

THE CASE OF ARMENIA

Digital Transformation and Governance Gaps

Challenges for German Foreign
and Development Policy



Alena Epifanova
Research Fellow, Center for
Order and Governance in
Eastern Europe, Russia, and
Central Asia (ed.)



Arpiné Grigoryan, Digital
Operations, Technology and
Innovation Manager at APRI
Armenia



Samvel Martirosyan,
Co-Founder of CyberHUB-AM
and Dean of Digital Marketing
Department at ARDY
Academy



Digital transformation is reshaping governance worldwide, yet technical modernization does not automatically translate into more democratic institutions. Artificial intelligence is changing how bureaucracy functions, how public debates are shaped, and how decisions are made – against a backdrop of strengthening digital authoritarianism, as surveillance and online-censorship technologies increasingly penetrate Germany’s partner countries, posing not only a risk to democracy but security threats. These developments raise new and urgent challenges for German and European foreign and development policy.

This report is the first in a series examining digital transformation and the governance structures emerging around it through single case studies in the South Caucasus, the Western Balkans, and Central Asia. The series begins with Armenia, a country shifting its foreign policy toward strategic alignment and a closer partnership with the European Union, and moving fast on digital infrastructure while its governance frameworks struggle to keep pace.

Inhalt

Armenia's Tech Hub Ambition: Fast Infrastructure, Slow Governance	4
Armenia's Technological Ambition and Success	4
Governance Gaps and Vulnerabilities	5
Commitments for Good Governance	7
Recommendations	8
AI in Practice: How Armenian Civil Society Organizations Navigate the Policy Gap	10
A Three-Level Governance Gap	11
How CSOs Use AI Tools	11
Risks of Informal Use	12
Conclusion	13
Recommendations	13
Civil Society Lessons From Armenia's Cybersecurity Legislation	15
The Consultation Process: What Worked and What Did Not	16
The Cybersecurity Community and e-draft.am as Participation Infrastructure	17
Trust, Accountability, and Future Civic Engagement	17
Implications for AI and Digital Governance	18
Conclusion and Recommendations	18

Armenia's Tech Hub Ambition: Fast Infrastructure, Slow Governance

Germany and the European Union Should Support Closing the Gap

ALENA EPIFANOVA,
RESEARCH FELLOW, CENTER FOR ORDER AND
GOVERNANCE IN EASTERN EUROPE, RUSSIA,
AND CENTRAL ASIA

Armenia has the ambition to become a tech hub connecting the South Caucasus with Europe and Asia. The government has placed digital transformation at the center of its national development strategy. Adopting emerging technologies such as artificial intelligence (AI) promises economic growth and a brighter exports perspective. Digital technologies bring also the democratic promise of more transparent public services, broader citizen access to information and participation, and a government more accountable to the people. Under Prime Minister Nikol Pashinyan and the Civic Contract party, Armenia has achieved significant results and advanced swiftly in securing major infrastructural projects as well as in digitizing dozens of public services and introducing e-participation platforms. However, success in these areas does not fully match what is needed for sustainable democratic digital governance: personal data protection, digital literacy, and cybersecurity. Germany and the European Union are well placed to support Armenia and to ensure it achieves its ambition of regional technological leadership without compromising its political choice of democratic and open governance.

ARMENIA'S TECHNOLOGICAL AMBITION AND SUCCESS

Armenia strives to become a leading regional tech hub by building an advanced digital infrastructure and modernizing its public administration. The 2021 Digitalization Strategy set as a national goal comprehensive transformation across government, economy, and society, with the aim to modernize public administration, drive economic growth, and ensure inclusive access to digital technology for all citizens.¹ It also set internationally benchmarked targets. One was climbing from 67th place in the UN's e-Government Development Index to be among the top 25 countries by 2025. This target has not yet been met, but there has been substantial progress: in 2024, Armenia reached 48th place, putting it in the "Very High" tier.²

The establishment of the unified e-government services platform (e-gov.am) was one of the key initiatives that contributed to this achievement. It is the central gateway to online public services, including tax filing, property registration, and requests or complaints to state bodies. Various administrative bodies have also launched dozens of specialized official electronic platforms, such as the Ministry of Justice's e-draft.am for public consultation on draft legislation. Subsequently, between 2022 and 2024, Armenia rose

1 Government of the Republic of Armenia: Approval of the Digitization Strategy of Armenia, the Strategy Action Plan and the Result Indicators (February 11, 2021): <https://www.arlis.am/hy/acts/149957> (accessed August 20, 2026)

2 United Nations, UN E-Government Knowledgebase, Country Information Armenia: <https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/8-Armenia/dataYear/2024>, (accessed August 21, 2026)

from 64th to 27th place in the UN's E-Participation Index, which measures the extent to which governments enable citizens to access information and engage in public consultations.³ However, this ranking captures the availability of participatory tools more than the quality of participation they enable and people's trust in them.⁴

Armenia has moved from digitizing services to building its computational capacity. The government's principal achievements in this regard include the Nvidia-powered AI supercomputer at Yerevan State University,⁵ a partnership with Mistral AI, and the Nvidia-backed data center rank in Hrazdan. The largest of its kind in the South Caucasus, the latter is the result of a \$500 million public-private partnership with the Armenian-American AI cloud company Firebird.ai and is built on Nvidia's DSX platform. It was launched in August 2026 with the aim to deploy more than 70,000 most-advanced Nvidia Rubin and Blackwell graphics processing units (GPUs). When it was first announced in June 2025, the aim for the capacity of the data center was 100 MW,⁶ but it is now expected to reach 300 MW by the end of 2027.⁷

Another signature project is the Virtual Institute of Artificial Intelligence. Launched in July 2025 by the Ministry of High-Tech Industry, it is supported by Amazon Web Services (AWS) and Mistral AI.⁸ It is designed as an open platform for researchers, startups, and technology companies. Combined with mentorship and funding support, the institute aims to foster domestic innovation and to integrate Armenian talent into the global networks of AWS and Mistral AI, positioning the country as a regional AI hub.

The government strongly prioritizes AI and has increased its ambition in this field. The new five-year program for 2026–2031 sets the goal of building AI

computing capacity equivalent to at least 100,000 advanced GPUs, with 10 percent made accessible to research, education, startups, and the public sector.⁹ It also enshrines “AI first” as a core principle of public-administration reform, alongside “zero bureaucracy” and “digital by design.”¹⁰ Under this principle, state bodies must consider AI applications as a first option when addressing administrative tasks. In another clear institutional signal, the Ministry of High-Tech Industry had “Artificial Intelligence” added to its name in August 2026.¹¹

GOVERNANCE GAPS AND VULNERABILITIES

Armenia's government is going to deploy AI in public administration and has committed itself to the “AI first” principle under a framework that contains no requirement for impact assessment and no provision governing algorithmic decision-making yet. An independent assessment of the country's public administration by the SIGMA program of the Organisation for Economic Co-operation and Development and the EU, published in late 2025, noted the absence of legal acts regulating the use of algorithms in administrative decision-making or of strategies for the uptake of AI and emerging technologies in the public sector.¹² This shows that the digital infrastructure is being built faster than the rules to govern it are being written.

