

International Comparative Legal Guides

Technology Sourcing 2026

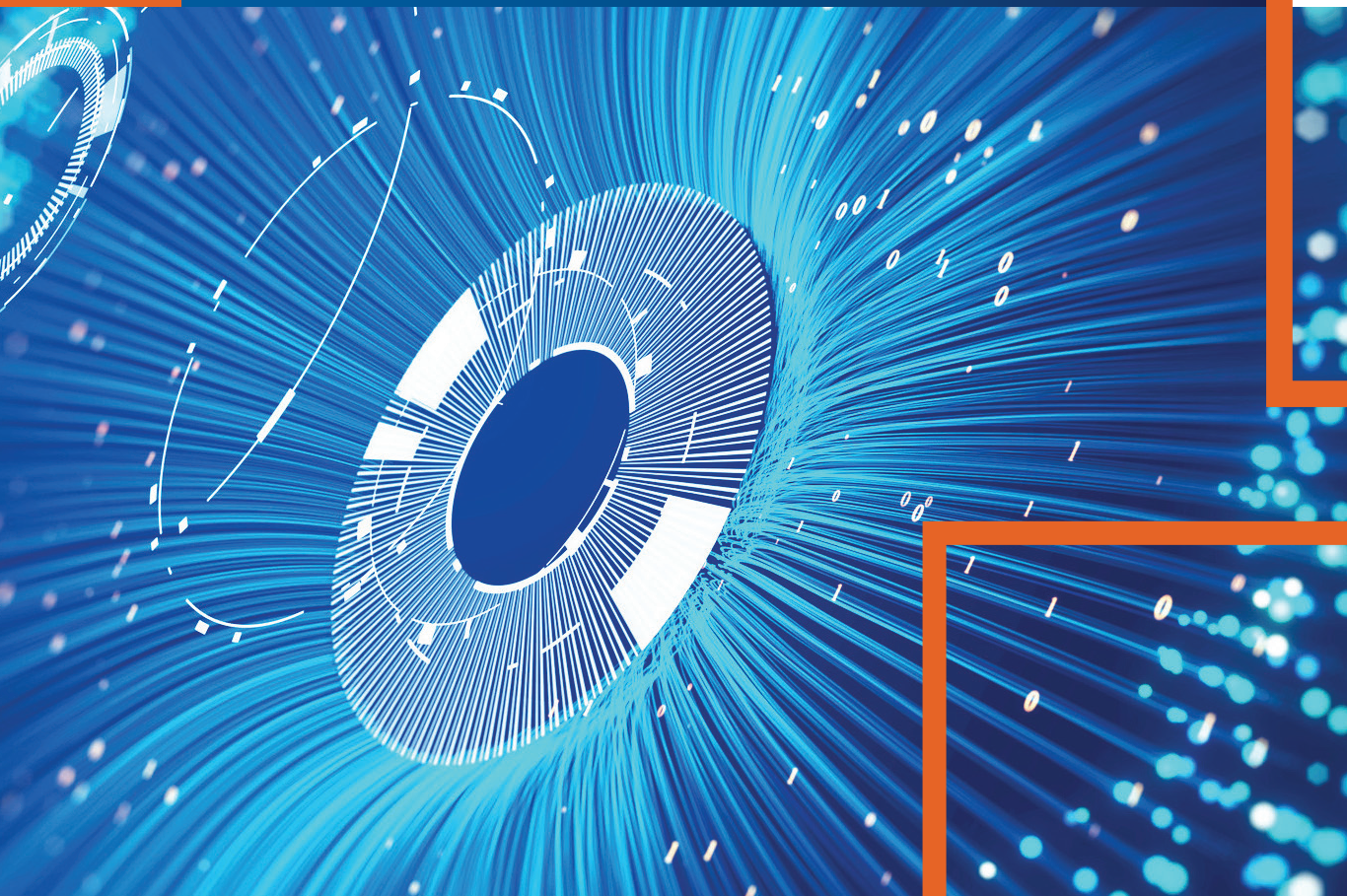
A practical cross-border resource to inform legal minds

Sixth Edition

Contributing Editors:

