PANORAMIC

# DATA PROTECTION & PRIVACY

Armenia

LEXOLOGY

# Data Protection & Privacy

Contributing Editors

**Aaron P Simpson and Lisa J Sotto**

Hunton Andrews Kurth LLP

**Generated on: July 6, 2024**

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. Copyright 2006 - 2024 Law Business Research

Explore on **Lexology**

# Contents

## Data Protection & Privacy

## SHARING AND CROSS-BORDER TRANSFERS OF PI



## RIGHTS OF INDIVIDUALS



## EXEMPTIONS, DEROGATIONS AND RESTRICTIONS



## SPECIFIC DATA PROCESSING



## UPDATE AND TRENDS

# Contributors

## Armenia

Concern Dialog Law Firm

**Narine Beglaryan** narine.beglaryan@dialog.am
**Ani Mkrtumyan** ani.mkrtumyan@dialog.am

## LAW AND THE REGULATORY AUTHORITY

### Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The RA Constitution determines the right to protection of personal data of an individual as a fundamental human right. It also establishes that the more detailed regulations related to the protection of personal data shall be prescribed by law.

Accordingly, in 2015 the Law of the Republic of Armenia on protection of personal data (the Law) was adopted, which sets out general rules concerning the processing of personal data applicable in both the private and public sectors.

Regarding supranational agreements, it should be noted that the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) is not applicable in Armenia.

However, 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.

Additionally, as a member of the Council of Europe, Armenia ratified the Convention for the Protection of Individuals regarding Automatic Processing of Personal Data (CETS No.108) on 1 September 2012. On 26 November 2021, Armenia also ratified the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed on 10 October 2018.

Armenia does not have a specific cybersecurity law, but it is part of the Convention on Cybercrime, which makes it illegal to access or change personal information stored on computer systems without permission. In addition, there is currently a legislative project to pass a law on cybersecurity, which among other things provides for the creation of a new regulatory authority in the sphere of cybersecurity.

**Law stated - 21 May 2024**

### Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The authorised body for the protection of personal data is the Personal Data Protection Agency (PDPA) of the Ministry of Justice of Armenia, which operates independently based on the respective Armenian legislation. It is a separate subdivision of the Ministry of Justice (the PDPA is financed by the state budget) according to its charter; however, the PDPA is directly managed by the Head of the PDPA. Among the responsibilities of the PDPA are the following:

-

verifying personal data processing compliance with the Law on its initiative or based on an application;

- imposing administrative sanctions for violations of the Law;
- requiring that personal data processing be blocked, suspended or terminated where the processing violates the requirements of the Law;
- requiring data processors to rectify, modify, block or delete personal data;
- fully or partially prohibiting personal data processing following the PDPA's examination of a notice submitted by the data processor;
- recognising electronic systems used for processing personal data as ensuring an adequate level of protection and including them in the corresponding register;
- ensuring that data subjects' rights are protected;
- submitting, once a year, a public report on the current situation in the field of personal data protection and on the activities of the previous year;
- considering applications brought by natural persons regarding personal data processing and issuing decisions within the scope of its authorities;
- conducting research and providing advice on data processing on request or on its own initiative and advising on best practices for processing personal data; and
- reporting criminal violations identified in the course of its activities to law enforcement bodies.

**Law stated - 21 May 2024**

## Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

There are no such obligations imposed on the PDPA by Armenia legislation because currently there are no other officials with data protection-related responsibilities.

The PDPA is deemed an administrative body, which means the decision of PDPA is subject to judicial review as per claims brought to the specialised administrative court of Armenia.

**Law stated - 21 May 2024**

## Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

A breach of the Law entitles individuals to seek judicial or administrative remedies.

Data subjects may appeal the decisions, actions or inaction of the data controller both before the PDPA or through judicial procedure if the data subject considers that the processing of

their personal data is carried out in violation of the requirements of the Law or otherwise violates their rights and freedoms.