This matters because of the democratic logic and promise attached to digitalization: digital services are supposed to reduce barriers for citizens to participate in decision-making, and open data to allow journalists, civil society, and citizens to see what government does and to hold it accountable. In this context, the protection of personal data¹³ is a cornerstone of democracy as it safeguards privacy, free expression, and

3 Ibid.

4 See “Civil Society Lessons From Armenia's Cybersecurity Legislation” by Samvel Martirosyan in this publication.

5 Charlotte Trueman, “Legrand Delivers Nvidia-Powered Supercomputer to Armenia's Yerevan State University”, DatacenterDynamics (August 19, 2026): <https://www.datacenterdynamics.com/en/news/legrand-delivers-nvidia-powered-supercomputer-to-armenias-yerevan-state-university/>.

6 Jason Ma, “US Approves Sale of Nvidia Chips to Armenia for 100MW Data Center” DatacenterDynamics (August 19, 2026): <https://www.datacenterdynamics.com/en/news/us-approves-sale-of-nvidia-chips-to-armenia-for-100mw-data-center/>.

7 Charlotte Trueman, “Firebird AI Launches 300MW Nvidia-Powered AI Data Center in Armenia”, DatacenterDynamics (August 19, 2026): <https://www.datacenterdynamics.com/en/news/firebirdai-launches-300mw-nvidia-powered-ai-data-center-in-armenia/>.

8 “Virtual Institute of AI Launched in Armenia”, Armenpress (July 8, 2025): <https://armenpress.am/en/article/1224355>.

9 “Armenia's Government Approves 2026–2031 Program, Sets out Key Development Targets”, Public Radio of Armenia, n.d.: <https://en.armradio.am/2026/08/20/armenias-government-approves-2026-2031-program-sets-out-key-development-targets/> (accessed August 20, 2026).

10 “Armenia Adopts AI First Principle for Public Administration: AI to Be the Mandatory First Option for Officials”, IXBT Armenia (August 24, 2026): <https://ixbt.am/en/news/2026/08/24/430046-armeniia-perevodit-gosupravlenie-na-ai-first-ii-stanet-obiazatelny-m-pervym-variantom-dlia-cinovnikov.html>.

11 “Three ministries to be renamed as National Assembly adopts bill in full”, Armenpress (August 27, 2026): <https://armenpress.am/en/article/1259066>.

12 SIGMA (Support for Improvement in Governance and Management), “Public Administration in Armenia 2025” (December 5, 2025): https://www.sigmaweb.org/en/publications/public-administration-in-armenia-2025_f996600c-en.html.

13 Personal data is any information related to an individual that allows or may allow for direct or indirect identification of that individual's identity. It may vary from a first name, surname, or email address to an Internet Protocol (IP) address, geolocation data, or other information.

trust in public institutions. Secure data rights and adequate governance prevent surveillance, ensure electoral integrity, and increase public trust.

Three foundations play a crucial role in realizing digitalization's democratic promise: the framework for governing data, human capacity, and the security of systems. In Armenia, each is currently lagging the technology.

Data

Armenia's solid data governance framework has become outdated due to the rapid adoption of technologies, and it has significant institutional limits. In 2015, the protection of personal data was given constitutional status as part of fundamental rights and freedoms.¹⁴ That same year, the Law on the Protection of Personal Data was adopted and the Personal Data Protection Authority was created to oversee its implementation. The law declares the authority independent, but its structure is set by government decision and its head is appointed by the prime minister following nomination by the justice minister, albeit from a list of people recommended by at least five nongovernmental organizations. The accountability and independence of the Personal Data Protection Authority remain limited. It operates under the Ministry of Justice, through which it receives state funding. It is also constrained by its limited human resources, which is due mostly to the lack of specialists in the field of data protection in Armenia.¹⁵

The 2015 Law on the Protection of Personal Data was an important milestone and is a solid base for data protection. However, while it provides a broad framework for data protection in the country, data processing in individual sectors is regulated by sector-specific legislation. In many cases, this legislation has failed to keep pace with the speed of digitalization, and it was not compliant from the outset with the data protection principles established by the 2015 law

and comparable to those under the EU's General Data Protection Regulation (GDPR). SIGMA's assessment points out that, while there has been notable progress in digitalizing public services and in digital availability, there is insufficient alignment with the EU's standards, including the GDPR.¹⁶ Harmonizing sector-specific legislation governing personal data processing is therefore emerging as one of the central challenges at the intersection of digitalization and data protection.

So far, no systematic use of AI tools across state bodies has been documented. However, there has been a case of the State Revenue Committee using AI to detect fraud, improve tax compliance, and determine taxpayers' risk levels.¹⁷ A report on AI use in the public sector in 2025 indicated that AI adoption by public administration bodies is likely to grow quickly, inevitably involving personal data processing.¹⁸ The adoption of the "AI first" principle will accelerate this.

People

SIGMA has identified limits in human capacity and the lack of a structured approach to developing or retaining IT talent in the public sector. Only about 42 percent of surveyed public servants reported having received sufficient training on cybersecurity skills to understand risks and gain the know-how to avoid them.¹⁹ There is a structural mismatch at the core of Armenia's digital transformation: the political will to adopt new technology is clear and consistently demonstrated but the public administration's capacity to implement it is inadequate. Human resources in the public sector remain insufficient in number and staff are inadequately trained to apply new technologies, and capacity-building has not kept pace.²⁰ As a result, the government's ambitious decisions are not fully grounded in state capacity – a gap likely to persist in the coming years of reforms and to limit the government's success, regardless of the strength of its intentions.²¹

14 President of the Republic of Armenia, Constitution of the Republic of Armenia: <https://www.president.am/en/constitution-2015/> (accessed August 20, 2026)

15 Author's interviews conducted with Armenian experts, representatives of civil society and the public and private sectors, February 2026, Yerevan.

