani.mkrtumyan@dialog.am

Anahit Aloyan

Legal Assistant | anahit.aloyan@dialog.am

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Armenia.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

ARMENIA
DATA PROTECTION & CYBERSECURITY

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered by them; what sectors, activities or data do they regulate; and who enforces the relevant laws).

Article 34 of the Constitution of the RA and Article 8 of the European Convention on Human Rights set forth the core principles of privacy and data protection. Armenia is also a party to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter referred to as the Convention).

Apart from that, general rules concerning the processing of personal data are set out in the RA Law on Protection of Personal Data (hereinafter also referred to as the Law), adopted in 2015, which is the main legal act regulating the sphere.

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

At the same time, the Law lists the cases when the sectoral laws may define special rules. Namely, issues such as state and official secrets, banking, notarial, and insurance secrecy, legal professional privilege, personal data use during operations concerning national security or defense, personal data use in preventing and detecting money laundering, terrorism financing, and operational intelligence activities and proceedings are regulated by subsequent sectoral laws. Such laws include but are not limited to the RA Law on Medical Assistance and Service to the Population, the RA Law on Bank Secrecy, the RA Law on Insurance and Insurance Activity, the RA Law on Combating Money Laundering and Terrorism Financing, the RA Law on Circulation of Credit Information and Activities of Credit Bureaus, the Labor Code of RA, the RA Law on Electronic Communications, the Code on Administrative Offenses of RA, etc.

There is currently no specific law governing cybersecurity in the RA's jurisdiction (see questions 2 and 48). However, Armenia is a party to the Convention on Cybercrime, which penalizes the unauthorized access to and manipulation of personal data stored in computer systems.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2024–2025 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments (together, "data protection laws"))?

There is currently a legislative project on the Law of RA on Cybersecurity. This law aims to create a cyber-safe environment in information systems and critical information infrastructures used to provide vital services in the Republic of Armenia. The law aims to regulate relations related to the detection of cyber incidents, their notification, prevention and resolution, monitoring, control, and cyber security audit of compliance with the requirements of this law, as well as defines the scope of the subjects who are obliged to ensure the information systems and critical information they use, cyber security of infrastructures, their continuous, uninterrupted, and safe use. In the case of passing this law, there are also suggestions for making corresponding amendments to other laws of the RA containing data protection regulations, as presented in question 48.

In addition, the RA Government's action plan for years of 2021 to 2026 establishes as a goal the improvement of the personal data protection level in the RA, particularly by the help of alignment of newly adopted as well as current legal acts concerning personal data protection

with the provisions and general principles set forth in the Law, as well as strengthening the capacities such as human, professional and technical resources of the Agency. Concerning the strengthening of the capacities of the Agency, first of all, it implies the increase of its operational independence and the increase of the staff.

However, it should be noted that according to the Government's action plan it should have been conducted before the end of December of 2023, meanwhile, according to the report of the Government for the year of 2023, such strengthening has not been conducted because of the lack of financial resources. Hence, it is expected to be conducted before the end of 2026.

3. Are there any registration or licensing requirements for entities covered by these data protection laws, and if so what are the requirements? Are there any exemptions?

The data protection laws of RA do not require licensing or registration for entities covered by the Law.

4. How do these data protection laws define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data") versus special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction?

Under the Law, personal data is defined as any information relating to a natural person that allows or may allow for direct or indirect identification of a person's identity.

In addition, the Law differentiates between certain categories of personal data.

It defines the concept of special category personal data, which is information relating to a person's race, national identity or ethnic origin, political views, religious or philosophical beliefs, trade union membership, health condition, and sexual life.

Another key definition set forth in the Law is biometric personal data, which is information relating to a person's physical, physiological, and biological characteristics.

As well as, the Law defines the category of publicly available personal data, which means information, which, by the data subject's consent or by conscious operations aimed at making his or her personal data publicly available, becomes publicly available for certain scope of persons or public at large, as well as information, which is provided for by law as publicly available information.

Together with these definitions, the Law differentiates between personal data and the data on personal life. According to the Law the second one is a narrower concept and means the information on personal life, family life, physical, physiological, mental, social condition of a person or other similar information.

5. What are the principles related to the general processing of personal data in your jurisdiction? For example, must a covered entity establish a legal basis for processing personal data, or must personal data only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

Armenian legislation on data protection provides for four general principles, which reflect the main principles also established by the RA Constitution and the Convention.