Will Bryson & Ben Woodfield

Bird & Bird LLP



iclg

Expert Analysis Chapters

1

Sourcing AI Solutions

Will Bryson & Ben Woodfield, Bird & Bird LLP

10

The Future of Strategic Sourcing: AI, Agility and the New Commercial Model

Kerry Hallard, Global Sourcing Association

Q&A Chapters

14

Armenia

Narine Beglaryan, Artur Hovhannisyan,
Shushan Stepanyan & Yevgenya Nikoghosyan,
Concern Dialog Law Firm

22

Australia

Kate Morton & Gianluca Pecora, Bird & Bird

32

Austria

Wolfgang Freund, Grama Schwaighofer Vondrak
Rechtsanwälte GmbH

40

Cyprus

Zena Spanou & Angelica Achilleos,
Markos P. Spanos & Co LLC

49

France

Stéphane Leriche, Bird & Bird

60

Germany

Dr Henriette Picot, Michaela von Voß,
Dr Rolf Schmich & Vincent Kirsch, Bird & Bird LLP

71

Hong Kong

Wilfred Ng, Hwee Yong Neo, Jennifer Lau &
Rachel Tang, Bird & Bird

85

India

Harsh Kumar, Indraneel Chakraborty &
Vanshika Tandon, Kaizen Law

96

Japan

Aya Saito & Fumiko Masuda, Bird & Bird

104

Malaysia

Lo Khai Yi, Ong Johnson & Aida Suhailah
Halim Hong & Quek

112

Nigeria

Josephine Tite-Onnoghen, Ishaq Apalando &
Emmanuel Matuluko, Ikeyi Shittu & Co.

121

Philippines

Kerwin K. Tan, Veronica S. Balbin,
Jose Maria B. Buenagua, Tan Hassani and Counsels

130

Saudi Arabia

Peter Koh, Charlie Christie, Nikita Manro &
Reem Abu Alsaud, Bird & Bird

142

Singapore

Jeremy Tan & Chester Lim, Bird & Bird ATMD LLP

150

South Africa

Tayyibah Suliman, Izabella Gutlar-Balkovic, Sadia Rizvi
& Taryn York, Cliffe Dekker Hofmeyr Incorporated

160

Switzerland

Martina Arioli, Arioli Law

169

Taiwan

Bo-Sen Von, Tsung-Yuan Shen, Rachel Chen &
Effie Peng, Lee and Li, Attorneys-at-Law

178

United Kingdom

Will Bryson & Ben Woodfield, Bird & Bird LLP

194

USA

Sonia Baldia, Kilpatrick Townsend & Stockton LLP

Armenia

Concern Dialog Law Firm



**Narine
Beglaryan**



**Artur
Hovhannisyan**



**Shushan
Stepanyan**



**Yevgenya
Nikoghosyan**

1 Procurement Processes

1.1 Is the private sector procurement of technology products and services regulated? If so, what are the basic features of the applicable regulatory regime?

In Armenia, private sector procurement of technology products and services is generally not subject to a dedicated public-procurement-style regulatory regime. Unlike government procurement, private companies are largely free to choose their suppliers and negotiate contract terms. However, technology procurement is still affected by general commercial, competition, data protection, intellectual property, telecommunications, cybersecurity, and consumer protection laws.

1.2 Is the procurement of technology products and services by government or public sector bodies regulated? If so, what are the basic features of the applicable regulatory regime?

Yes. In Armenia, the procurement of technology products and services by government and other public sector bodies is regulated under the general public procurement framework. There is no separate procurement regime exclusively for information technology (IT) or technology-related procurements; instead, technology procurements are subject to the same rules that apply to other public contracts, with certain sector-specific technical requirements where relevant.

The principal legislation governing public procurement is:

- the Law of the Republic of Armenia on Procurement;
- the Civil Code of the Republic of Armenia (for contractual matters);
- government decrees implementing the Procurement Law, including rules on procurement procedures, electronic procurement, and standard documentation; and
- other sector-specific legislation where applicable (e.g., cybersecurity, personal data protection, telecommunications or state secrets, Law on Public information, etc.).

2 General Contracting Issues Applicable to the Procurement of Technology-Related Solutions and Services

2.1 Does national law impose any minimum or maximum term for a contract for the supply of technology-related solutions and services?

No. Under Armenian law, there is generally no statutory

minimum or maximum term for contracts relating to the supply of technology products, software solutions, IT services, cloud services, maintenance, outsourcing, or other technology-related solutions.