16 SIGMA (Support for Improvement in Governance and Management), "Public Administration in Armenia 2025" (December 5, 2025): https://www.sigmaweb.org/en/publications/public-administration-in-armenia-2025_f996600c-en.html

17 Khuram Farooq and Arman Vatyan, "AI to Modernize Tax Administration: The Story behind Armenia's Success", World Bank Blogs (May 1, 2026): <https://blogs.worldbank.org/en/governance/ai-to-modernize-tax-administration--the-story-behind-armenia-s-s>

18 Gevorg Hayrapetyan, "The use of artificial intelligence tools in state bodies of the Republic of Armenia", Media Diversity Institute Armenia (January 10, 2026): <https://dphub.am/ai-in-public-bodies-of-the-ra/>

19 SIGMA (Support for Improvement in Governance and Management), "Public Administration in Armenia 2025" (December 5, 2025): https://www.sigmaweb.org/en/publications/public-administration-in-armenia-2025_f996600c-en.html

20 Author's interviews conducted with Armenian experts, representatives of civil society and the public and private sectors, February 2026, Yerevan.

21 Author's interviews with Armenian experts, representatives of civil society and the public and private sectors, February 2026, Yerevan.

There has been no comprehensive quantitative assessment of the population's level of digital literacy.²² This leaves the government without a baseline for targeted strategies on digital literacy, digital hygiene, or cybersecurity in formal or informal education. A further problem highlighted by Armenian practitioners in the digital field is the lack of awareness about data protection.²³ A general understanding of privacy and the risks of digital surveillance is not fully internalized across society. While the government recognizes the problem and addresses it in its action plans, attention to data protection across the public and private sectors is insufficient and not fully addressed.

Cybersecurity

Armenia has begun to address the cybersecurity challenge systemically only in the last few years. In December 2025, after a long and intensive consultation process between the Ministry of High-Tech Industry, business, civil society, and the IT community, the first Law on Cybersecurity was adopted. It aims to set unified standards, given that until now every business and state body has developed its information systems independently while often neglecting cybersecurity altogether. The law defines critical information infrastructure, mandates incident reporting, and creates an independent regulatory authority, addressing the fragmentation that SIGMA identified in Armenia's digital governance.

Armenia's exposure to cyber threats has increased amid geopolitical tensions as the country's pivots toward the EU and the United States, and as it integrates Western technologies into its infrastructure while decoupling from security institutions led by and long-standing dependencies on Russia. The digital domain has become the primary theatre for hybrid pressure and intelligence collection within Armenia.²⁴ State-aligned actors, reportedly Russia's APT28 (Fancy Bear) and cluster UNC5792, have intensified their attacks against government institutions and other targets, and shifted their operations from email to encrypted messaging platforms, exploiting the public's trust in Signal and WhatsApp.²⁵

Given their role in strengthening democracy, human right defenders, independent media, and civic activists are strategic targets for such authoritarian actors. Civil society and independent media are the most heavily targeted sector in Armenia, and they experienced "at least eight" significant documented incidents in 2025.²⁶ They are also the least prepared. Severely limited resources when it comes to hardware and software, backups, and clouds make civil society highly vulnerable.²⁷

COMMITMENTS FOR GOOD GOVERNANCE

In the 2026 elections, Pashinyan and his party secured a mandate for their drive for Armenia's technological leadership in the region. The government has started to close the gaps in digital governance and is trying to catch up with regard to regulations for securing digital democracy. But most of the responses so far have remained at the level of stated commitments and implementation of new legislation will be crucial.

Armenia has taken first steps toward meeting international standards by signing the Council of Europe's Framework Convention on AI, Human Rights, Democracy and the Rule of Law in January 2026.²⁸ The convention is the world's first legally binding international treaty of its kind. It requires that AI systems be compatible with human rights, democracy, and the rule of law throughout their entire lifecycle: from design and development through deployment and retirement. It also obliges signatories to prevent algorithmic discrimination and unfair treatment, and to apply a risk-based approach to AI oversight, with obligations extending across the public and private sectors.

The government's 2026–2031 program aims for a unified, secure AI environment for the public sector and a separate regulatory framework for the state's AI use, to be grounded in risk assessment, data protection, cybersecurity, and mandatory human oversight, which closely tracks the Council of Europe

22 USAID, Digital Ecosystem Country Assessment (DECA), Armenia, May 2024, p. 31.

23 Author's interviews conducted with Armenian experts, representatives of civil society and the public and private sectors, February 2026, Yerevan.

24 CyberHUB-AM, "Armenia Cybersecurity Threat Landscape", 2025: <https://cyberhub.am/wp-content/uploads/2026/04/Armenia-Cybersecurity-Threat-Landscape-2025.pdf-eng.pdf> (accessed August 20, 2026)

25 Ibid.

26 Ibid.

27 Author's interviews conducted with Armenian experts, representatives of civil society and the public and private sectors, February 2026, Yerevan.

28 Ministry of Foreign Affairs of the Republic of Armenia: "Signing of the Convention on the Protection of Human Rights in the Field of the Use of Artificial Intelligence" (January 27, 2026): https://www.mfa.am/en/press-releases/2026/01/27/Mirzoyan_convention/13747

convention. Implementing this quickly and creating an implementation and oversight body is as crucial as strengthening the protection of personal data, which will be inevitably impacted by the “AI first” principle.

Success regarding this commitment will significantly depend on the implementation of a parallel reform already underway: the transformation of the Personal Data Protection Authority. This is driven by the Visa Liberalization Action Plan that the European Commission presented in November 2025, which conditions progress toward visa-free travel with the EU on deliverables that include data protection. This requires a genuinely independent authority with adequate powers and the human and financial resources to exercise its mandate, effective implementation of data protection legislation across the public and private sectors, and training and awareness-raising programs for public institutions and officials.²⁹ Given how politically salient the issue of visa liberalization is in Armenia, this is the strongest conditionality attached to any digital-governance reform currently available.

A package of draft legislative acts for ensuring the independence of the Personal Data Protection Authority has been presented for public consultation. One of these would introduce mandatory data protection impact assessments (DPIAs) where processing involves special categories of personal data or biometric data; where the nature, scope, purposes, or technology of processing may pose a high risk to rights and freedoms; or where the authority's criteria classify processing as high risk. In principle, this could apply to AI use in public administration: such processing may qualify as high-risk under the criteria, which the authority has yet to define. But the legislation regarding DPIAs is still at the draft stage, and it is not yet clear to what extent it will cover the use of AI. Moreover, the time legislating and implementing will likely take means such a mechanism might not be in place before 2028.

Another key area is the capacity to enforce the Cybersecurity Law. Its provisions defining vital sectors for the country's normal functioning. It aims for the adoption of international standards and introduction of a regulatory authority. These provisions are designed to bring clarity to sectors now rapidly adopting digital solutions and to end the fragmentation of responsibility across ministries. Together, they are intended to build a more resilient foundation for

Armenia's efforts to become a tech hub. However, the authority has yet to be established, while the shortage of specialists that constrains the Personal Data Protection Authority applies also here. The law's provisions are sound but the capacity to implement them still needs to be built.