First is the principle of lawfulness, which obliges the data controller/processor to comply with and ensure that personal data is processed in compliance with the requirements prescribed by law. Additionally, personal data should be processed for specified and legitimate purposes and cannot be used for purposes other than those for which the data subject has given consent (purpose limitation clause). The processing of data is deemed lawful, where:

- the data have been processed in observance of the requirements of the Law and the data subject has given their consent, except for cases directly provided for by Law or other laws or
- the data being processed have been obtained from publicly available sources of personal data. As per court practice the data subject should be notified about processing of his/her personal data received from publicly available sources.

Second is the principle of proportionality, which establishes that data processing should be justified by specific and legitimate purposes, and the means to achieve them must be adequate, necessary, and proportionate. Personal data should be processed in the

minimum amount necessary to achieve the specified purposes. The processing of such personal data, which is unnecessary or incompatible with the intended purposes, is prohibited. Moreover, the processing of personal data is prohibited if the purpose of processing the data can be achieved in a depersonalized manner. Finally, personal data shall be preserved in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which those data are processed.

According to the third principle, which is that of reliability, processed data shall be complete, accurate, clear, and, where necessary, kept up to date.

Fourth is the principle of minimum engagement of data subjects in the process. This means that the state and local self-government bodies or the notary can obtain personal data from another body through the unified electronic information system, then the data subjects are not themselves required to submit the personal data necessary for certain actions. If it is directly indicated in the written consent of the data subject, natural or legal persons considered to be processors of personal data may receive from the state or local self-government bodies the personal data necessary for a certain operation. The procedure for the transferring of personal data through the electronic information system is defined by the Government of the Republic of Armenia.

6. Are there any circumstances for which consent is required or typically obtained in connection with the general processing of personal data?

The RA legislator adopted the approach that the data subject's consent is always required except for the cases directly provided by RA legislation.

In the event of the death of the data subject, their personal data, such as the name, gender, year, month, date of birth and death of the deceased person may also be processed without consent.

Other specific cases when consent is not required to process personal data are established by sectoral laws. For example, the RA Law on Medical Assistance and Service to the Population establishes cases when the personal data of patients can be processed without their consent. One such case is the processing of the personal data for the purpose of organizing and implementing preventive measures (including medical care and services) in emergency situations without the consent of a data subject.

7. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

It is important to note that Armenian court of cassation has established that in compliance with the requirements of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter: the Directive) and taking into account that the Law has been drafted based on the principles set forth in the Directive, the data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

As for the domestic regulations, according to the Law, the data subject's consent is deemed to have been given, and the controller has the right to process relevant data in the presence of the below mentioned conditions:

- the personal data is indicated in the document addressed to the controller and signed by the data subject, except for the cases when the content of the document is an objection to the processing of personal data;
- the controller has received the data on the basis of the contract signed with the data subject and uses it for the purposes defined by that contract,
- the data subject verbally transmits information about their personal data to the controller for the purpose of use.

Hence, the consent may be incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations), the important is that the consent is given freely and contains the specific and informed indication of data subject's wishes, as well as the data to be processed and the exact purposes of the data processing.

The consent of the data subject shall be given either in writing or verbally.

In order to obtain the data subject's consent, the

controller/processor shall notify the data subject. The requirements set for the content of notification reflect the requirements posed to the content of consent as well. Namely, it shall include the following information:

- last and first names and the patronymic of the data subject;
- the legal basis and purpose of personal data processing;
- the list of personal data to be processed;
- the list of actions to be performed with personal data for which the consent of the data subject is requested;
- the range of persons to whom personal data may be transferred, the name (surname, first name, patronymic, position) of the controller/processor requesting the consent of the subject of personal data and the place of location or registration (actual residence);
- information on requesting correction, destruction of personal data, termination of data processing or performing other processing-related actions by the data subject; and
- the period of validity of the requested consent, as well as the procedure for withdrawing the consent and its consequences.

In addition, as for the rules governing the administration of consent, the Law states that the data subject can give its consent in person or through a representative if the power of attorney specifically provides for such authorization. As well as, it is noted that in case of incapacity or limited capacity of the data subject or of being a minor under the age of 16, consent for processing his or her personal data shall be given by a legal representative of the data subject.