The duration of such contracts is primarily determined by the agreement of the parties, subject to general contractual principles established under Armenian civil law.

2.2 Does national law regulate the length of the notice period that is required to terminate a contract for the supply of technology-related services?

No. Under Armenian law, there is generally no specific statutory notice period applicable to the termination of contracts for the supply of technology-related services (such as software development, IT support, cloud services, system maintenance, outsourcing, or similar arrangements).

2.3 Is there any overriding legal requirement under national law for a customer and/or supplier of technology-related solutions or services to act fairly according to some general test of fairness or good faith?

Yes, The Civil Code of the Republic of Armenia recognises the principle that participants in civil-law relationships must exercise their rights and perform their obligations in good faith. Parties may not abuse their rights or act in a manner that contradicts the purpose of the law or the principles of fair dealing.

2.4 What remedies are available to a customer under general law if the supplier breaches the contract?

Under Armenian law, if a supplier breaches a contract for the provision of technology-related solutions or services, the customer may generally rely on the remedies available under the Civil Code of the Republic of Armenia and the terms of the contract. There are no technology-specific remedies; rather, the available remedies are based on general contractual liability principles.

The main remedies available to a customer include:

- Claim for performance of contractual obligations (specific performance).
- Repair, correction, or remediation of defects.
- Compensation for losses caused by the supplier's breach.
- Contractual penalties or liquidated damages.
- Price reduction.

- Suspension of performance (for example: suspension of the payment obligations).
- Termination of the contract.

2.5 What additional remedies or protections for a customer are typically included in a contract for the provision of technology-related solutions or services?

Parties are largely free to choose various additional remedies in the contract for the provision of technology-related solutions or services, such as transition assistance, return or deletion of customer data, transfer of documentation, delivery of source codes, support during migration to another provider, etc.

2.6 How can a party terminate a contract without giving rise to a claim for damages from the other party to the contract?

Under a contract for the provision of services for consideration, both the customer and the service provider are entitled to withdraw from the performance of the contract at any time, provided that they compensate the other party accordingly. The other option is to terminate the contract on the grounds of a material breach. The obligation may be terminated if performance of the contract is impossible and if the reason is it impossible is a result of circumstances for which neither party is responsible. In such a case, the creditor shall not have the right to demand performance of the obligation from the debtor.

2.7 Can the parties exclude or agree additional termination rights?

Yes, the parties may provide additional grounds for termination of the contract in the agreement or exclude certain grounds, except for those provided for by law. An agreement limiting the debtor's liability, concluded under an adhesion contract or any other contract where the creditor is a consumer individual, shall be null and void if the amount of liability for the relevant type of obligation or for the relevant breach is established by law, or if such agreement was concluded before the circumstances giving rise to liability for non-performance or improper performance of the obligation had arisen.

2.8 To what extent can a contracting party limit or exclude its liability under national law?

The parties may provide additional grounds for termination of the contract in the agreement or exclude them, except for the grounds that are mandatory as provided by law.

2.9 Are the parties free to agree a financial cap on their respective liabilities under the contract?

Yes. Under Armenian law, parties to technology-related contracts are generally free to agree contractual limitations of liability, including financial caps on the amount of damages or compensation payable by either party, subject to certain mandatory legal restrictions.

The principle is based on the general freedom of contract under the Civil Code of the Republic of Armenia, which allows

parties to determine the terms of their contractual relationship, including the allocation of risks and liability. The only applicable limitation is the following: Any prior agreement to exclude or limit liability for an intentional breach of an obligation shall be null and void.

2.10 Do any of the general principles identified in your responses to questions 2.1–2.9 above vary or not apply to any of the following types of technology procurement contract: (a) software licensing contracts; (b) cloud computing contracts; (c) outsourcing contracts; (d) contracts for the procurement of AI-based or machine learning solutions; or (e) contracts for the procurement of blockchain-based solutions?

No. The general principles described in responses to questions 2.1–2.9 generally apply to all of the listed categories of technology procurement contracts in Armenia.

3 Dispute Resolution Procedures

3.1 What are the main methods of dispute resolution used in contracts for the procurement of technology solutions and services?

