Market
Intelligence

PRIVACY & CYBERSECURITY 2022

Armenia

LEXOLOGY
Getting the Deal Through

Armenia

Narine Beglaryan is an attorney who joined the Concern-Dialog law firm in September 2013 as senior associate. Since 2016, she has been a partner of the firm.

Narine specialises in banking law, corporate law (she heads the corporate law and banking law and compliance areas of practice of the firm), contract law and in-court representation of her clients' interests in administrative and civil cases. At present, she specialises in the sphere of anti-money laundering and combating the financing of terrorism and data protection.

In the sphere of law, she started her practical activity in 2007. Prior to joining our team, Narine had worked with Armentel CJSC (now Team Telecom Armenia) as a legal adviser at the Department of Legal Support to the Business. For many years, she had been employed at the legal office of BTA Bank CJSC in the position of chief lawyer of the Legal Office.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

By decision No 183-L of 11 February 2021, the Armenian government approved the Digitalisation Strategy of Armenia, as well as the Action Plan of the Digitalisation Strategy of Armenia and its performance indicators.

The Strategy was developed by the Ministry of HighTech Industry of the Republic of Armenia, which is the main department responsible for the implementation of the strategy.

As the main objective, the Strategy envisages the digital transformation (digitalisation) of the government, economy and society of Armenia. Among the means to achieve this goal, the introduction and development of a cybersecurity system in the country was highlighted.

As a first step in the implementation of the cybersecurity system, it is envisaged that the Ministry of HighTech Industry will develop a comprehensive overall cybersecurity policy and action plan. At the moment, such a document is not available on public discussion platforms (for example, on the e-draft.am website) and the platforms of normative legal acts that have entered into force (for example, arlis.am).

The same strategy provided for the establishment of a Cybersecurity Centre of Excellence, which should develop cybersecurity standards (it is proposed to take the experience of the US, the UK and Israel as a basis and localise international cybersecurity standards).

The Action Plan of the Strategy provides that the Cybersecurity Centre of Excellence, after the start of its activities, will check the compliance of state platforms with the developed standards, periodically conduct review of cybersecurity standards and approve standards, check the application of standards, and certify systems, provide expert advice, monitor the level/condition of cybersecurity, develop guidelines for cybersecurity literacy enhancement and knowledge development and provide incubation programmes, conduct artificial intelligence research projects, support and promote start-ups in the field of cybersecurity. According to the information currently available, the Cybersecurity Centre of Excellence has not been established yet.

The government has also determined the classification of the risks associated with cybersecurity, the development of an additional cybersecurity enhancement plan and relevant scenarios in order to strengthen cybersecurity in the event of emergencies, war, the establishment of exercises related to certain incidents and measures and principles aimed at coordinated accident management (at the moment these are also not adopted).


Narine Beglaryan

It is important to note that for the effective implementation of programmes related to cybersecurity, the need for the formation and development of cybersecurity literacy is highlighted, and the implementation of measures and programmes in this direction is envisaged.

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

The regulation of unlawful operations performed upon personal data in Armenian normative legal Acts may be found exclusively in the main Act regulating the sphere, which is the Armenian Law on Personal Data Protection.

The obligation to take measures against unlawful operations performed upon personal data is provided by the Armenian Law on Personal Data Protection exclusively for the controller.

When unlawful operations performed upon personal data are revealed that at the same time do not qualify as outflow of personal data from electronic systems,

the controller shall be obliged to eliminate the committed violations. If the controller cannot eliminate the violations committed within three working days, or it is initially obvious that it is impossible to eliminate the violations, the controller shall be obliged to immediately destroy the personal data. When the controller eliminates the violation or destroys personal data, the controller shall inform the data subject or his or her representative about it. If a violation was discovered based on a request from the Agency for Protection of Personal Data of Armenia, the controller must also notify the Agency for Protection of Personal Data of Armenia. Notification to both the data subject (representative) and the Agency for Protection of Personal Data of Armenia shall be sent within the three working days after the elimination of the violation or destruction of personal data.

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 the Police of the Republic of Armenia, as well as the Agency for Protection of Personal Data of Armenia.