8. What special requirements, if any, are required for processing sensitive personal data? Are any categories of personal data prohibited from collection or disclosure?

It is prohibited to process special category personal data without the data subject's consent, except when the data processing is directly allowed under the law. Moreover, the processing of such data shall immediately be stopped if the grounds and purpose of data processing have ceased to exist.

On the other hand, in the case of biometric personal data, the consent of the data subject is always required, except for cases provided by law and if the purpose pursued by law can be achieved only through processing such biometric data.

It should be noted that for processing the biometric and special category personal data, one should notify the Personal Data Protection Agency as well as provide additional security rules prescribed for the processing of the mentioned information.

The general rule is that if the requirements of laws and other normative legal acts are followed, then there is no specific type of data that is forbidden from being collected or disclosed.

According to the Law the data controller/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 under ratified international agreement and that law or agreement directly provides for the possibility of the information's transfer and the adequate level of protection.
- in order to protect the data subject's life, health, or freedom in exceptional cases provided by law.

Concerning the technical requirements applicable to the biometric personal data, the Law establishes that its use and storage on information systems can only be carried out through tangible media and technology that ensure protection from unauthorized access, unlawful use, destruction, alteration, blocking, copying, dissemination, and so on.

Meanwhile, the Labor Code of the RA has established a different approach concerning certain categories of personal data. Particularly, as a general rule it prohibits the employer from collecting or processing the personal data of the employee concerning its membership in public associations, or activity in trade unions, except for the cases provided by the RA legislation. As well as, the employer in any case is prohibited to collect or process personal data concerning employee's political, religious, and other beliefs. As for the personal data on the personal life, the employer has the right to receive and process data about the employee's personal life only with his written consent in cases directly related to employment relations.

9. How do the data protection laws in your jurisdiction address health data?

The RA Law on Medical Assistance and Service to the Population defines the concept of medical secret, which

is information about the patient's health condition or about applying for or receiving medical care and service, as well as data revealed during the provision of medical care and service. Meanwhile, depersonalized data cannot be considered as a medical secret and can be used for conducting scientific activities.

The law also establishes the concept of transfer of data considered a medical secret. It refers to any action (inaction) aimed at transferring or disclosing such data to a certain or indefinite group of people, including publishing confidential data through mass media, placing it on information communication networks or making it available to another person in another way. As a general rule, for transferring such data the consent of the patient or their legal representative is needed, except for cases expressly provided by the same law. For example, when transfer of information is required for provision of medical care and service to the patient, if such provision will be impossible without this data, etc. In any case, such transfer should be carried out according to the procedure established by the Government.

Moreover, carrying out an act considered to be a transfer of a medical secret in violation of the law by the person in possession of a medical secret causes liability under the law (see answer to question 33). The duration of retention periods of data considered a medical secret (including electronic documents) is also established by the Government and varies depending on the type of data

It is also worth noting that currently Armenia is in the process of implementing an electronic healthcare system, therefore, a number of Government decisions and orders are being passed to, including those regulating the procedure of accessing and viewing the patient personal data, including special category personal data, stored in the electronic information access windows as well as other similar issues.

10. Do the data protection laws in your jurisdiction include any derogations, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

The Armenian Constitutional Court's decision on determining the question of the conformity of obligations established by the amendments to the Convention with the RA Constitution guarantees that the Convention will not be applied to data processing carried out by an individual in the course of purely personal or household activities.

11. Do the data protection laws in your jurisdiction address children's and teenagers' personal data? If so, please describe how.

According to the Law the consent to the processing of personal data is given by the legal representatives of the data subject under the age of 16. No special regulations are established for the processing of personal data of children over 16, which means that the data subject under the age of 16 gives itself the consent on the data processing. The general regulations concerning the data subject's consent, as defined in questions 6 and 7, apply to the consent required both from the legal representatives and the children (above the age of 16) themselves.

It's also important to note that the Agency has published guidelines and advisory decisions on the specifics of protecting children's personal data, which particularly emphasizes the importance of the application of the principle of the best interests of the child when processing its data. Additionally, in the annual report of Human Rights Defender of the RA, a separate section is dedicated to the issues related to the protection of children's personal data in the RA (for more detail, see question 13).