RECOMMENDATIONS

- The EU should address through the Partnership Council with Armenia and in the implementation of the Visa Liberalization Action Plan the need for aligning an independent and well-resourced Personal Data Protection Authority with an up-to-date legislation on data protection and algorithmic accountability.
- Through its Federal Ministry for Economic Cooperation and Development and Federal Foreign Office, Germany should support a sustained training program in data protection and AI law to address shortages in human resources in the public sector and civil society.
- Germany and the EU should support the capacity of Armenia's civil society to shape and monitor the country's digital and AI governance. Funding for targeted legal and technical training in AI governance and data protection is needed now as the “AI first” regulatory framework is being drafted and civil society can contribute its perspective through the e-draft.am platform and consultations with the government. Additionally, civil society needs the technical capacity to monitor deployed systems for transparency, non-discrimination, and meaningful human oversight.
- Given that civil society and independent media face the greatest volume of cyberattacks and remain poorly equipped technically, the European External Action Service should establish a long-term (five-year minimum) technical and institutional support package for them, directed at capacity-building, raising awareness about data protection, and cybersecurity.
- Germany and the EU should fund public-awareness work on data rights alongside their technical assistance, and they should encourage Armenia's

29 European Commission: “First Progress Report on the Implementation by Armenia of the Action Plan on Visa Liberalisation,” COM(2026) 168 final, April 30, 2026, transmitted as Council of the European Union doc. 8858/26, May 5, 2026 <https://data.consilium.europa.eu/doc/document/ST-8858-2026-IN17/en/pdf>

government to build capacity based on genuine feedback and response data for its e-participation platforms, which will make the state's performance visible and increase societal acceptance for reforms in this area.

- European and German international cooperation organizations should support Armenia's government in measuring the population's digital literacy and developing a baseline for a targeted strategy in formal and informal education.
 - European and German international cooperation organizations should embed data-protection safeguards with clear rules and responsibilities in all stages of their projects in Armenia. European companies involved with Armenia should likewise be encouraged to require the standards of data protection and algorithmic accountability that Armenian law has not yet established, exporting EU-equivalent practice through commercial relationships while the domestic legislation is being shaped.
-

AI in Practice: How Armenian Civil Society Organizations Navigate the Policy Gap

Emerging Practices, Informal Norms, and Operational Challenges in the Use of AI Tools Among CSOs

ARPINÉ GRIGORYAN, DIGITAL OPERATIONS, TECHNOLOGY AND INNOVATION MANAGER AT APRI ARMENIA

Across Armenian civil society, artificial intelligence (AI) tools have gradually become part of the daily work of drafting grant proposals, conducting and summarizing research, and translating documents without any rules governing their use. This is happening during a period of rapid, state-backed expansion of the country's AI sector. So far in 2026, the government has added "Artificial Intelligence" to the name of the Ministry of High-Tech Industry, thus formally elevating the sector,³⁰ while major private investors³¹ have launched large-scale compute facilities.³² The Ministry of Education is partnering with OpenAI and Firebird to provide 50,000 users with free access to ChatGPT Edu and Codex.³³

In terms of the legal framework for regulating AI adoption, Armenia's key external reference points are the Council of Europe Framework Convention on Artificial Intelligence, which it signed in January 2026, and the EU's AI Act. It agreed with the EU in May 2026 to explore cooperation on AI in line with the act, which is framed as part of broader integration into the EU's digital single market. This nonbinding commitment, however, is contained within a joint statement focused on infrastructure, investment, and

market access rather than on how AI should be used or governed. Armenia has no AI legislation, and the reference to the EU act has not yet been translated into operational rules for organizations using AI tools. That gap is most visible in civil society.

This policy brief argues that the widespread adoption of AI without the institutional capacity to mitigate risks creates serious vulnerabilities. At the same time, through everyday practice, Armenian civil society organizations (CSOs) are developing informal norms around the use of AI tools and becoming de facto co-creators of AI governance, and this should inform the country's emerging AI regulatory framework.

This policy brief draws on 12 semi-structured interviews conducted with representatives of Armenian CSOs working across the fields of public policy, media, human rights, culture, governance, youth development, and social services. It is also informed by the author's professional experience in leading digital systems and AI adoption efforts at the APRI Armenia think tank, including the development of internal guidance on AI use and staff training. More broadly, the analysis builds on over 14 years of the author's work in supporting CSOs in Armenia through digital systems development, digital literacy training, and technology capacity-building initiatives.

30 "Armenia Plans to Rename High-Tech Ministry to Include AI Focus," Armenpress, May 11, 2026, <https://armenpress.am/en/article/1249847>

31 "Armenia as a Global AI Hub: The Firebird AI Center in Hrazdan to Place the Country Among the World's Top Five Leaders," Ministry of High-Tech Industry of the Republic of Armenia, June 5, 2026, <https://hightech.gov.am/en/articles/%D5%B6%D5%B8%D6%80%D5%B8%D6%82%D5%A9%D5%B5%D5%B8%D6%82%D5%B6%D5%B6%D5%A5%D6%80/firebird-06-1>

32 "Eleveight AI Opens Region's First AI Factory in Gagrar: Minister of High-Tech Industry Attends the Event," Ministry of High-Tech Industry of the Republic of Armenia, June 1, 2026, <https://hightech.gov.am/en/articles/%D5%B6%D5%B8%D6%80%D5%B8%D6%82%D5%A9%D5%B5%D5%B8%D6%82%D5%B6%D5%B6%D5%A5%D6%80/eleveight-ai-opens-regions-first-ai-factory-in-gagrar-minister-of-high-tech-industry-attends-the-event>

33 Gayane Gaboyan, "Armenia to Introduce ChatGPT Edu Across Its Education Sector," Armenpress, May 29, 2026, <https://armenpress.am/en/article/1251545>

A THREE-LEVEL GOVERNANCE GAP

The practices of AI adoption within Armenian civil society can be understood through three connected levels: national regulation, organizational governance, and individual practice.

At the national level, the government has made international commitments and is developing a national AI strategy, but it has not yet adopted domestic regulations. In January 2026, Armenia signed the Council of Europe Framework Convention on Artificial Intelligence, the first internationally binding instrument in the field.³⁴ The convention – which no signatory except the EU has ratified yet³⁵ – sets out high-level principles like human dignity, nondiscrimination, privacy, and data protection. As for the EU's AI Act, for the government it is mainly about market access rather than governance. The Ministry of High-Tech Industry is developing a national AI strategy, with responsible development, data protection, and accountability among its declared objectives.³⁶ As of July 2026, there was no adopted framework, implementation guidance for civil society, or public timeline.