In particular, the RA Code of administrative offences, in article 189.17, provides administrative sanctions for infringements of the Law that are not subject to criminal liability. Fines vary depending on the rule violated (violation of the procedure established by law for the destruction or blocking of personal data, or not using encryption tools when processing personal data, failure by the personal data controller to notify the PDPA or violation of the notification procedure, etc.). The highest fine is 500,000 drams for violating the rules on destroying or blocking personal data.

In addition, the Criminal code of Armenia criminalises actions such as violations of privacy of personal or family life, 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; violation of the secrecy of correspondence, telephone conversations, postal, telegraph or other communications; and divulging medical secrets. The applicable punishments range from fines to imprisonment.

**Law stated - 21 May 2024**

### Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

Data subjects are entitled to appeal the action or inaction of the PDPA or the legality of the decisions of the PDPA before the Armenian administrative court.

**Law stated - 21 May 2024**

## SCOPE

### Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Law of the Republic of Armenia on protection of personal data (the Law) regulates the procedure and conditions for processing personal data by the state administration or local self-government bodies, state or community institutions or organisations, and legal or natural persons, as well as the exercise of state control over such processing.

The Law specifies that specific regulations concerning the following matters are also provided by other laws:

- state and official secrets;
- banking, notarial and insurance secrecy;
- legal professional privilege;
- personal data used during operations concerning national security or defence; and
-

personal data used in preventing and detecting money laundering, terrorism financing, and operational intelligence activities and proceedings.

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

**Law stated - 21 May 2024**

## Interception of communications and surveillance laws

### Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The interception of communications, electronic marketing or monitoring and surveillance of individuals is not specifically addressed by the Law. The interception of communications, monitoring and surveillance of individuals are are regulated by the Criminal Procedural Code of Armenia, which establishes specific regulations concerning two categories of confidential investigative actions:

- control of correspondence and other non-digital communications; and
- digital control, including telephone communication.

There are no regulations on electronic marketing or related PI processing regulations established by the Law. Nevertheless, the Armenian law on electronic communications protects the privacy and confidentiality of customer information held by operators and service providers. This includes data such as types of services used, customer location, purpose and destination of communications, data volume, technical details and customers' personal data.

The mentioned law outlines specific situations in which operators or service providers may disclose customer information. For instance, the operator may disclose the customer data required by law for investigations, inquiries or criminal prosecutions related to national security threats or other offences as per regulation defined under these laws.

The law on electronic communications also protects the confidentiality of text messages and email communications. Generally, only the sender and recipient of a message can intercept, record or disclose its content. Exceptions include cases where both parties have provided written consent for disclosure, or a court order has granted access to correspondence content following specific legal conditions.

**Law stated - 21 May 2024**

## Other laws

### Are there any further laws or regulations that provide specific data protection rules for related areas?

The relevant sectoral laws include, but are not limited to, the following:

- the Law of Armenia on banking secrecy, which aims to protect data collected by banks;
- the RA Law on Medical Assistance and Service to the Population, which aims to protect medical secrets;
- 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 credi t 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; and
- the Law of Armenia on electronic communications, which protects electronic communications service providers' clients' data.

The procedural codes (such as the Civil Procedural Code, Criminal Procedural Code) regulate the processing of personal data within the scope of the relevant processing.

**Law stated - 21 May 2024**

## PI formats

### What categories and types of PI are covered by the law?

As per the definition of the Law, PI is all information relating to a natural person, which allows or may allow for direct or indirect identification of a person's identity.

Further, the Law differentiates between two other categories of PI: biometric PI and special category PI.

Biometric data means any information characterising the physical, physiological and biological characteristics of a person, while special category data encompasses any information relating to race, national identity or ethnic origin, political views, religious or philosophical beliefs, trade union membership, health and the sex life of a person.

**Law stated - 21 May 2024**

## Extraterritoriality

### Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The Law is applicable to data processing in the territory of Armenia and to the processing of data performed by controllers or processors that are established and operating in Armenia.

Armenian law does not require the collection of personal data in a server located in Armenia prior to its transfer abroad (ie, a data subject may transfer its data to an entity abroad directly and the Law will not be applicable to that processing).

**Law stated - 21 May 2024**

### Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The Law guarantees the rights of natural persons (data subjects) and imposes mandatory requirements on personal data controllers, processors and third parties.