12. Do the data protection laws in your jurisdiction address online safety? Are there any additional legislative regimes that address online safety not captured above? If so, please describe.

No data protection laws in Armenia's jurisdiction specifically address online safety, but the general principles and procedures defined by the Law broadly encompass online safety. Particularly, the Law authorizes the Agency to recognise electronic systems for processing of personal data of legal persons as having an adequate level of protection and include them in the register. Correspondingly, the legal persons processing personal data, for having recognised electronic systems for processing of personal data under their possession as having an adequate level of protection and including them in the register, may apply to the Agency for the protection of personal data.

The law also establishes that in the event of outflow of personal data from electronic systems, the controller must immediately publish an announcement about the incident. In parallel with the publication of the announcement, the controller shall officially report on the outflow to the Police of the Republic of Armenia, as

well as the Agency for Protection of Personal Data of Armenia.

13. Is there any regulator in your jurisdiction with oversight of children's and teenagers' personal data, or online safety in general? If so, please describe, including any enforcement powers. If this regulator is not the data protection regulator, how do those two regulatory bodies work together?

There is no special regulator as such in the RA jurisdiction with oversight of children's and teenagers' personal data. In general, administrative control over personal data protection in Armenia is carried out by the Agency, however, the Agency does not have the personal data audit capacities . Additionally, the Human Rights Defender of the RA is responsible for monitoring compliance with the provisions of the UN Convention on the Rights of the Child, which, among others, includes a child's right to privacy. Hence, there is a separate department for the protection of children's rights at the Office of the Human Rights Defender (see question 11).

14. Are there any expected changes to the online safety landscape in your jurisdiction in 2024-2025?

There is currently a legislative project on passing a law on cybersecurity as presented in questions 2 and 48, which will also involve the amendments to the Law.

15. Does your jurisdiction impose 'data protection by design' or 'data protection by default' requirements or similar? If so, please describe the requirement(s) and how businesses typically meet such requirement(s).

Armenian legislation does not address the issues of data protection by design or by default, i.e. no rules such as defined under Article 25 of GDPR could be found out under the Law.

16. Are controllers and/or processors of personal data required to maintain any internal records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

The Law does not require the controllers/processors to maintain any internal records of their processing activities. However, the sectoral laws provide such requirements, particularly in accordance with the requirements of the RA Law on Medical Assistance and Service to the Population, the decision N 99-Ա dated 17.01.2022 of the Minister of heath of the RA has been adopted on the procedure for updating data in the e-health system, patient visits, services provided, medical interventions, diagnoses, appointments, human health and personal data entry, including data of a special category.

17. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? If so, please describe such requirement(s).

Data protection laws in Armenian jurisdiction do not require or recommend data retention and/or data disposal policies and procedures.

Nevertheless, in case of labor relations, the RA Labor code establishes that the transfer of the personal data of the employees shall be carried out in accordance with the internal legal acts of the employer, in addition it is also mentioned that the employees and their representatives by their signature shall become familiarized with legal acts of the employer that define the procedure for processing the personal data, as well as about their rights and obligations in this sphere. Hence, even though it is not explicitly requested to the employers to have internal policies on the personal data processing or retention, however, it may be implied from the logic of the regulations.

18. Under what circumstances is a controller operating in your jurisdiction required or recommended to consult with the applicable data protection regulator(s)?

No specific circumstances are defined by the Law when the controller operating in Armenia's jurisdiction is required or recommended to consult with the applicable data protection regulator. However, the Law establishes the function of the Agency to conduct research and, based on requests or disclosures from controllers,

provide consultation or information about best practices for processing personal data. Hence, in any circumstances, controllers have the right to consult with the regulator if necessary.

19. Do the data protection laws in your jurisdiction require or recommend risk assessments in connection with data processing activities and, if so, under what circumstances? How are these risk assessments typically carried out?

The data protection laws in the jurisdiction of RA do not require or recommend any risk assessments in connection with data processing activities.

20. Do the data protection laws in your jurisdiction require a controller's appointment of a data protection officer, chief information security officer, or other person responsible for data protection, and what are their legal responsibilities?

The data protection laws in Armenia's jurisdiction do not require a controller to appoint a data protection or privacy officer or chief information security officer or other person responsible for data protection.

21. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s).

There are no requirements or recommendations on employee training related to data protection in RA's jurisdiction.

22. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

The Law requires controllers to provide notice to data subjects of their processing activities to gain consent for such processing (for further details see question 7).

In addition, the Law also establishes that where the personal data have been obtained not from the data subject, except for cases provided for by law, as well as publicly available data, the processor, before processing such personal data, shall be obliged to provide the data subject with the following information:

- name (surname, name, patronymic) of the processor or his or her authorized person (if any) and registered office or place of registration (actual residence);
- purpose and the legal ground for processing personal data, the list of data being processed;
- scope of potential users of personal data;
- rights of the data subject prescribed by Law.

23. Do the data protection laws in your jurisdiction draw any distinction between the controllers and the processors of personal data, and, if so, what are they?

The RA legislation does not distinguish between the concepts of "controller" and "processor." Particularly, the Law does not use the term "**controller**", as used in GDPR and instead uses the terms "processor" and "authorized persons".

According to the Law the **data processor (the "Controller")** is a state administration or local self-government body, state or community institution or organization, legal or natural person, which organizes and/or carries out processing of personal data.

Meanwhile **the authorized person** (**the "Processor"**) is considered to be a person that a data controller authorizes to collect, input, organize, or otherwise process personal data in cases prescribed by law or under an agreement.

Hence, one can conclude that in the meaning of Armenian legislation, the person receiving personal data is addressed as the "processor," whereas the further processor of the personal data by the assignment of the controller is referred to as the "authorized person." Despite the difference in terminology, they shall all comply with the same rules set forth for the processor of personal data.

24. Do the data protection laws in your jurisdiction place obligations on processors by operation of law? Do the data protection laws in your jurisdiction require minimum contract terms with processors of personal

data?

The Law obliges the processors to process personal data only within the framework of the assignment received from the controller. The controller is responsible for the processing of personal data within the scope of the assignment. If the assignment does not meet the requirements of the Law, the processor must inform the controller in writing and refuse to complete it.

The assignment is given in writing and must state the legal basis and conditions for processing personal data, the purpose, the list of personal data to be processed, the scope of data subjects, the scope of persons to whom personal data can be transferred, technical and organizational measures for the protection of personal data and other necessary information.

Further specifics of personal data processing by the processor may be defined by other laws or agreements concluded between the controller and the data processor, which, however, may not refer to the rights and obligations of other persons.

25. Are there any other restrictions relating to the appointment of processors (e.g., due diligence, privacy and security assessments)?

There aren't any other restrictions relating to the appointment of processors in Armenian legislation.

26. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these terms defined, and what restrictions on their use are imposed, if any?

Monitoring, automated decision-making, or profiling, including through the use of tracking technologies such as cookies, are not specifically addressed by the Armenian legislation. However, the main principles set forth by the Convention and further stipulated in the Law, as well as the requirements for gaining the data subject's consent, broadly encompass the restrictions imposed on any type of automated processing of personal data (see questions 5 and 6).

27. Please describe any restrictions on targeted advertising and/or cross-contextual behavioral advertising. How are these terms or any similar terms defined?

Neither the Law nor the Convention directly addresses targeted advertising or cross-contextual behavioral advertising. However, the general principles of data protection and respect for individuals' rights shall serve as a foundation for regulating these practices (see questions 5 and 6).

Nevertheless, the Agency has published its advisory decision on the use of the personal phone numbers for the advertising purposes, in which it has addressed the principles applicable to direct marketing highlighting the need of the data subject's consent and the importance of the availability of opt-in and opt-out options (see question 29).

28. Please describe any data protection laws in your jurisdiction addressing the sale of personal data. How is the term "sale" or such related terms defined, and what restrictions are imposed, if any?

The RA legislation does not directly address the question of the sale of personal data.

The Law in addition to the definition of the personal data also gives the definition of the database as the is a collection of personal data systematized according to certain characteristics. The RA Law on Copyright and Related rights also defines the concept of a database being type of derivative work as a collection of works, data or other independent materials arranged in a systematic or methodical way the individual elements of which shall be separately accessible by electronic or other means and the acquisition, verification or presentation thereof shall require substantial qualitative and (or) quantitative contribution. Hence, it is possible to address the possibility of the sale of personal data being collected as a database in the light of the RA law on Copyright and related rights.