At the organizational level, most CSOs operate without formal AI policies or internal guidelines. At the time of writing, of the ones included in the research, only two had developed a written AI policy. A small number had verbal agreements within their team about acceptable use, typically focused on content accuracy or avoiding the input of personal data. The majority relied entirely on individual judgment, with no shared understanding of what constitutes acceptable AI use, what counts as sensitive data in their context, and no requirements for internal or external disclosure.

At the individual level, AI adoption is driven primarily by productivity needs. CSO staff members use AI to increase productivity, experimenting with tools (often through personal accounts) based on curiosity or peer recommendations. Levels of AI literacy vary considerably. Many users have a limited understanding of how generative AI systems process and retain data, what privacy and confidentiality risks arise from sharing organizational information with third-party

platforms, how to detect inaccuracies or biases in AI-generated content, or when disclosure of AI use may be expected by partners and the public.

Each of the issues observed pushes responsibility downward to the next level: with no national guidelines, organizations improvise; with no organizational rules, individual staff members are left to decide on their own judgment what is safe to share and when to disclose.

HOW CSOS USE AI TOOLS

Across the 12 CSOs looked at, generative AI platforms – particularly ChatGPT, Gemini, and Claude – have been used most consistently for three purposes: drafting and editing text (grant proposals, reports, communications materials); translation and proofreading; and research-support tasks such as summarizing documents, transcribing meetings, and generating ideas.

For CSOs operating in multilingual environments with small teams, AI-powered translation and editing tools provide immediate practical value. One human rights CSO described using AI extensively for drafting reports, grant proposals, and research and translation support, particularly following staff layoffs after losing a significant funding source. A cultural CSO reported using ChatGPT and Grok for tasks ranging from drafting emails and grant applications to creating design mockups of folk costumes. A youth CSO uses AI primarily for participant outreach and communications, while limiting its use to non-sensitive documents.

The level of AI integration varies sharply across the CSOs. At one end of the spectrum, the management of an educational one encourages all staff to use AI and has invested in paid subscriptions. At the other, a youth CSO reported minimal adoption with no organizational position on AI at all. In most cases, adoption depends on individual initiative – a single enthusiastic staff member drives a CSO's entire AI use, sometimes over management skepticism. This means that AI governance, where it exists, is often tied to a person rather than embedded in the organization.

34 "Armenia Signs the Council of Europe's Framework Convention on Artificial Intelligence," Council of Europe, <https://www.coe.int/en/web/artificial-intelligence/-/armenia-signs-the-council-of-europe-s-framework-convention-on-artificial-intelligence-duplicate-2>

35 Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, adopted May 17, 2024, opened for signature September 5, 2024, <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>

36 "Armenia Outlines Strategic Resources and Priorities for AI-Driven Future," EU4Digital, April 30, 2026, <https://eufordigital.eu/armenia-outlines-strategic-resources-and-priorities-for-ai-driven-future/>.

In most CSOs, staff members make daily decisions about data-sharing, AI tool usage, and disclosure without a shared framework to guide them. Several key patterns emerged from the interviews.

Informal, verbal rules and lack of written safeguards: The most common form of “policy” consists of verbal understandings communicated informally by the CSOs’ leadership. For instance, a cultural one has verbally advised caution regarding historical and religious content, while a think tank has verbally banned AI content generation but encouraged it for translation and proofreading. None of these verbal rules have been formally documented. Conversely, a youth CSO has established a strict verbal rule against inputting participant data. However, even the most cautious CSO lacked written protocols or systematic safeguards, leaving management largely unaware of exactly how extensively AI is being used across the organization.

Data privacy blind spots: Several of the CSOs admitted that staff input internal documents, donor communications, and project details into generative AI tools without understanding platform privacy settings. One interviewee noted a total lack of concern about inputting financial data, reasoning that this was not sensitive because their CSO’s work was legal (“We have nothing to hide”).

Inconsistent disclosure practices: Most of the CSOs do not disclose AI use in their outputs. The reasons given for this vary. Some view AI editing as too minor to mention while others simply have not considered it. A few disclose AI-generated images but not AI text. Exceptions include one think tank with an online disclosure policy,³⁷ and media organizations bound by the Media Ethics Observatory’s Code of Ethical Principles.³⁸ No CSO reported receiving donor requests to disclose its use of AI in grant proposals or reports.

Shared account vulnerabilities: To save money, many of the CSOs share a single paid AI subscription (like ChatGPT Plus) among multiple team members. A cybersecurity expert warned that this creates severe security risks: it exposes individual conversation histories, eliminates accountability for what is shared, and increases the likelihood of data leaks if credentials are compromised.

Isolation in AI governance: Awareness of peer practices is very limited, with most of the CSOs developing rules in total isolation. Outliers include a youth network of 40+ organizations co-developing shared guidelines, and a social development CSO that received a draft internal policy from its US head office.

Unequal access to capacity-building: While nearly all of the CSOs express a need for it, access to AI training is uneven. Internationally connected ones and donor-supported media outlets receive regular training. Conversely, smaller, regional CSOs rely purely on self-taught experimentation and lack the time and expertise to build internal guidelines.

RISKS OF INFORMAL USE

The interview findings reveal three operational risks, each one compounded by the absence of institutional governance frameworks.

Data Security and Confidentiality

The most immediate risk involves the uncontrolled sharing of sensitive information with AI platforms. These platforms typically store user inputs and their free-tier services may use conversation data to improve their models, creating the possibility that confidential information entered by one user could surface in outputs generated for others.³⁹ A CSO has no control over data once it is entered. For those working with vulnerable populations or on sensitive research, a staff member entering personal information into an AI tool creates an exposure that it cannot monitor, limit, or reverse.

Content Accuracy and Overreliance

AI-generated outputs are often polished and persuasive, which can mask inaccuracies, fabricated references, or misleading summaries. For human rights CSOs producing advocacy reports or think tanks publishing policy analysis, the credibility cost of an undetected factual error is significant. The risk of overreliance is also generational and behavioral: a youth CSO specifically flagged concern that younger team members and participants in projects may substitute AI outputs for original thinking, treating AI as a source of truth rather than a supporting tool. Extensive dependence on AI-generated drafting may weaken internal

37 APRI Armenia’s Statement on the Ethical Use of Generative AI, <https://apri.institute/statement-on-ethical-genai-use/>

38 Code of Ethical Principles of Armenian Media and Journalists, sections 6.5–6.8, https://ypc.am/wp-content/uploads/2024/06/Code-of-Ethics_arm_edites_May-18-2024.docx.pdf

39 Fast Company, “Stop letting ChatGPT and other AI chatbots train on your data,” May 2, 2026, <https://www.fastcompany.com/91529322/stop-letting-chatgpt-ai-chatbots-train-on-your-data-anthropic-claude-perplexity-google-gemini-opt-out>

analytical and writing capacity, particularly among younger staff members.