In Armenia, disputes arising from contracts for the procurement of technology solutions and services are primarily resolved through negotiation, litigation before the Armenian courts, and arbitration. There are no technology-specific dispute resolution mechanisms; instead, disputes are governed by the general rules of Armenian contract and procedural law.

The main methods of dispute resolution are as follows:

- **Negotiation and amicable settlement**
Most technology procurement contracts require the parties to attempt to resolve disputes through good-faith negotiations before commencing formal proceedings. Contracts often include provisions requiring senior management discussions and may specify a negotiation period before litigation or arbitration may be initiated.
- **Litigation before the Armenian courts**
The most common formal dispute resolution mechanism is litigation before the competent courts of Armenia. Contractual disputes involving technology products and services are generally heard by the courts of general jurisdiction in accordance with the Civil Procedure Code of the Republic of Armenia. The courts may determine disputes concerning, among other matters:
 - payment obligations;
 - breach of contract;
 - defective software or hardware;
 - delays in implementation;
 - service level failures;
 - warranty claims;
 - intellectual property ownership arising under the contract;
 - termination of the agreement; and
 - claims for damages or specific performance.

4 Intellectual Property Rights

4.1 How are the intellectual property rights of each party typically protected in a technology sourcing transaction?

In technology sourcing transactions, the allocation and protection of intellectual property rights are primarily governed by contract, subject to the mandatory provisions of Armenian legislation, including the Civil Code of the Republic of Armenia, the Law on Copyright and Related Rights, the Law on Patents and the Law on Industrial Designs. As a rule, each party retains ownership of its pre-existing intellectual property rights, including software, databases, trademarks, inventions and independently developed know-how. Under the Law on Copyright and Related Rights, the economic rights in works created by an employee in the course of employment generally vest in the employer unless otherwise agreed. Similar statutory mechanisms exist for employee inventions and employee-created industrial designs. No equivalent statutory rule applies to works, inventions or industrial designs created by independent contractors. Accordingly, rights in software, documentation and other deliverables created by contractors should be expressly assigned in writing.

4.2 Are there any formalities which must be complied with in order to assign the ownership of Intellectual Property Rights?

The applicable formalities depend on the nature of the intellectual property concerned.

Under the Civil Code of the Republic of Armenia, assignments and licences relating to patents, industrial designs and trademarks must be concluded in written form and registered with the Intellectual Property Office. Failure to comply with these requirements renders the relevant transaction invalid.

Under the Law on Patents, inventions made in Armenia are subject to foreign filing restrictions. Before filing a patent application abroad, the applicant must first file the application with the Armenian Intellectual Property Office. Unless the Office objects on national security grounds within three months, the applicant may subsequently proceed with foreign filings.

Under the Law on Copyright and Related Rights, copyright and related rights may be assigned or licensed by means of a written agreement specifying the rights transferred, the scope of use, duration, remuneration and other material terms. Rights not expressly transferred remain with the right holder.

Under the Civil Code of the Republic of Armenia, agreements concerning future intellectual property must sufficiently identify the nature of the intellectual property to be created and the intended purposes or methods of its use. Contractual provisions requiring an author to grant exclusive rights to all future intellectual creations are void.

Authors' moral rights, including the right of authorship and the right to protection of the author's reputation, are inalienable and remain with the author indefinitely.

4.3 Are know-how, trade secrets and other business critical confidential information protected by national law?

Yes. Armenian law recognises and protects trade secrets, confidential business information and know-how. Under

the Civil Code of the Republic of Armenia, information qualifies for protection where it has actual or potential commercial value because it is not generally known to third parties, is not freely accessible on lawful grounds, and the lawful holder has taken reasonable measures to preserve its confidentiality. Protection is available without registration or any other formality. The Civil Code further recognises undisclosed information, including production secrets (know-how), as an intellectual property object. The lawful holder may prevent unlawful acquisition, disclosure or use of such information and may seek damages for losses caused by infringement. Courts may also order the cessation of unlawful use.

Confidentiality obligations are frequently reinforced through contractual arrangements, including non-disclosure agreements, technology licensing agreements and service contracts. The Civil Code also provides that a party receiving confidential technical, commercial or business information while performing a contract may not disclose such information to third parties without the consent of the other party.

Protection continues for as long as the information satisfies the legal requirements for confidential treatment.

5 Data Protection and Information Security

5.1 Is the manner in which personal data can be processed in the context of a technology services contract regulated by national law?