According to this law the maker of a database shall be deemed any person by whose initiative and on whose own responsibility substantial qualitative and (or) quantitative contribution is made for the acquisition, verification, or presentation of the content of the database. The latter may transfer/sell the proprietary rights of the database to a third person wholly or in part by a contract, or may allow the use of the database provided that the contract specifies the form and term of use of the database, the amount of remuneration and the payment order, the area, etc.

29. Please describe any data protection laws in your jurisdiction addressing telephone calls, text messaging, email communication, or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

The RA Law on Electronic Communications obliges the operators and service providers to keep the confidentiality of their customers' information. Namely, they are obliged to treat and keep confidential information regarding the type of services used by the customer, location, purpose, destination, quantity, technical conditions, and the personal data of customers. This law also provides for situations when an operator or service provider shall be entitled to disclose such information, for example, in situations provided for by law in connection with surveillance, inquest, or criminal prosecution with regard to a criminal offense or threat to national security;

- upon the written consent of the customer;
- where the disclosure is necessary in defense of the operator or service provider (proceedings are pending against that operator or service provider);
- in case of emergency situations and other cases provided by the law.

The RA Law on Electronic Communications also regulates the confidentiality of text messaging email communication by providing that a person other than a party to a message transmitted by any electronic communications means may intercept, record, or disclose the content of such message only upon the written consent of the parties to the message or upon a court order in cases and in the manner provided for by law.

As for the direct marketing regulations, there are no specific domestic regulations adopted, however as mentioned (see question 27), the Agency has published its advisory decision on the use of the personal phone numbers for the advertising purposes. In this decision, the Agency states that the persons engaged in direct marketing, as well as organizations (or operators) providing electronic communication services, have the following minimum obligations:

- use personal data, including personal phone number, only with the consent of the data subject, for a predetermined purpose, in appropriate, necessary and moderate amount for achieving the goal,
- provide data subject with the information on the processed personal data, as well information about the source, purposes and legal grounds for collecting personal data, terms of use, as well as information about the organization carrying out direct marketing,
- implement organizational or technical (software) tools that allow to protect personal data from accidental or illegal destruction, modification, illegal acquisition or other illegal use,
- allow data subject preliminarily (opt-in) or at any time (opt-out) stop processing of the personal data for direct marketing purposes,
- take the necessary and maximum organizational, technical (programmatic) measures to prevent the use of data subject's personal data by third parties for direct marketing purposes without the consent of the data subject,
- provide regulations on the use of the personal data for the purposes of direct marketing in the contracts being concluded between electronic communication provision organizations and the data subject-subscriber.

30. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined, and what restrictions are imposed, if any?

Biometric personal data is a type of sensitive data, hence, restrictions are imposed on the processing of such data by the Law as defined in question 8, as well as the requirements for the material carriers of biometric personal data and the technologies for maintaining such personal data outside the information systems are defined by the decision of the Government of the Republic of Armenia from 15 October 2015 N 1175-Ա. Finally, the use and storage of biometric personal data outside of information systems can be carried out only through such material carriers, using technologies or forms that ensure the protection of such data from illegal access, illegal use of personal data, destruction, transformation, blocking, duplication, dissemination, etc.

31. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

There aren't any data protection laws in Armenia's jurisdiction addressing artificial intelligence or machine learning ("AI").

32. Is the transfer of personal data outside your jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

Personal data may be transferred to another country with the consent of the data subject or if the transfer of data results from the purposes of personal data processing and/or is necessary for the fulfillment of these purposes.

The authorization of the Agency to transfer personal data to another country may not be needed if a sufficient level of protection of personal data is ensured in the receiving country. A sufficient level of personal data protection is considered to be provided if personal data is transferred in accordance with international agreements or personal data is transferred to any country included in the list officially published by the Agency. Personal data may be transferred to the territory of a state that does not provide a sufficient level of protection only with the permission of the Agency, if the personal data is transferred on the basis of a contract, and the contract provides such guarantees of personal data protection, which have been approved by the Agency as providing sufficient protection. In such cases, the controller is obliged to apply in writing to the Agency and receive permission to transfer. The Law also specifies the requirements for the application.

33. What security obligations are imposed on data controllers and processors, if any, in your jurisdiction?

Generally, the Law does not impose specific security obligations on data processors/controllers, however it is mentioned that the data controller in the course of processing personal data shall be obliged to use encryption keys to ensure the protection of information systems containing personal data against accidental loss, unauthorized access to information systems, unlawful use, recording, destructing, altering, blocking, copying, disseminating personal data and other interference.