According to the Law the data processor (the 'controller' in the meaning of the GDPR) is a state administration or local self-government body, state or community institution or organisation, legal or natural person, which organises or carries out the processing of personal data.

In addition, an authorised person (the 'processor' in the meaning of the GDPR) is considered to be a person who is authorised by a data controller to collect, input, organise or otherwise process personal data in cases prescribed by law or under an agreement.

Both the controller and the processor shall process personal data based on the consent of data subjects. The obligation of the controller is determined under the Law, while the obligation of the processor is subject to regulation under the agreement between the controller and the processor, which, however, shall correspond with the obligations of the controller.

**Law stated - 21 May 2024**

## LEGITIMATE PROCESSING OF PI

### Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The Law of the Republic of Armenia on protection of personal data (the Law) prescribes among the principles of data processing the principle of lawfulness. The processing of data is deemed lawful, where:

- the data has 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 the Armenian legislation (ie, cases in which the legislation allows processing without consent, such as surveillance); or
- the data being processed has been obtained from publicly available sources of personal data. The data subject must still be notified about the processing of his or her publicly available data.

**Law stated - 21 May 2024**

### Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

There are specific rules related to the processing of sensitive data prescribed under the Law. For instance, it is required to notify the Personal Data Protection Agency prior to commencing the processing of biometric or special category PI.

Another example of special rules is that the processing of personal data must cease if and when the grounds and purpose of processing are eliminated.

Employee PI processing is regulated under the Labor code of Armenia. For example, it is stated that the employer may not receive information on the employee's political, religious and other beliefs, public associations, or activity in trade unions. On another note, the employer has the right to receive and process the data of an employee's personal life only with his or her written consent in cases directly related to employment relations.

Medical secrets, as defined under the Armenian Law on Medical Assistance and Service to the Population, stands for 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. Generally, medical secrets must be processed as per the patient's or legal representative's consent. Medical secrets may be processed without consent if the case is one of those listed under a special law, for instance, when the transfer of information is required for the provision of medical care and service to the patient and such provision would be impossible without this data. In any case, such transfer should be carried out according to the procedure established by the government.

Similarly, specifics concerning the processing and disclosure are regulated under the sectorial laws listed above.

**Law stated - 21 May 2024**

## DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

### Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The controller or processor must notify the data subject of its intention to process personal data and with the aim to receive consent for such processing.

Notification of the intention to process personal data must contain the following:

- name and surname, patronymic name 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 and processor requesting the consent of the subject of personal data and the place of location or registration (actual residence);
- information on how to request correction, erasure or cessation of processing of personal data by the data subject; and
- the period of validity of the requested consent, as well as the procedure for withdrawing consent and its consequences.

**Law stated - 21 May 2024**

## Exemptions from transparency obligations

When is notice not required?

The requirement of notification prior to data processing is not applicable if any law specifically allows the processing of personal data without consent or notification. For some cases, the legislation prescribes the additional procedures to be followed instead of notification of processing; for instance, a special court decision may be required in the case of processing of certain data in the scope of criminal proceedings.

**Law stated - 21 May 2024**

## Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

The Law of the Republic of Armenia on protection of personal data (the Law) determines that the data subject to processing must be reliable (ie, data must be complete, accurate, simple and where necessary, kept up to date).

Accordingly, the Law imposes on the data controller the obligation to carry out necessary operations for making PI complete, and keeping up to date, rectifying or deleting incomplete, inaccurate, outdated or unlawfully obtained PI or data that is unnecessary to achieve the processing's purposes. Similarly, the data subject is entitled to request the data controller to rectify, block or erase his or her personal data, where the personal data is not complete or accurate or is outdated or has been obtained unlawfully or is not necessary for achieving the purposes of the processing. In case of such a request the data controller is obliged immediately, but not later than within three working days, to carry out the necessary operations for completing, updating, rectifying, blocking or erasing the data.

**Law stated - 21 May 2024**

## Data minimisation

Does the law restrict the types or volume of PI that may be collected?

