Cybersecurity Regulation and Its Impact on Business Processes

On December 4, 2025, the National Assembly, upon second reading, adopted the new Laws of the Republic of Armenia "On Cybersecurity"[1] and "On the Regulation of Information Systems"[2] , as well as a number of other normative legal acts aimed at regulating cybersecurity.

The purpose of this material is to generally outline the impact of the creation of a legal regulatory framework for cybersecurity on business processes and to briefly present the expected developments and required actions. Particular attention will be paid primarily to the regulations set forth in the Law of the Republic of Armenia "On Cybersecurity."

Entry into force: The Law of the Republic of Armenia "On the Regulation of Information Systems" entered into force on December 26, 2025, while the Law of the Republic of Armenia "On Cybersecurity" (hereinafter referred to as the Law) entered into force on January 4, 2026. [3]

The Law stipulates that the provisions defining the obligations of economic operators shall enter into force with respect to those obligations only after the entry into force of subordinate normative legal acts establishing detailed requirements concerning such obligations. However, the rule set forth in Article 27 of the Law of the Republic of Armenia "On Normative Legal Acts," must be highlighted which specifically states, that where the implementation of a norm is conditional upon the adoption of another normative legal act, such norm shall not apply until the said other normative legal act enters into force.

Scope of application of the Law: If you intend to understand whether the requirements of the Law apply or will apply to your business, the following questions must be considered:

Question 1. Is your business a service provider operating in a critical sector or not?

Although the list of critical sectors is approved by the Law (see List 1), at this stage the identification process cannot yet be carried out, as the Government still needs to define the types of services /classifiers/ corresponding to the types of services provided within critical sectors.
If you are a legal entity or an individual entrepreneur that meets the criteria for classification as a micro or small business entity as provided under the Law "On State Support of Small and Medium Entrepreneurship," the Law does not apply to you, except in cases where you operate critical information infrastructure.

Question 2. Do you operate an information system?

When the Law uses the term "information system," it understands that this refers to, in critical sectors, an operated:

- electronic communications network,
- any device or a group of interlinked or adjacent (connectable) devices, or
- an aggregate of technical and software-and-hardware tools,

and it is specified that one or several of the above, taken together, must perform automated processing of digital data,

- or it refers to digital data that are stored, processed, acquired, or transmitted by the above-listed means, for the purposes of their use, protection, and maintenance.

1 The Law is available at the following link: https://www.arlis.am/hy/acts/218672/latest
2 The Law is available at the following link: https://www.arlis.am/hy/acts/218686
3 The entry-into-force dates of the remaining laws aimed at regulating cybersecurity generally coincide with the date on which the Law enters into force.

It is important to remember that the mere operation of an information system, in and of itself, does not, within the meaning of the Law, lead to qualification as a service provider; however, it grants the regulatory authority in the field of cybersecurity (referred to in the Law as the "Autonomous Body") the right to review the information system, by qualifying it as meeting the identification criteria for critical information infrastructure operated in a critical sector, and to temporarily recognize it as critical information infrastructure within a critical sector. **That is, the operator of an information system may be temporarily recognized, within the meaning of the Law, as a service provider.**

Question 3. Do you operate critical information infrastructure?

Again, it is important to understand the substance of the term. The Law recognizes as **critical information infrastructure**, within critical sectors, the following that are operated:

- automated control systems,
- information systems,
- equipment or a part thereof,

provided that the disruption or destruction of the above must create threats to national security, defense, the economy, social welfare, public health, the environment, public order, international relations, and continuity of governance (governance continuity), for the infrastructure to be qualified as critical.

It is important to remember that the definition alone, in and of itself, will not serve as a basis for determining the conditions for qualifying infrastructure as critical.

It has been established that **identification criteria** for critical information infrastructure operated in a critical sector will be developed and approved by the Government, on the basis of which the infrastructure will be qualified, or not qualified, as critical.

It is extremely important to note that the Law provides that the Government will also approve a **list of critical information infrastructure** for the purpose of carrying out state governance and regulation in the field of cybersecurity. And, in turn, the National Security Service will have the competence, in relation to the information systems and critical information infrastructure approved in the list established by the Government, to exercise the powers and functions authorized by the Law and reserved to the Autonomous Body.