As a general rule, the Law of the Republic of Armenia on the Protection of Personal Data (the Data Protection Law) permits the processing of personal data by the authorised person (processor) based on the instructions of the collector. Armenian law is not as sophisticated as, for instance, GDPR, and does not distinguish between collector-to-collector, collector-to-processor, or other modes of data processing and transfer.

However, the Data Protection Law defines the requirements for this instruction; it must be in writing and must include the legal grounds and conditions, the purpose of the processing of personal data, the list of personal data subject to processing, the scope of data subjects, the scope of persons to whom personal data may be transferred, technical and organisational measures for the protection of personal data, and other necessary information. The processing must be limited to the scope of this assignment and comply with the principles of processing and other requirements as defined under the Data Protection Law.

On December 4, 2025, the new Law of the Republic of Armenia on Public Information (the "Public Information Law") was adopted, which regulates the collection, processing, and use of public information by state and local self-government bodies, the creation of databases, the management of such databases, and the availability of information. The Public Information Law also applies to databases or information systems belonging to legal entities in the field of public services within the meaning of the Law of Armenia On the Public Services Regulatory Authority and to legal entities or individuals who have concluded contracts as defined in the Public Information Law, through which, in the course of exercising the powers stipulated by law or providing services, an individual is identified by means of personal identification data, regardless of whether such data are collected or processed on the basis of law or with the consent of the data subject.

5.2 Can personal data be transferred outside the jurisdiction? If so, what legal formalities need to be followed?

The Data Protection Law allows the transfer of personal data to third parties and abroad. Personal data may be transferred abroad based on the consent of the data subject, or where the transfer of data stems from the purpose of processing personal data and/or is necessary for the implementation of these purposes. As a general rule, personal data may not be transferred outside the jurisdiction unless it is transferred to a jurisdiction with an adequate level of data protection.

An adequate level of protection of personal data is deemed to exist where:

- personal data are transferred in compliance with international agreements; or
- personal data are transferred to any of the countries included in the list officially published by the Data Protection Authority.

5.3 Are there any legal and/or regulatory requirements concerning information security?

As a general rule, the Data Protection Law stipulates a few rules on security measures, such as:

- the personal data must be destroyed or blocked if it is not necessary for achieving the legitimate purpose;
- encryption keys must be used to protect information systems containing personal data in the course of processing, with the aim of protecting such systems against accidental loss, unauthorised access, unlawful use, recording, destruction, alteration, blocking, copying, dissemination of personal data, and other interference;
- access to personal data must be granted only to authorised persons and be limited to the purposes of processing; and
- confidentiality obligations are imposed on data collectors and processors.

The new Law of the Republic of Armenia on Cybersecurity (the “Cybersecurity Law”) was adopted on 4 December 2025. The Cybersecurity Law applies to information systems and critical information infrastructure in the vital sectors as defined under the law.

6 Employment Law

6.1 Can employees be transferred by operation of law in connection with an outsourcing transaction or other contract for the provision of technology-related services and, if so, on what terms would the transfer take place?

Under Armenian law, outsourcing technology-related services to another company does not trigger an automatic transfer of employees by operation of law. If the original company no longer needs these employees, it lays them off following standard legal procedures. The new service provider assumes no responsibility or liability for the former company’s staff.

6.2 What employee information should the parties provide to each other?

This is not applicable in Armenia.

6.3 Is a customer or service provider allowed to dismiss an employee for a reason connected with the outsourcing or other services contract?

If the customer outsources its technology department to a third party, it no longer requires its internal IT staff. Under the Labor Code of Armenia, this constitutes a legitimate ground for the termination of employment contracts based on the redundancy of the IT positions. However, the customer cannot dismiss the employees immediately. To ensure legal compliance, the customer must:

- **Give the employees two months’ advance written notice** or pay compensation *in lieu* of notice equal to the employee’s average salary.
- **Pay severance** equal to one average monthly salary of the employee.
- **Check for alternative vacancies** within the company that these employees are qualified to fill before implementing the layoff. If such positions exist and the company refuses to offer them to the redundant employees, this can be deemed an unlawful termination. Consequently, the company may be obligated to pay compensation for the entire period of forced idleness, as well as an additional indemnity for non-reinstatement ranging from 1 to 12 months of the employee’s average salary.