In addition, the Law also establishes that the data controller shall be obliged to prevent the access of appropriate technologies for processing personal data for persons not having a right thereto and ensure that only data, subject to processing by him or her, are accessed by the lawful user of these systems and the data which are allowed to be used. Besides, the Law states that the requirements for ensuring the security of personal data processing in information systems should be defined by the RA Government decision, however no such decision is still adopted.

As for the responsibility, article 189.17 of the RA Code of Administrative Offences establishes liability for violating the requirements of the Law. Depending on the type of violation, the liability may range between AMD 50,000 to AMD 500,000. Further, the Criminal Code of the RA criminalizes actions such as violations of privacy of personal or family life (Art. 204), divulging medical secrets (Art. 205), violation of the secrecy of correspondence, telephone conversations, postal, telegraph or other communications (Art. 206), Illegal use, collection or divulging of commercial, insurance, tax, customs, pension, service or bank confidential information or credit history or credit information available at a credit bureau (Art. 278-280). For such crimes punishments ranging from fine to imprisonment are envisaged.

34. Do the data protection laws in your jurisdiction address security breaches and, if so, how do such laws define a “security breach”?

The Law addresses a security breach such as the leakage of personal data from electronic systems. In such a case, the controller is obliged to immediately publish a statement about it while also informing the Police of the RA and the Agency.

Another security breach envisaged by the Law is the detection of illegal actions with personal data. In such a case, the controller is obliged to eliminate the committed violations immediately but not later than within three working days. In case of impossibility to eliminate the violations, the latter is obliged to immediately destroy the personal data and inform the data subject or his representative about eliminating violations or destroying personal data within three working days, also inform the Agency if the request was received from it.

35. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecom, infrastructure, AI)?

Armenian legislation imposes specific security requirements on the telecom sector, which are established in the Law of the Republic of Armenia on

Electronic Communications (see question 29).

36. Under what circumstances must a business report security breaches to regulators, impacted individuals, law enforcement, or other persons or entities? If breach notification is not required by law, is it recommended by the applicable regulator in your jurisdiction, and what is customary in this regard in your jurisdiction?

It is required to inform the Agency, impacted individuals, and law enforcement bodies about the leakage of personal data from electronic systems and the detection of illegal actions with personal data in cases and through the procedure defined in question 34.

37. Does your jurisdiction have any specific legal requirements or guidance for dealing with cybercrime, such as in the context of ransom payments following a ransomware attack?

The Armenian legislation does not have any specific legal requirements or guidance for dealing with cybercrime, however as explained in question 1 Armenia has ratified the Convention on Cybercrime.

38. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

Currently, there is no cybersecurity regulation adopted in Armenia. However, according to the project of the RA law on Cybersecurity such a regulator with the responsibility to impose administrative penalties for violations of the requirements of the expected Law on Cybersecurity should be created (for more detail, see questions 2 and 48).

39. Do the data protection laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, any exceptions and any other relevant details.

The Law provides the data subject with the right to withdraw their consent in the cases and procedures provided by the laws (as mentioned, the prior notification sent to the data subject for receiving its consent on the data processing should contain the information on the procedure of the withdrawal of the consent). In case of withdrawal of the data subject's consent, the controller shall be obliged to terminate the processing of personal data and destruct the data within ten working days following the receipt of the withdrawal, unless otherwise provided for by mutual consent of the data subject and the controller or by law. The controller shall be obliged to inform the data subject on the destruction of personal data within three working days upon destruction.

In addition, the data subject also has the right to receive information about their personal data, the basis and purposes of its processing, on the processor of the data, its location, as well as the scope of the persons to whom the personal data can be transferred. The data subject has a right to receive this in an accessible form. Not only the data subject has the right to get familiarized with his or her personal data, but also to require from the data controller 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.

40. Are individual data privacy rights exercisable through the judicial system, enforced by a regulator, or both?

Individual data privacy rights are exercisable through both the judicial system and enforced by the regulator. Namely, in case the data subject has required from the controller 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, and as a result has doubts concerning personal data being edited, blocked, or destroyed by the controller, then the data subject can apply to the Agency with a request to investigate the issue and inform them.