The principle of proportionality, defined under the Law, requires that the collector must process the data in the minimum volume necessary to achieve the legitimate purposes of processing.

Further, the Law lists the principle of minimum engagement of subjects,which states that where the state administration or local self-government body, or a notary are able to obtain the PI from another body through a uniform electronic information system, the PI subject shall not be required to submit PI necessary for certain operations.

**Law stated - 21 May 2024**

## Data retention

### Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Depending on the purposes of the processing of the PI, the Law may stipulate the time frame during which the PI needs to be kept. For instance, in cases where a company processes personal data for accounting purposes, the data may not be deleted for at least five years. Also, if processing takes place for anti-money laundering or countering the financing of terrorism purposes, the information needs to be kept for five years A similar obligation to maintain information may be stipulated explicitly or implied under the different legislation acts.

**Law stated - 21 May 2024**

## Purpose limitation

### Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

The principle of proportionality requires that the processing of data pursue the legitimate purpose and the measures to achieve it must be suitable, necessary and moderate. Processing personal data that is not necessary for the purposes of processing or incompatible with it is banned.

Processing of data must be depersonalised if the purpose of processing may be achieved in doing so.

As a matter of practice, the purposes of processing must be defined in the data subject's consent and if processing for new purposes is required which is not compatible with those listed in the consent, the data controller and processor must pursue the issuance of a new consent with the purposes of interest listed in it. Regardless, the purposes shall be legitimate: for instance, the employer cannot request a consent for processing of certain sensitive information about its employees.

**Law stated - 21 May 2024**

### Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The Law does not explicitly address automated decision-making, which may or may not affect people. It is assumed that the general principles and regulations defined under the Law must be applicable to automated decision-making-related issues.

However, because Armenia has ratified Convention 108, including its 2nd protocol, and hence the Convention has become part of the Armenian legislation system, the matter may be considered resolved as per Convention 108.

**Law stated - 21 May 2024**

## SECURITY

### Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Generally, the Law of the Republic of Armenia on protection of personal data (the Law) imposes mandatory technical and organisational security measures requirements on personal data controllers. For instance, it is required that the data controller:

- uses encryption keys; and
- prevents unauthorised access.

The Law defines that a government decree that is not yet adopted will regulate the requirements for ensuring security of processing of personal data.

In addition, the Law states that the use and storage of biometric personal data outside information systems may be carried out only through such tangible media and the application of such technologies or forms, that ensure the protection of data from unauthorised access, unlawful use, destruction, alteration, blocking, copying, dissemination of the personal data, etc. More detailed requirements for tangible media for biometric personal data and technologies for storage of such personal data outside information systems are set forth by the decision of the Government of the Republic of Armenia N 1175-Ա dated 31 October 2015.

In its decision of 17 February 2021, the government approved the digitisation strategy of Armenia (the program of strategic measures and performance indicators) which establishes the necessity of overview of digital business legislation, development of cybersecurity standards (including verification of the applicability of standards and certification of systems) for the protection and security of personal data.

The cybersecurity legislation is now under development. For the time being there are no specific technical and organisational security measures, including international certification (eg, ISO) requirements.

**Law stated - 21 May 2024**

### Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

There are relevant provisions established under Armenian legislation (the Law) that address the obligation of notification in case of data breaches. The Law mandates specific actions by data controllers upon discovering unlawful processing of personal data (excluding data outflow). In particular, the data controller is obliged to immediately, but not later than within three working days, eliminate the violation concerning the processing of the PI. However, if such elimination is impossible the data controller should destroy the data. It should be highlighted that in each described case the data controller has an obligation to notify the data subject (or the Personal Data Protection Agency (PDPA) if the request is received from the PDPA) of the elimination of the violations or the destruction of the PI within three working days.

Additionally, in the event of an outflow of personal data from electronic systems, the controller must immediately publish an announcement about the incident. Simultaneously, the controller must officially report the outflow to the police of the Republic of Armenia (the Ministry of Internal Affairs), as well as the PDPA.