As for the service provider, it cannot terminate an employment contract for a reason connected to the outsourcing. As noted above, the provider is under no obligation to hire the former company’s laid-off personnel. If they voluntarily hire any of those individuals, those workers become new employees of the service provider under fresh contracts. Should the service provider wish to dismiss them down the line, it must establish a completely independent, valid ground under the Armenian Labor Code (such as poor performance, a breach of labour discipline, or the provider’s own separate organisational redundancy).

6.4 Is a service provider allowed to harmonise the employment terms of a transferring employee with those of its existing workforce?

As there is no transfer of employees by operation of law in Armenia, any harmonisation of employment terms is not legally mandated and can only occur on a voluntary, contractual basis upon re-hire.

6.5 Are there any pensions considerations?

No, there are not.

6.6 Are there any employee transfer considerations in connection with an offshore outsourcing?

In the event that a customer implements an offshore outsourcing model in Armenia, the two companies are treated as entirely separate legal entities. Because employees do not transfer by operation of law, the customer must first terminate the employment contracts of its onshore staff in accordance with local legislation. The Armenian service provider can then subsequently hire these individuals. Under this structure, the offshore employer is under no obligation to match or harmonise the new employment conditions with the terms of the

employees' previous onshore agreements. Instead, the terms must be newly negotiated; if the proposed conditions are unfavourable, the employees maintain the right to refuse employment with the offshore company.

7 Outsourcing of Technology Services

7.1 Are there any national laws or regulations that specifically regulate outsourcing transactions, either generally or in relation to particular industry sectors (such as, for example, the financial services sector)?

Armenian legislation does not specifically regulate outsourcing transactions.

As a general rule, outsourcing technical services is permitted. While the Armenian Civil Code regulates transactions, obligations, liability, and contracts broadly, it also defines the specifics of service provision agreements without further distinction by service type or sector.

Consequently, sector-specific requirements primarily relate to the service provider's professional standing, such as the possession of compliance certificates, relevant expertise, and audit histories.

7.2 What are the most common types of legal or contractual structure used for an outsourcing transaction?

The most common type of contractual structure used for outsourcing transactions is a service provision agreement that includes the statement of work as a contractual clause, an annex to the contract, or separate orders/instructions of the client.

7.3 What is the usual approach with regard to service levels and service credits in a technology outsourcing agreement?

Comprehensive service level agreements are common in the electronic communications sector, where they are typically incorporated into technology outsourcing agreements as an Exhibit. These contracts often specify the fines and penalties for breach of service level obligations by service providers. By contrast, outsourcing agreements in other sectors may address service levels and associated breach penalties in more general terms.

7.4 What are the most common charging methods used in a technology outsourcing transaction?

Armenian legislation allows charging based on any payment model the parties find acceptable, as per their arrangements and agreements. The Armenian tech sector mostly uses time and material or dedicated team models, though a project-based fixed fee may also be agreed upon. Services such as ongoing support, network maintenance, and IT operations are usually provided on a fixed monthly fee basis.

7.5 What formalities are required to transfer third-party contracts to a service provider as part of an outsourcing transaction?

Third-party contract transfers to a service provider as part

of an outsourcing transaction are subject to the standard formalities. The client must ensure that the service provider gains access to the tools necessary to provide the outsourced services in compliance with existing agreements. For instance, the client must verify that third-party contracts permit the engagement of an outsourcing provider and allow system and tool access to external entities or individuals; alternatively, the client must obtain the necessary third-party consents. In the event that personal data is processed, the client must ensure that the data subjects' consent explicitly covers this outsourcing scenario.

7.6 What are the key tax issues that can arise in the context of an outsourcing transaction?

Key tax considerations include compliance with transfer pricing rules for related-party transactions, assessing Permanent Establishment (PE) risks for foreign service providers, ensuring the correct application of Armenian VAT rules to cross-border services (including reverse-charge where applicable), and determining whether payments to non-resident service providers are subject to Armenian withholding tax, taking into account the applicable domestic legislation and any relevant double tax treaties.

8 Software Licensing (On-Premise)

8.1 What are the key issues for a customer to consider when licensing software for installation and use on its own systems (on-premise solutions)?