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

The requirements for security measures during the processing of personal data are set out in the Armenian Law on Personal Data Protection. The Armenian Law on Personal Data Protection requires the controller to use encryption keys. This security measure should protect personal data, particularly: the protection of information systems containing personal data against accidental loss, unauthorised access to information systems, unlawful use, recording, destroying, altering, blocking, copying, disseminating personal data and other interference.

The list of security measures also includes the controller's obligation to prevent persons without the right from processing personal data. The controller should also restrict access and use of technologies and data to permitted purposes and lawful use.

In the context of security, in the case of data transfer to the processor by the controller, the agreement with the processor must specify technical and organisational measures for the protection of personal data that the processor will be obliged to comply with when processing personal data transmitted by the controller.

With the exception of certain industry organisations (specifics are discussed in the following question 6), there is no requirement for controllers or processors to obtain a certificate of compliance with the requirements of international standards and the requirements of relevant standards applied in the field of information security.

> "Liability is currently applied to a natural person who, in the event of an administrative offence, is the director of a legal person considered as a processor or controller of personal data."

In Armenia, the legal consequences of violations of personal data processing security requirements arise in the form of administrative or criminal sanctions. In both cases, liability is currently applied to a natural person who, in the event of an administrative offence, is the director of a legal person considered as a processor or controller of personal data, and in the event of a crime – the persons who committed the crime.

Administrative responsibility for security arises for non-use of encryption keys, and the fine is about US$200. Another security- related administrative offence is the violation of the requirements for ensuring the security of personal data processing in information systems, where the fine amounts to between US$200 and US$400. These violations are considered an administrative violation if they do not constitute a crime.

Personal data subjects cannot claim moral (intangible) damages for violations committed by controllers or processors when processing their data, but they must be able to prove material damage (actual damage or lost benefit, or both), which is rather complicated as regards to the feasibility of proving it.

In general, considering the security requirements and the consequences of their violation, it turns out that for violations of the security requirements for processing personal data, the risk to the controller and processor is not directly financial, but rather reputational, such as possible business losses after gaining a reputation for not ensuring the security for processing of personal data.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

In Armenia, the most regulated sphere in terms of information security is the financial and banking sphere. Here, since 2014 in accordance with the procedure on establishing minimum requirements for ensuring information security approved by the Board of Central Bank of the Republic of Armenia, priorities, and compliance requirements for information security of financial and banking organisations have been determined.

The information security management system for banks operating in the territory of Armenia – regulatory market operator, central depository, credit bureaus,

Photo: shutterstock.com/Leonid Andronov

leveraged transactions, including persons providing investment and non-core services related to Forex transactions and crowdfunding platform operators, as well as insurance companies and payment and settlement organisations – has been brought into compliance with the requirements of international standards applied in the field of information security. At the same time, regardless of compliance, these organisations are obliged to ensure continuous satisfaction of the requirements established by the procedure on establishing minimum requirements for ensuring information security, approved by the board of Central Bank. As a result of these measures, the financial and banking organisations listed here are mostly protected.

As mentioned in question 5, the main rules of the security of personal data are mostly generic and at the same time, organisations are not required to comply with international standards and confirm this compliance with a certificate. This leads to the fact that a significant part of organisations (especially small and medium-sized businesses) do not take technical security measures or do not take sufficient measures.

It is also important to note that the requirements of the security of personal data processing imposed by an organisation by its internal acts differ depending on the composition of the company's participants: that is, organisations with foreign investments (mainly European countries and the US) have technical security measures and requirements adopted, unlike other organisations. Information security measures are highlighted in certain industry companies (electronic communication service providers).

5 Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

The use of the original cloud technologies in the processing of personal data is not prohibited as such; therefore, it can be carried out in compliance with the general rules.

However, during the transfer or transmission of personal data to the cloud hosting environment, several issues requiring solving have arisen before the organisations.

First, when transferring personal data to the cloud hosting environment, the organisation should find out whether personal data is transferred to a third party and whether personal data is transferred to another country or not.