Qualification as a **service provider** will result in the emergence of new obligations for your business. The obligations are listed below in general terms:

► adoption of internal acts,
► implementation of organizational and technical measures aimed at continuously identifying and managing cyber threats, preventing, detecting, stopping, and resolving cyber incidents, as well as ensuring the uninterrupted operation of information systems and critical information infrastructure,
► conducting risk assessments and managing such risks,
► notification of the Autonomous Body of cyber incidents and compliance with the requirements of the Law related to cyber incidents, including following the instructions of the Autonomous Body and granting the Autonomous Body access to systems,
► appointment of a cybersecurity specialist or delegation of the function to a cybersecurity service provider company that complies with the requirements of the Law,
► mandatory cybersecurity audit at a three-year interval,
► granting the Autonomous Body access to information systems for the purpose of conducting conformity assessments.

Liability is established for the following acts (presented in general terms and not literally corresponding to Article 193.4 of the Code of Administrative Offenses) and in the following amounts:

► Violations of security requirements (failure to ensure minimum cybersecurity

requirements, failure to comply with or improper compliance with criteria and requirements established by international or national standards in the field of cybersecurity, or absence of a document certifying compliance): a fine of AMD 7,000,000 – 10,000,000

► Violations of requirements related to the adoption of internal acts and internal business processes (absence of internal cybersecurity regulations, failure to conduct risk assessment (or develop a risk assessment scale), failure to determine the severity/scale of the potential consequences of a cyber incident or to approve a preventive action plan, failure to appoint a cybersecurity specialist, violation of requirements for delegating the functions of a cybersecurity specialist): a fine of AMD 200,000 – 300,000

► Violation of the requirement to notify of a cyber incident and violation of other obligations related to a cyber incident: a fine of AMD 500,000 – 700,000, except for violation of the obligation to notify affected persons, for which a fine is established in the amount of AMD 200,000 – 300,000

► Failure to undergo a cybersecurity audit: a fine of AMD 200,000 – 300,000

► Violation of the requirement to submit the cybersecurity audit conclusion: a fine of AMD 100,000 – 200,000

► Violation of established deadlines for providing documents and information upon the request of the Autonomous Body: a fine of AMD 200,000 – 300,000.

List 1

Critical Sectors

1. the energy sector.
2. the manufacturing sector (manufacturing of chemical, food, weapons and ammunition, medical, electrical, computer, electronic and optical devices).
3. the transport sector.
4. the water supply and wastewater disposal sector.
5. the communications sector, including telecommunications.
6. the postal services sector.
7. the financial services sector.
8. the healthcare sector.
9. the information technology sector, including digital infrastructure.
10. the radioactive materials, subsoil use, and hazardous waste management sector.
11. the space activities sector.
12. the database management and operation sector.
13. the security provision in emergency situations sector.
14. the public administration sector, including digital infrastructure operated by state bodies.

About Authors

Narine Beglaryan

Senior Partner, Attorney

Narine Beglaryan leads the firm's corporate law and M&A area of practice, as well as banking law and capital markets, data protection and privacy practices. Her role encompasses providing expert legal advice and litigating on behalf of clients. Narine Beglaryan has been a licensed attorney since 2012. Joined the Concern Dialog team in 2013. With over 15 years of experience, her expertise is recognised internationally, as evidenced by her inclusion in the main ranking lists such as the prestigious Chambers Global, Chambers Europe, and IFLR1000, as well as being featured in the Legal500 ranking of leading individuals. Prior to joining the Concern Dialog team, she worked for seven years in a bank and in the telecommunication sector (in-house counsel).

About Concern Dialog

Concern Dialog is a top-tier, full-service law firm, headquartered in Yerevan, Armenia. It has been a trusted partner for businesses and individuals seeking legal counsel and representation since 1998. The firm is renowned for its work in the areas of corporate law, labour law, competition law, tax law, contract law, family law (including child abduction cases), and regulatory issues. Concern Dialog has extensive experience in regulatory matters in TMT, mining, energy, utilities, banking and finance, medical services, real estate, and notfor-profit sectors. In addition to its renowned consulting and transaction practice, the firm's litigation practice is regarded as one of the leaders in Armenia for landmark litigation and arbitration cases. Concern Dialog's membership of TagLaw and Nextlaw networks, as well as its co-operation with individual law firms from various jurisdictions, allow the firm to provide services to its Armenian clients virtually worldwide.