The customer in Armenia must consider the same key issues as customers in other jurisdictions. That is, the customer needs to understand the scope of the licence and the pricing model, and how these align with its needs, human resources, and budget forecasts. The customer also needs guarantees regarding the software's lifecycle, including updates, upgrades, support, and maintenance. The requirements for using the software, including the scope of access the licensor has to the customer's system, must be considered carefully depending on the customer's industry and applicable data access rules.

8.2 What are the key issues to consider when procuring support and maintenance services for software installed on customer systems?

The key issues Armenian customers face with support and maintenance services for software installed on their systems are fairly common. The parties need to clearly identify the support and maintenance services in the contract, which is typically not an easy task given service providers' insistence on more general wording. Service providers are often not keen on service level agreements, and as a general practice, these agreements lack the necessary level of detail, which leads to disputes over the assessment of service quality. The determination of a fair price for support and maintenance of the software, and access to the client's premises (where applicable), systems, and data, are also very important matters for negotiation and agreement.

8.3 Are software escrow arrangements commonly used in your jurisdiction? Are they enforceable in the case of the insolvency of the licensor/vendor of the software?

The concept of software escrow is not recognised under Armenian legislation. Where a contract is governed by Armenian law, escrow arrangements cannot be validly established through the agreement itself. Because the concept does not exist under Armenian law, such an arrangement would be unenforceable in the event of the licensor's/vendor's insolvency.

9 Cloud Computing Services (including SaaS)

9.1 Are there any national laws or regulations that specifically regulate the procurement of cloud computing services (including Software-as-a-Service)?

The Public Information Law requires that the public information controller (i.e., state bodies and self-governance bodies; legal entities in the field of public services within the meaning of the Law of Armenia On the Public Services Regulatory Authority; and legal entities or individuals who have concluded contracts as defined in the Public Information Law (see the answer to question 5.1)) organises the selection of a cloud computing service provider in accordance with the procedure prescribed by procurement legislation.

9.2 What are the key legal issues to consider and address in the contract when procuring a Software-as-a-Service solution (as opposed to or in addition to issues that apply to on-premise solutions)?

The key legal issues in procuring a Software-as-a-Service solution are fairly typical. The customer needs to ensure it has adequate access to the vendor's systems, compliance with data protection and cybersecurity regulations (including transfer of data from the vendor's system to the customer's system in the event of termination of the service), a warranty that the vendor will not access the customer's data during provision of the service, and that the vendor will permit cybersecurity testing and audits, where applicable.

10 Artificial Intelligence

10.1 Are there any national laws or regulations that specifically regulate the procurement or use of AI systems?

No, Armenian legislation does not separately regulate the procurement or use of AI systems.

10.2 What rights subsist in the data used to train, test or operate an AI system?

There are no special laws or rules that define the rights related to the data used to train, test, or operate an AI system. The

general rules relating to data protection, confidentiality, copy-right, etc., will apply at each stage of the AI system's operation.

10.3 What are the key legal issues to consider and address in the contract when procuring an AI system or AI enabled services (as opposed to or in addition to issues that apply to non-AI software)?

The key legal issue with contracts for procuring an AI system or AI-enabled services is that the fact that the system or service is fully or partially AI-based is often not addressed as such in the technology outsourcing contract. To the best of our knowledge, the market continues to sign these contracts without incorporating the necessary specifications.

10.4 Who owns the intellectual property rights to AI models that are improved or developed by machine learning techniques without the involvement of a human programmer?

Armenian IP laws do not specify who owns the IP rights in AI models that are improved or developed by machine learning technologies without the involvement of a human programmer.

11 Blockchain

11.1 Are there any national laws or regulations that specifically regulate the procurement of blockchain-based solutions?

No, there is no law or regulation that specifically regulates the procurement of blockchain-based solutions.

11.2 In which industry sectors in your jurisdiction are blockchain-based technologies being most widely adopted?

On 29 May 2025, Armenia adopted the Law on Crypto-Assets, which regulates the cryptocurrency market in Armenia. Among other things, the law regulates the tokenisation of electronic money and payments. Thus, the financial and capital markets sectors are one of the most visible and regulated sectors using blockchain-based technologies.

The free economic zone ECOS, which aims to create a favourable environment for IT businesses to operate in and stimulate the production of innovative digital products and services, states that it has made a significant contribution to the development of the blockchain industry in Armenia.