**Law stated - 21 May 2024**

## INTERNAL CONTROLS

### Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

The Law of the Republic of Armenia on protection of personal data does not require the implementation of internal controls. However, to process the personal data of employees an employer must have certain internal controls, as per the requirements of the Labor Code of Armenia. The same is true also for the processing of bank secrecy, insurance secrecy or credit secrecy, when the Central Bank is required to establish a certain internal control environment for the protection of secrecy. A more or less similar approach is in place for a number of sectors where the protection of secrecy is the primary concern.

**Law stated - 21 May 2024**

### Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

Armenian legislation does not require the appointment of a data protection officer.

**Law stated - 21 May 2024**

### Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

As a general rule, no requirement is stated that the collector or processor must keep an internal record of the PI held.

**Law stated - 21 May 2024**

### Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

No risk assessment requirements are provided under Armenian legislation.

**Law stated - 21 May 2024**

### Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

Armenian legislation does not define the requirements for how the PI processing systems must be designed.

**Law stated - 21 May 2024**

## REGISTRATION AND NOTIFICATION

### Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

Even though the Personal Data Protection Agency (PDPA) keeps a register of controllers of personal data, generally, there are no such mandatory registration obligations imposed on data controllers for all PI processing cases. Hence, data controllers are requested to register with the PDPA only in certain specific cases, such as processing of sensitive personal data. Failure to notify the PDPA about the processing of sensitive personal data may cause the imposition of a penalty of up to 100,000 drams.

**Law stated - 21 May 2024**

### Other transparency duties
Are there any other public transparency duties?

No, there are no such duties imposed on data controllers.

**Law stated - 21 May 2024**

## SHARING AND CROSS-BORDER TRANSFERS OF PI

### Sharing of PI with processors and service providers
How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The Law of the Republic of Armenia on protection of personal data (the Law) provides specific provisions dedicated to the regulation of the relations between data controllers and authorised persons (processors). The legal basis for the processor to process personal data is an agreement with the controller, which must be written and must contain the following information:

- legal grounds of the PI processing;
- the conditions for PI processing;
- the purpose of the PI processing;
- a list of the PI subject to processing;
- the scope of data subjects;
- the scope of persons to whom PI may be transferred; and
- the technical and organisational measures for the protection of personal data and other necessary information.

It should be noted that the PI may be processed only within the scope of the assignment, for which the data controller bears full responsibility. Furthermore, if the assignment contradicts the requirements of the Law the authorised person has an obligation to inform the data controller and refuse the processing of PI.

**Law stated - 21 May 2024**

### Restrictions on third-party disclosure
Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

According to the definition given by the Law, a third party is any person, body, institution or organisation other than the data subject, controller of PI or authorised person whose rights or legitimate interests are affected or may be affected due to the processing of PI.

Furthermore, it is specified that the PI is considered to be transferred to the third party in the case of an operation aimed at transferring PI to a certain scope of persons or the public at

large or at familiarising them with the PI, including by disclosure through the mass media, posting in information communication networks or otherwise making PI available to another person.

The general rule for such a transfer to be valid is the consent of the data subject. Cases in which the data may be transferred to third parties without consent are defined under the specific regulations.

There is a specific rule, for instance, for the transfer of sensitive data to third parties. This data may be transferred when:

- the data controller is considered as a controller of special category personal data prescribed by law or an interstate agreement, the transfer of such information is directly according to Armenian legislation or ratified international agreements, and has an adequate level of protection; and
- in exceptional cases provided for by Armenian legislation, special category personal data may be transferred to protect the life, health or freedom of the data subject (eg, transfer of medical secrets in exceptional cases provided for by the Armenian law on medical assistance and service to the population).

**Law stated - 21 May 2024**

## Cross-border transfer

### Is the transfer of PI outside the jurisdiction restricted?

Personal data may be transferred to another if there is:

- consent of the data subject: the data subject has provided explicit and informed consent to the transfer; or
- necessity for processing: the transfer stems from the purposes of processing personal data or is necessary for the implementation of these purposes.

The transfer may be exercised with or without the permission of the Personal Data Protection Agency (PDPA), depending on which country the transfer is aimed at.