As a rule, the transfer of personal data to the cloud hosting environment is a transfer to a third party, unless, of course, the organisation uses its own servers. Here, the organisation must make sure that the consent of the personal data subject has been obtained for the transfer of data to a third party.

Also, as a rule, the transfer of personal data to the cloud hosting environment involves the transfer of personal data to the territory of another country, since usually the servers are physically located in the territory of another country outside of Armenia. The approach is that if the server, technologies or data processing centres are physically located outside Armenia, the organisation transfers personal data to another country. The organisation must make sure before transferring personal data that it has received the consent of the personal data subject and must check.

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

The Investigative Committee has a Department of Investigation of Cybercrime and High Technology Crime. This department of a law enforcement body is authorised to investigate of crimes against the security of computer information.

The Criminal Code of Armenia in force defines seven main crimes against computer information security (articles 251–257). These are: (i) access (penetration) into computer information systems without permission; {ii) change in computer information; (iii) computer sabotage; (iv) illegal appropriation of computer data; (v) manufacture or sale of special devices for illegal penetration into a computer system or network; (vi) manufacture, use and dissemination of hazardous software; and (vii) breach of rules for operation of a computer system or network.

The new Criminal Code of Armenia will enter into force on 1 July 2022. Again, seven crimes against the security of a computer system and computer data have been established (articles 359–365): (i) penetration into a computer, computer system or computer network; (ii) change in computer data; (iii) computer sabotage (smuggling); (iv) illegal seizure of computer data or their appropriation; (v) illegal circulation of special software or tools; (vi) fraud; and (vii) violation of the rules or requirements for the operation of a computer, computer system or network. One of the main changes is that the list of technologies, solutions and tools with which or by which computer crimes can be committed has been expanded and clarified to some extent.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

In most transactions, clients do not require due diligence prior to M&A deals or in M&A deal negotiations and the conclusion of transactions and do not plan to check issues related to personal data protection.

"The main rules of the security of personal data are mostly generic and at the same time, organisations are not required to comply with international standards and confirm this compliance with a certificate."

When considering personal data and their security issues for M&A deals themselves, the compliance with the Law on Personal Data Protection should be verified. It is necessary to pay attention to the actual situation of data processing by the organisation, including the consent of the subjects of personal data, the purpose of processing, the scope of data transmission and the provision of access to data. Then, it is necessary to compare the factual situation with the provisions of the law and to find out the inconsistencies. The main risks concern the legality of processing and proportionality; thus there may be incomplete consents or non-purpose uses.
We believe that during M&A deals it is important to pay attention to, and to exclude, the sale of personal data during the transaction. Personal data is not an asset of a company. If as a result of the acquisition of a company or company's assets the circle of persons with access to the data will be changed, ensure that the consent of the personal data subjects is obtained

Narine Beglaryan
narine.beglaryan@dialog.am

Concern Dialog CJSC
Yerevan
www.dialog.am

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

It is necessary to choose a lawyer with an understanding of the specifics of information technology. It is important that a lawyer can fully visualise and understand business process in order to be able to offer practical solutions or assess practical risks. At the same time, as a personal data lawyer, it is preferable to have at least a general knowledge of other countries' approaches and acts in the field of personal data protection.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

Advising on cybersecurity and privacy is sometimes complex due to the lack of regulation. The privacy regulations are in place; however, most concepts were adopted in 2015, and since then no major changes took place. Regulation is generic, for example, in comparison with the GDPR rules; on the one hand this is positive thing because it allows the avoiding of bureaucracy and more flexibility, but on the other it sometimes leads to an absence or lack in data security, which may cause leakage.

How is the privacy landscape changing in your jurisdiction?

After the adoption in 2015 of the Law on Personal Data Protection and the creation of the Agency for the Protection of Personal Data, special attention is paid to the issue of personal data protection in the country. Cybersecurity issues became more relevant and problematic because of the hacking by Azerbaijan during the 44-day Artsakh War in 2020.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

The dangers of cybersecurity incidents in Armenia are similar to the dangers in other countries. In general, organisations should be able to implement information security systems, which will include both the use of technological means and the availability of internal procedures. As with any system, human resource management requires efficiency.