There are blockchain development companies specialising in blockchain technologies established and operating in the territory of Armenia.

11.3 What are the key legal issues to consider when procuring blockchain-based technology?

To the best of our knowledge, contracts for procuring blockchain-based technology do not specify in detail the peculiarities of blockchain-based technologies and the associated risks.

12 Looking Ahead

12.1 Looking ahead, what technological or legal development which is likely to occur in the next five years poses the biggest challenge for technology procurement, and how should businesses prepare for it?

The biggest challenge for the upcoming year or two will be the cybersecurity legislation, once all secondary legislation is adopted and the Cybersecurity Law enters into full legal force.



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 and joined the Concern Dialog team in 2013.

With nearly 20 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 Legal 500* ranking of leading individuals.

Concern Dialog Law Firm

1 Charents str., Office 207

Yerevan, 0025

Armenia

Tel: +374 99 353 452

Email: narine.beglaryan@dialog.am

LinkedIn: www.linkedin.com/in/narine-beglaryan-8a3b604b



Artur Hovhannisyan leads general administrative law, administrative law litigation, tax law, and Governmental Relations (legislation drafting and concept development) practices of the firm. His work encompasses consulting in these areas, alongside representation in judicial and administrative bodies. He obtained his attorney's licence in 2013 and joined the Concern Dialog team in 2019.

Before joining the firm, Artur Hovhannisyan dedicated 14 years to the Ministry of Justice, where he held several positions, including First Deputy Minister of Justice of the Republic of Armenia (RA). Additionally, he served as the First Deputy President of the RA Chamber of Advocates for three years.

Concern Dialog Law Firm

1 Charents str., Office 207

Yerevan, 0025

Armenia

Tel: +374 91 414 139

Email: artur.hovhannisyan@dialog.am

LinkedIn: www.linkedin.com/in/artur-hovhannisyan-b08484210



Shushanik Stepanyan leads the labour law practice at Concern Dialog Law Firm. She has been a licensed attorney since 2020. She provides advice on labour law and representation in labour disputes for both employers and employees. She also performs judicial representation in other civil cases. Shushanik joined the Concern Dialog team in 2019.

Previously, Shushanik Stepanyan served for over five years as a judge's assistant in the RA Civil Court of Appeal, gaining valuable insights into civil law procedures and practices.

Concern Dialog Law Firm

1 Charents str., Office 207

Yerevan, 0025

Armenia

Tel: +374 98 147 379

Email: shushan.stepanyan@dialog.am

LinkedIn: www.linkedin.com/in/shushanik-stepanyan-632727269



Yevgenya Nikoghosyan is a specialised attorney in the fields of intellectual property and civil law. She has been a member of the Armenian Bar Association since 2013 and has held the status of a registered Patent and Trademark Attorney since 2023.

She provides legal counsel to both corporate and individual clients in matters relating to intellectual property law, including copyright, trademarks, geographical indications, industrial designs, and patent protection. She also represents clients in civil and commercial litigation proceedings.

Concern Dialog Law Firm

1 Charents str., Office 207

Yerevan, 0025

Armenia

Tel: +374 55 777 317

Email: yevgenya.nikoghosyan@dialog.am

LinkedIn: www.linkedin.com/in/yevgenya-nikoghosyan-b1849722a

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.

The firm has extensive experience in regulatory matters in technology, media, and telecommunications, mining, energy, utilities, banking and finance, medical services, real estate, and not-for-profit sectors. In addition to its renowned consulting and transaction practice, the firm's litigation practice is regarded as one of the leading ones in Armenia

for landmark litigation and arbitration cases. The firm's membership of TagLaw and Nextlaw networks, as well as its co-operation with individual law firms from various jurisdictions, allow it to provide services to its Armenian clients virtually worldwide.

<https://dialog.am>





The **International Comparative Legal Guides** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 59 practice areas.

Technology Sourcing 2026 features two expert analysis chapters and 19 Q&A jurisdiction chapters covering key issues, including:

- Procurement Processes
- Contracting Issues
- Dispute Resolution Procedures
- Intellectual Property Rights
- Data Protection and Information Security
- Outsourcing of Technology Services
- Software Licensing
- Cloud Computing Services (including SaaS)
- Artificial Intelligence
- Blockchain