Authorisation for the transfer is not required if the receiving country offers an adequate level of PI protection. Adequacy can be established through two means:

- the transfer complies with the terms of relevant international agreements on data protection; or
- the receiving country is included in an official list published by the Agency, signifying that it provides a sufficient level of protection.

Authorisation for transfers to countries with no adequate level of data protection is possible:

- with the prior permission of the PDPA;
- if the PI is transferred on the basis of an agreement; and
-

the agreement provides for such safeguards with regard to the protection of PI that have been approved by the PDPA as ensuring adequate protection.

As for the procedural formalities, the data processor must submit a written application to the PDPA outlining the transfer details established by the Law and seeking permission. Within 30 days the PDPA may permit or reject the application or set the additional security measures to be provided to authorise the transfer.

**Law stated - 21 May 2024**

### Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The general rules regarding the transfer of the PI outside the jurisdiction specified in the Law apply also to transfers to service providers and onwards transfers in the case that such transfer is conducted outside the jurisdiction of Armenia.

**Law stated - 21 May 2024**

### Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There are no such requirements applicable to PI in the Armenian jurisdiction.

**Law stated - 21 May 2024**

## RIGHTS OF INDIVIDUALS

### Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

A data subject has the right to access its personal data, which means that the data subject is entitled to receive the information regarding the processing of its PI, grounds and purposes of such processing, ways of processing, the controller of the PI (its address) and the maximum term of the processing, as well as the scope of persons to whom PI may be transferred. Such information should be provided in an accessible format.

The mentioned right may be exercised by way of the submission of a written request to the data processor.

The data controller must provide access to the information within five days of receipt of the request. Access may be rejected; however, it must be fully justified. The said rejection may be appealed to the Personal Data Protection Agency (PDPA), and the latter may force the controller or processor to provide access to the data.

**Law stated - 21 May 2024**

## Other rights

### Do individuals have other substantive rights?

The data subject is entitled to require the processor to rectify, block (temporarily) or destroy (erase) their personal data, where the personal data:

- is not complete;
- is not accurate;
- is outdated;
- has been obtained unlawfully; or
- is not necessary to achieve the purposes of the processing.

The Law of the Republic of Armenia on protection of personal data (the Law) does not provide any regulations regarding cases where the obligation of the processor or controller to erase the data at the request of the data subject does not apply.

If the data subject has doubts about the rectification, blocking or destruction of their personal data by the collector, the Law entitles the data subject to apply to the PDPA to make clear the fact of his or her personal data being rectified, blocked or destroyed and to be provided with that information.

The data subject has the right to appeal the decisions, actions or inaction of the collector before the PDPA or through judicial procedure if the data subject considers that the processing of their personal data is carried out in violation of the requirements of the Law or otherwise violates their rights and freedoms.

The data subject is entitled to object to the processing or to withdraw their consent. The Law establishes that the data subject shall have the right to withdraw their consent if there is established legislative ground for it. The Law also states that the controller shall be obliged to terminate the processing of personal data and destroy the data within 10 working days following receipt of the withdrawal, unless otherwise provided for by mutual consent of the data subject and the controller or by law.

Even though the specific legitimate grounds and purposes of the restrictions of the right to object to processing are not explicitly mentioned by law, it is clear that this right is not absolute and is subject to restrictions depending on various scenarios (eg, public security reasons).

**Law stated - 21 May 2024**

### Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

In case of a breach of the Law, the data subject is entitled to compensation for damages. Damages include actual damage, that is to say, the expenses incurred by the data subject that have been or must be covered by them to restore the violated right and the loss of or harm to the property thereof. In addition, it also includes lost benefit: the income that the data subject would have received under the usual conditions of civil practices had the right thereof not been violated.

Intangible damages or damages caused to the feelings of the data subject are subject to compensation only where the criminal prosecution body or court has confirmed that the fundamental rights of the data subject guaranteed by the Constitution of the RA and the Convention for the Protection of Human Rights and Fundamental Freedoms have been violated as a result of a decision, action or omission of a state or local self-government body or official.