Accountability and Transparency Toward Partners

None of the CSOs has received any AI use guidance on the likes of disclosure requirements and acceptable practices from donors or international partners. They assume their current approach is acceptable, and donors may not realize how extensively AI tools contribute to the reports, proposals, and deliverables they receive. As AI-generated content becomes harder to distinguish from human-written text, this gap in awareness poses a growing reputational risk for both sides.

CONCLUSION

AI governance in Armenia's civil society is shaped more by informal adaptation than by institutional rules. That flexibility lets CSOs experiment and adopt tools quickly, but the absence of formal policies and disclosure standards puts transparency, accountability, and public trust at risk. As AI use grows, the shift from improvised norms to deliberate governance will become central to organizational credibility.

A comprehensive national AI regulatory framework is unlikely to materialize soon. Armenia's commitments remain statements of intent rather than enforceable rules that cover civil society. For now, the only concrete governance many CSOs encounter is sectoral self-regulation, most visibly through the Media Ethics Observatory's code, which a large share of the country's outlets has signed. CSOs will keep using AI tools, driven by the same resource constraints and productivity pressures, regardless of whether formal governance catches up. The relevant question is whether the informal norms CSOs develop in the interim will be recognized and built upon when regulation arrives.

RECOMMENDATIONS

For German and EU policy-makers

Ensure CSO consultation is built into AI governance technical assistance. When providing technical assistance on AI legislation to Armenia, its EU partners should require that consultation with civil society – including CSOs working with vulnerable groups, in the regions, and in the media field – is built into the process. Technical assistance should also include developing practical guidance documents, toolkits, or templates that organizations without legal or IT departments can use.

Facilitate peer learning between EU and Armenian CSOs. Armenian CSOs have almost no awareness of how their peers elsewhere handle AI governance. EU CSO networks that have already developed AI policies could share their experience through structured exchanges, particularly through existing networks like the Eastern Partnership Civil Society Forum.

For donor organizations

Provide practical support. Armenian CSOs' donors and international partners should communicate clear expectations regarding the acceptable use of AI in the production of grant proposals and reports, but they must also match those expectations with resources. CSOs would benefit from donor assistance in three areas. First, access to paid AI tools, which offer stronger privacy protections and more reliable outputs than free versions but remain out of reach for many CSOs. Second, access to expert guidance, whether through dedicated consultants, peer-learning programs, or partnerships with organizations experienced in AI governance, which can help CSOs develop internal policies suited to their context. Third, structured capacity-building programs that go beyond basic introductions to AI and address practical questions of data security, risk assessment, and verification. Some of this support already reaches media organizations and CSOs connected to international networks, but it has not extended to the sector as a whole.

For Armenia's policy-makers

Include civil society as a partner in AI policy design. As Armenia develops its national AI policy, CSOs that have accumulated practical experience should be included as partners in the process, rather than be treated just as subjects of future regulation. They bring operational experience with AI tools and, importantly, the perspectives of the communities they serve. Human rights CSOs can flag the sensitivity of the data they handle and the specific risks that poorly designed regulation could create for their work. Media organizations bring practical experience with self-regulatory approaches to AI governance.

Structured consultation with CSOs – whether through the e-draft platform, dedicated working groups, or targeted dialogues – would help ensure that the resulting framework is practical enough to be useful and proportionate enough to encourage voluntary adoption in civil society.

For Armenia's CSOs

Develop clear internal AI guidance. CSOs do not need to rewrite their charters or to draft comprehensive

formal policies immediately. A short internal memo or practical handbook is a more realistic and manageable starting point. Such a document should cover approved tools, acceptable and prohibited use cases, data-protection rules (particularly regarding personal and sensitive information), human oversight and verification expectations, and basic disclosure principles. It should be written in plain language, integrated into existing procedures, and treated as a living document that is reviewed periodically as technology and circumstances change. The Media Ethics Observatory, which incorporated AI-specific provisions into its Code of Ethical Principles, offers a practical model of sector-level self-regulation without heavy bureaucratic infrastructure.

Civil Society Lessons From Armenia's Cybersecurity Legislation

SAMVEL MARTIROSYAN, CO-FOUNDER OF CYBERHUB-AM AND DEAN OF DIGITAL MARKETING DEPARTMENT AT ARDY ACADEMY

Armenia's rapid digitalization has expanded access to public services, but it has also enlarged the country's attack surface. In 2025, researchers documented distributed denial-of-service attacks, phishing, account compromise, website intrusions, and operations linked to state-aligned actors. In January 2026, the authorities investigated the alleged sale of a database advertised as containing more than eight million government-related records.⁴⁰

Armenia has pursued its digitalization transformation while participating in the Open Government Partnership and seeking closer alignment with European standards. The International Telecommunication Union's 2024 Global Cybersecurity Index placed the country in Tier 4 ("evolving"), the second-lowest of its five tiers. This indicates that important elements of a national cybersecurity framework are present, but that significant institutional, legal, capacity, and co-operation gaps remain.⁴¹

The European Union's Strategic Agenda for the EU-Armenia Partnership commits the two sides to strengthening Armenia's cyber resilience and to developing its cybersecurity laws and regulations aligned with key EU legislation. The EU's NIS2 Directive is therefore a relevant benchmark because it combines risk-based supervision, incident reporting, sectoral coverage,

and enforcement. Armenia's 2025 cybersecurity legislation is not presented in official materials as a formal transposition of NIS2, however, and differences in legal context and institutional capacity remain important. Germany's role has been primarily supportive: initiatives it funded and supported have contributed to increasing cybersecurity skills, institutional cooperation, and ecosystem development.⁴²

Against this background, the Ministry of High-Tech Industry, working with the Information Systems Agency, developed a legislative package comprising the Law on Cybersecurity, the Law on Public Information, the Law on the Information Systems Regulatory Body, and related amendments. In 2025, the government approved the package and the National Assembly adopted the three core laws.⁴³

The core cybersecurity reform is a new system for identifying and supervising essential services and critical information infrastructure. It establishes risk-management and incident-reporting duties, cybersecurity audits, regulatory oversight, and a framework for coordinating responses to significant incidents. The connected public-information reforms address a closely related area of digital governance: they introduce the "once only" principle for data submitted to the state (mandating single, synchronized data submission across state agencies), expand proactive publication requirements, and reorganize the management of public information. Distinguishing these elements is essential because cybersecurity

40 CyberHUB-AM, Armenia Cybersecurity Threat Landscape 2025 (April 12, 2026): <https://mdi.am/en/archives/42043>; Recorded Future News, "Armenia Probes Alleged Sale of 8 Million Government Records on Hacker Forum" (January 13, 2026): <https://therecord.media/armenia-probes-alleged-sale-government-records>.