In case the data subject considers that the processing of their personal data is being carried out in violation of the requirements of the Law or in any other way that infringes upon their rights and freedoms, it has the right to appeal the actions or inaction or decisions of the controller to the Agency or in court.

41. Do the data protection laws in your jurisdiction provide for a private right of

action and, if so, under what circumstances?

As it is described in the answer to question 40 the Law allows data subjects to appeal the controller's actions, inactions, or decisions to the Agency or in court. The right to private action can be exercised by reporting a crime (see question 33) or filing a civil lawsuit. If the controller is a state or local self-government body, then the claim must be filed with the Administrative Court of the RA.

42. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual damage to have been sustained, or is injury to feelings, emotional distress or similar sufficient for such purposes?

The Law also establishes the data subject's right to compensation for damages in accordance with the law. The damages shall comprise expenses, incurred by the data subject, which have been or must be covered by data subject in order to restore the violated right, the loss of or harm to the property thereof (actual damage), unearned income that the data subject would have received under the usual conditions of civil practices had the right thereof not been violated (lost benefit).

The data subject can seek compensation for injury to feelings, emotional distress or similar only if the preliminary investigation body, the prosecutor or the court has confirmed that as a result of the decision, action or inaction of the state or local self-government body or its official, the fundamental rights guaranteed by the Constitution of the RA and the European Convention on Human Rights of the data subject have been violated.

43. How are data protection laws in your jurisdiction enforced?

Data protection laws are enforced primarily through administrative enforcement by the Agency. The Agency has investigative and corrective powers such as checking the compliance of personal data processing with the requirements of the laws, applying measures of administrative responsibility (see question 33), demanding to block, suspend, or terminate the processing of personal data violating the requirements of the Law, require the processor to correct, change, block or destroy personal data, prohibit the processing of personal data in whole or in part, etc. The decisions of the Agency are not directly subject to state compulsory enforcement, hence in case of not being enforced voluntarily the Agency can file a claim with the Administrative Court of the RA. In addition, the decisions of the Agency are subject to judicial appeal.

The Agency can also submit reports to the law enforcement authorities in case of suspicions regarding violations of a criminal nature as it is indicated in the answer to the question 33.

44. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

The sanctions range from fines to imprisonment depending on the nature of violation as it is presented in the answer to question 33.

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

There aren't any specific guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions.

46. Can controllers operating in your jurisdiction appeal to the courts against orders of the regulators?

The Law establishes that decisions of the Agency can be appealed in court. Such a claim should be filed with a specialized Court, namely the Administrative Court of the RA in accordance with the general procedure defined in Administrative Procedure Code of the RA.

47. Are there any identifiable trends in enforcement activity in your jurisdiction?

Some identifiable trends in the enforcement activity in the Armenian jurisdiction have been set forth in the Government's action plan for years of 2021 to 2026, which foresees alignment of newly adopted as well as current legal acts concerning personal data protection with the provisions and general principles set forth in the Law and strengthening the capacities such as human, professional and technical resources of the Agency.

48. Are there any proposals for reforming data protection laws in your jurisdiction currently under review? Please provide an overview of any proposed changes and the legislative status of such proposals.

As discussed in question 2, there are legislative prospects for passing a law on cybersecurity. Along with this legislative project, proposals were also made on making minor amendments to the laws of the RA on the Protection of Personal Data and on Electronic Documents and Electronic Digital Signatures to align with the provisions of the proposed law on cybersecurity. The project of the discussed law also establishes the creation of a new regulatory authority in the sphere of cybersecurity.

Also, the same law project suggests making amendments in the Code of the Administrative Offences of the RA in order to regulate the violations of the requirements of the Law on Cybersecurity. Passing the Law on Cybersecurity will also require amendments and additions to the RA law on National Security Bodies, the legislative project of which has also been proposed.

One of the expected amendments, among others, that has found its place in the law project is the requirement of compliance with the ISO certification standards, as well as establishment of minimum requirements of the cybersecurity by the RA Government.

Contributors

Narine Beglaryan
Senior Partner, Attorney
narine.beglaryan@dialog.am

Ani Mkrtumyan
Associate, attorney
ani.mkrtumyan@dialog.am

Anahit Aloyan
Legal Assistant
anahit.aloyan@dialog.am