**Law stated - 21 May 2024**

### Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The data subject is entitled to challenge the action or inaction of the data controller or its decisions before the PDPA or through judicial procedure.

**Law stated - 21 May 2024**

## EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

### Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

In addition to the already described provisions, the Law of the Republic of Armenia on protection of personal data (the Law) also establishes that the publication of personal data by the foundation established on the basis of the Law of the RA 'On Compensation for damage caused to the life or health of military personnel in the protection of the RA' is not considered to be publication of the PI under the regulations of the Law.

**Law stated - 21 May 2024**

## SPECIFIC DATA PROCESSING

### Cookies and similar technology

### Are there any rules on the use of 'cookies' or equivalent technology?

There are no specific rules applicable to cookies or equivalent technology specified by Armenian laws.

**Law stated - 21 May 2024**

## Electronic communications marketing

### Are there any rules on marketing by email, fax, telephone or other electronic channels?

There are no such specific rules established by Law of the Republic of Armenia on protection of personal data (the Law). However, the Personal Data Protection Agency (PDPA) has published an advisory decision on the use of personal phone numbers for advertising p urposes, where it has highlighted 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. In particular, it is stated that the minimum following requirements should be complied with:

- processing of PI, including phone numbers, with the informed consent of the data subject according to the predetermined and legitimate purpose, must be limited to what is necessary and proportionate to achieve that purpose;
- implementation of the appropriate organisational and technical measures (including software tools) to safeguard personal data from accidental or unlawful destruction, alteration, unauthorised access, disclosure or other misuse;
- ensuring the right to opt in (provide prior consent) or opt out (withdraw consent) at any time;
- providing the data subject with information on the processed personal data, as well as information about the source, purposes and legal grounds for collecting personal data, and the terms of use, as well as information about the organisation carrying out direct marketing;
- taking necessary and reasonable organisational and technical measures to prevent the unauthorised use of data subjects' personal data by third parties for direct marketing purposes; and
- provision of the contractual regulations governing the use of PI for direct marketing purposes in the contract concluded between the data subject and electronic communication providers.

**Law stated - 21 May 2024**

## Targeted advertising

### Are there any rules on targeted online advertising?

Armenian legislation does not provide any rules on targeted online advertising. Nevertheless, online behavioural advertising should be conducted strictly following the principles of the PI processing established by the Law in respect of the consent of the data subject and being

guided by the PI processing purpose limitation clause. In addition, the rules set forth by the PDPA advisory decision on the use of personal phone numbers for advertising purposes, 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 should be respected.

**Law stated - 21 May 2024**

### Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

There are no other rules on the processing of sensitive categories of personal information in addition to those described as 'special category' and 'biometric' personal data or referred to as 'sensitive' data.

**Law stated - 21 May 2024**

### Profiling

Are there any rules regarding individual profiling?

There are no specific regulations provided at the Armenian national legislation level, but this is addressed in the scope of Convention 108, which is part of the legislation system of Armenia.

**Law stated - 21 May 2024**

### Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

There are no rules or regulatory guidance on the use of cloud services, which at the same time means that such use is not prohibited and should be conducted following the general principles set forth by the Law.

**Law stated - 21 May 2024**

## UPDATE AND TRENDS

### Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The Personal Data Protection Agency has been active during 2023. In particular, it has translated into Armenian law two key guidelines published by the EDPB: Guidelines 05/2022

on the use of facial recognition technology in the area of law enforcement, and Guidelines 01/2022 on data subject rights – Right of access.

In addition, currently there is draft legislation of the Law of Armenia on Cybersecurity. This law aims to establish a secure cyber environment for information systems and critical information infrastructures that support vital services within Armenia.

In conjunction with the Law of the Republic of Armenia on protection of personal data's passage, amendments to existing Armenian data protection laws are also proposed. These amendments aim to ensure consistency between the new cybersecurity framework and existing data protection regulations.

One of the proposed amendments in the draft Law on Cybersecurity concerns the establishment of cybersecurity standards. This amendment would likely introduce two key elements:

- compliance with ISO Certification Standards; and
- government-defined minimum requirements.

**Law stated - 21 May 2024**