41 International Telecommunication Union, Global Cybersecurity Index 2024 (2024): <https://www.itu.int/itu-d/reports/statistics/global-cybersecurity-index-2024/>.

42 European Union and Republic of Armenia, Strategic Agenda for the EU-Armenia Partnership (2026), pp. 13–14: <https://www.mfa.am/filemanager/%D5%80%D5%80-%D4%B5%D5%84/Strategic%20Agenda%20for%20the%20EU-Armenia%20Partnership.pdf>; European Union, Directive (EU) 2022/2555 of the European Parliament and of the Council of December 14, 2022 (NIS2): <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>; Information Systems Agency of Armenia, "Participants of the First CyberTech Sprint Were Hosted at the Agency" (February 6, 2025): <https://isaa.am/en/articles/%D5%B6%D5%B8%D6%80%D5%B8%D6%82%D5%A9%D5%B5%D5%B8%D6%82%D5%B6%D5%B6%D5%A5%D6%80/participants-of-the-first-cybertech-sprint-were-hosted-at-the-agency>.

43 Government of the Republic of Armenia, "The Government Approves Legislative Package on Cybersecurity and Public Information" (August 14, 2025): <https://www.gov.am/en/news/item/10665/>; Information Systems Agency of Armenia, "Cybersecurity and Public Information Bills Approved by Government" (August 15, 2025): <https://isaa.am/en/news/2025/08/15/cybersecurity-and-public-information-bills-approved-by-government/188>.

supervision, open data, and administrative data exchange raise different accountability and rights questions.⁴⁴

Together, the laws centralize Armenia's digital governance. Their creation of a specialized regulator for digital governance and cybersecurity may improve consistency, but it also concentrates authority over security and compliance. Transparent appointments, reporting, limits on discretion, and civil society oversight are essential.

THE CONSULTATION PROCESS: WHAT WORKED AND WHAT DID NOT

The cybersecurity legislative package was developed through several rounds of drafting and consultation from late 2023 to May 2025. The Ministry of High-Tech Industry published the final pre-adoption package on the e-draft.am platform. Parallel meetings with civil society organizations (CSOs), technical experts, and public institutions continued outside the platform. This hybrid process demonstrated that a digital consultation tool can provide public access but does not replace sustained expert and community engagement.⁴⁵

e-draft.am is Armenia's unified online platform for publishing and discussing draft legal acts. The Ministry of Justice launched it in 2017 and remains institutionally associated with its operation. Ministries use it to publish draft legislation, receive written proposals, and post summaries of consultation results. The Ministry of High-Tech Industry was the lead institution for the cybersecurity package.⁴⁶

What Worked

Early and repeated mobilization by civil society and the cybersecurity community produced concrete changes. Participants included ArmSec, the OWASP Yerevan community, CyberHUB-AM, media

organizations, the Freedom of Information Center of Armenia, the Law Development and Protection Foundation, and other legal and digital-rights specialists. Their input combined technical, freedom-of-information, privacy, and institutional-design expertise.⁴⁷

The consultation produced several substantive improvements:

- **Structural separation:** Public-data and cybersecurity rules were divided into distinct laws, allowing security obligations and information-access rights to be assessed separately.
- **Open-data safeguards:** The public-information law retained stronger proactive-disclosure and access provisions for nonclassified information.
- **A statutory civil society role:** The regulatory framework requires the authorities to cooperate with CSOs, providing a basis for implementation monitoring.
- **Freedom-of-information consistency:** Definitions, access procedures, and fees were revised to reduce conflicts with existing law.

The public record also shows the reach and the limits of the e-draft.am platform. The pre-adoption package had more than 33,000 views and generated 28 written proposals. These figures indicate high visibility but a narrow base of active participation. They are more useful than a simple count of comments because they distinguish passive access from substantive engagement.⁴⁸

What Did Not Work

The most important limitation was the concentration of meaningful participation among a relatively small group of specialists. Complex cybersecurity legislation requires technical, legal, human rights, business, and civil society analysis. The statutory maximum of

44 Republic of Armenia, Law on Cybersecurity, HO-442-N (December 4, 2025): <https://old.arlis.am/DocumentView.aspx?docID=218672>; Republic of Armenia, Law on Public Information, HO-443-N (December 4, 2025): <https://old.arlis.am/DocumentView.aspx?docID=218678>; Republic of Armenia, Law on the Information Systems Regulatory Body, HO-444-N (December 4, 2025): <https://www.arlis.am/hy/acts/218686>.

45 Ministry of High-Tech Industry of the Republic of Armenia, "Draft Laws on Cybersecurity, Public Information, and the Information Systems Regulatory Body," Project 8642, e-draft.am (2025): <https://www.e-draft.am/en/projects/8642>.

46 Ministry of Justice of the Republic of Armenia, "Unified Website for Publication of Draft Legal Acts Has Been Launched" (January 24, 2017): <https://moj.am/en/article/1708>.

47 CSO Meter, "Armenia Takes Next Steps to Improve Management of Public Information and Cybersecurity in Digital Public Services" (2025): <https://csometer.info/updates/armenia-takes-next-steps-improve-management-public-information-and-cybersecurity-digital>; CSO Meter, Armenia 2025 Country Report (March 2026): <https://csometer.info/sites/default/files/2026-03/Armenia%202025%20Country%20Report%20ENG.pdf>.

48 Ministry of High-Tech Industry of the Republic of Armenia, "Draft Laws on Cybersecurity, Public Information, and the Information Systems Regulatory Body," Project 8642, e-draft.am, project page and consultation digest: <https://www.e-draft.am/en/projects/8642>. Figures accessed July 16, 2026.

15 days for submitting a written contribution may be sufficient for narrow amendments, but it was poorly suited to a multi-law package covering regulatory institutions, incident-reporting duties, public-information rules, and critical-infrastructure governance.⁴⁹

The SIGMA program of the Organisation for Economic Co-operation and Development and the EU has found that public consultation in Armenia remains heavily dependent on e-draft.am and that other methods are used only to a limited extent. Publication on the platform should therefore be treated as the beginning of consultation, not as evidence that all affected groups have been reached. For complex legislation on digitalization, ministries should combine online publication with technical workshops, regional outreach, sector-specific meetings, and accessible explanatory materials.⁵⁰

THE CYBERSECURITY COMMUNITY AND E-DRAFT.AM AS PARTICIPATION INFRASTRUCTURE

Participation regarding the legislative package was active but narrow. CyberHUB-AM, ArmSec, and OWASP Yerevan addressed security standards and institutional design. The Freedom of Information Center of Armenia, the Law Development and Protection Foundation, Transparency International, and other rights groups focused on access, privacy, and safeguards. The American Chamber of Commerce contributed a business view. Operators, security teams, small and medium-sized enterprises, and firms outside established networks were less visible, mostly because no industry body took ownership of the issue and private firms saw little incentive to engage in a public consultation framed around rights and transparency rather than commercial compliance.

The e-draft.am platform also constrains systematic participation. It does not provide a public application programming interface (API) – a machine-readable connection that would allow CSOs, researchers, and businesses to automatically retrieve new drafts, comments, responses, and revisions. Without such a tool, organizations must repeatedly check the website, copy information manually, and build their own tracking spreadsheets. Germany's Deutsche Gesellschaft für

Internationale Zusammenarbeit reported the same concern from civil society: some CSOs must assign staff to monitor e-draft.am manually, reducing the time available for substantive analysis and advocacy.⁵¹

The platform publishes consultation summaries, but the quality and completeness of government response remain uneven. SIGMA's 2025 assessment found that five of ten sampled consultation files lacked a complete response on the platform. This makes it difficult to trace which proposal was accepted, partially accepted, or rejected and why. The problem is not only technical. A deliberative process requires a public reasoning trail, not merely proof that a draft was posted for a prescribed period.⁵²

Key changes resulted from online submissions combined with ministry meetings, coalition advocacy, public statements, and working groups. e-draft.am provided visibility and a formal record while offline engagement enabled iterative revision. The platform works better as a submission channel than as a full deliberative system.

TRUST, ACCOUNTABILITY, AND FUTURE CIVIC ENGAGEMENT

The effect of the public consultation on public trust was mixed. Civil society proposals contributed to visible changes, especially in separating cybersecurity and public-information regulation as well as in strengthening disclosure and cooperation. This showed that coordinated, evidence-based engagement can alter major legislation.

Yet trust requires visible influence. Participants must see how some proposals changed the text and why others were rejected. Incomplete responses, hard-to-compare drafts, and decisions made in closed groups make the process appear selective even when recommendations are accepted.

The burden is greatest for small organizations and groups outside Yerevan. Technical review requires expertise, time, and funding; when impact is uncertain, fatigue is a rational reaction. Broader participation will remain limited unless the government makes influence visible and reduces costs.

49 Republic of Armenia, Law on Normative Legal Acts, Article 27: <https://www.artis.am/hy/acts/152139>; OECD/SIGMA, Public Administration in Armenia 2025 (December 5, 2025), pp. 47, 49: https://www.sigmaweb.org/content/dam/sigma/en/publications/reports/2025/12/public-administration-in-armenia-2025_5c12af02/f996600c-en.pdf.

50 OECD/SIGMA, Public Administration in Armenia 2025, p. 48.

51 Written feedback from Deutsche Gesellschaft für Internationale Zusammenarbeit communicated during editorial review, June 2026.

52 OECD/SIGMA, Public Administration in Armenia 2025, p. 49.

Figure 1: From Formal Consultation To Deliberative Participation

Current Model	Passive Posting	15-Day Window	Incomplete or Opaque Response	Adoption
Proposed Hybrid Model	Co-Design	Active e-Draft	Public Response Matrix	Post-Adoption Monitoring

Source: Own compilation

IMPLICATIONS FOR AI AND DIGITAL GOVERNANCE

The 2025 laws did not create a dedicated AI regulator but they set requirements regarding standards, audits, data flows, incident reporting, and accountability. These may shape the governance of automated public services and algorithmic decisions, but a cybersecurity law cannot replace a dedicated AI framework.

AI legislation will require broader participation because it affects institutions, businesses, communities, and people subject to automated decisions. The procedural lesson is clear: influence begins before the publication of drafts, continues through traceable consultation, and requires independent monitoring after adoption.

AI may be used to cluster or summarize public feedback. This could reduce workload, but without disclosure and human review it may also flatten arguments, reproduce errors, or favor frequently repeated views over well-supported minority positions. Processing should be transparent, auditable, and subject to human decisions with related accountability.

CONCLUSION AND RECOMMENDATIONS

The case of Armenia’s legislative package demonstrates the value of organized expertise and the limits of consultation centered on publication compliance. Hybrid advocacy secured meaningful changes

but participation remained narrow, feedback uneven, and monitoring costly. Implementation and future AI reforms offer a chance to build a more inclusive and traceable system.

For EU and German policy-makers and development partners

- **Use EU benchmarks selectively:** Apply NIS2 principles to coverage, risk management, incident reporting, supervision, and safeguards, while adapting support to Armenia’s capacity and threat environment.
- **Invest in participation infrastructure:** Support an open API, automated alerts, version-comparison tools, and a mandatory public-response matrix for e-draft.am.
- **Broaden participation:** Fund regional engagement and sustained input from operators, security teams, small and medium-sized enterprises, journalists, and rights CSOs.
- **Tie assistance to accountability:** Set indicators for consultation quality, regulatory independence, implementation reporting, and civil society access.

For Armenian authorities

- **Make decisions traceable:** Publish a response matrix explaining acceptance or rejection and tracked versions of each draft.
- **Allow more time:** Provide at least 30 days for complex cybersecurity, data, digital-rights, and AI packages.

-
- **Use parallel formats:** Combine e-draft.am with workshops, sectoral meetings, regional outreach, and plain-language materials, and publish offline input.
 - **Operationalize oversight:** Define regulator-CSO cooperation, publish implementation data where security permits, and safeguard independence of civil society.
 - **Open consultation data:** Provide machine-readable drafts, comments, responses, deadlines, and version histories.

For civil society organizations

- **Engage early:** Participate during concept development, when ministries can still revise institutional choices and legal architecture.
- **Maintain a tech-civic coalition:** Combine legal, rights, technical, business, and sectoral expertise to monitor implementation and AI reforms.
- **Expand capacity:** Translate technical concepts into accessible materials and support CSOs outside Yerevan.
- **Preserve evidence:** Archive drafts, submissions, responses, meetings, and implementation decisions, and publish shadow reports.

Closing the gap between formal procedure and impact is essential to public trust, regulatory legitimacy, and democratic digital transformation.



Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 254231-0
info@dgap.org
www.dgap.org
[in](#) @dgapev

The German Council on Foreign Relations (DGAP) is committed to fostering impactful foreign and security policy on a German and European level that promotes democracy, peace, and the rule of law. It is nonpartisan and nonprofit. The opinions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the German Council on Foreign Relations (DGAP).

DGAP receives funding from the German Federal Foreign Office based on a resolution of the German Bundestag.

Publisher

Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2198-5936

Editing Nicolas Bouchet

Layout Luise Rombach

Design Concept WeDo

Author photo(s) © DGAP



This work is licensed under a Creative Commons
Attribution – NonCommercial – NoDerivatives 4.0
International License.

The publication was supported by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH.

The opinions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the German Council on Foreign Relations (DGAP) or the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH.