
Monitoring Kosovo's Digital Agenda 2030

Progress, gaps and the roadmap
towards digital alignment with the EU

Monitoring Kosovo's Digital Agenda 2030

Progress, gaps and the roadmap towards digital alignment with the EU

Publisher: Institute for Technology and Society (ITS)

Authors: Lirim Bllaca & Atdhe Lila

Prishtina, September 2026

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means—electronic, mechanical, photocopying, recording or otherwise—without the prior written permission of the Institute for Technology and Society (ITS), except for brief quotations used for analysis, criticism or review.

This report was prepared as part of the “Digital Agenda” project, supported by Open Society Foundations – Western Balkans (OSF-WB).

The views and opinions expressed in this report are those of the Institute for Technology and Society (ITS) and do not necessarily reflect the views or opinions of Open Society Foundations – Western Balkans (OSF-WB).

Executive summary

This report examines Kosovo's progress in implementing the Digital Agenda of Kosovo 2030 (DAK 2030) and the further action needed to align its digital transformation with the European Union's Digital Decade Policy Programme 2030. Prepared by the Institute for Technology and Society (ITS), the report combines published data and statistics with interviews, written questions to public institutions, private organisations and civil society, and a stakeholder workshop on preliminary findings.

The findings indicate that Kosovo has made clear progress in digital connectivity, online public services and support for innovation. The next stage of DAK 2030 depends on turning these investments into reliable services, wider business adoption and stronger institutional capacity. Coordination, sustained financing and consistent measurement remain central to achieving the agenda's objectives.

The implementation assessment covers 62 indicators and milestones. Of these, 20 are classified as achieved, 9 as mostly achieved, 13 as partially achieved and 4 as not achieved. Ten lack sufficient data, while six have no target. These figures do not constitute an overall implementation percentage: some indicators overlap, some rely on proxies, and two positive classifications reflect a 2025 target explicitly set at "No".

Connectivity is the most advanced area, with ten of its 15 indicators classified as achieved. Business digitalisation is less widespread, particularly among traditional SMEs. The expansion of e-Kosova and technical work on electronic identity provide foundations for digital government, but service availability still exceeds the ability to complete procedures entirely online. Digital skills figures require careful interpretation, including the large difference between estimates from the Kosovo Agency of Statistics and Western Balkans DESI. Advanced skills and research funding remain weaker. Progress in cybersecurity is constrained by operational capacity and the lack of regular data.

The European framework has become more specific since DAK was adopted in 2023. Developments in AI, data governance, platforms, digital identity, interoperability and cyber resilience affect the capacity Kosovo needs to implement its existing objectives. Legal approximation must be accompanied by practical supervisory, technical and administrative capability. EU rules and programme participation do not automatically create identical domestic obligations or access rights for Kosovo.

The priorities through 2030 are to restore regular coordination and public reporting, assign clear responsibilities, fund systems throughout their lifecycle, and measure outcomes for users and businesses. Practical SME support, specialist skills, secure and interoperable services, and a harmonised indicator framework should guide the next implementation period. The agenda's five objectives remain relevant; delivery arrangements need to become more consistent and accountable.

Contents

Executive summary	5
Chapter 1 Introduction	7
The project and its purpose	7
Project objectives and expected contribution	7
The Digital Agenda of Kosovo 2030	7
Research and stakeholder consultation	7
Scope and interpretation of the evidence	8
Structure of the report	8
Chapter 2 Implementation progress and achievement of objectives	9
Development of the implementation framework	9
Assessment method and overview of progress	9
Advanced and secure digital infrastructure	10
Digital transformation of businesses	12
Digital public services	13
Digital skills education and research	15
The cybersecurity ecosystem	17
Main implementation challenges	18
Chapter 3 The changing European digital framework and Kosovo's Digital Agenda 2030	20
Purpose and European context	20
How European digital policy is organised	20
What has changed since 2023	21
AI data markets privacy and intellectual property	22
Interoperable public services identity and health	23
Cyber resilience and digital infrastructure	24
Skills inclusion and trust	25
Kosovo European and regional integration	26
Conclusion	27
Chapter 4 Recommendations for implementing and updating DAK 2030	29
4.1 Improving governance and accountability	29
4.2 Mandatory measurement and publication of all indicators	29
4.3 Filling gaps in targets and objectives	30
4.4 Linking funding to results	31
4.5 Proposed additional indicators for 2030	32
4.6 Legal approximation and sequencing of actions	33
References	35

Chapter 1 Introduction

The project and its purpose

This report is an output of the project Monitoring Kosovo's Digital Agenda 2030: Progress, Gaps, and the Roadmap towards Digital Alignment with the EU, implemented by the Institute for Technology and Society (ITS). The project is supported and funded by the Open Society Foundations (OSF) and implemented with the support of the Ministry of Economy of the Republic of Kosovo. It examines how far Kosovo has advanced in implementing DAK 2030 and what further action is needed to align its digital transformation with the European Union's Digital Decade Policy Programme 2030.

Project objectives and expected contribution

The project has five connected objectives: assess progress across DAK's five strategic areas; compare Kosovo's approach with EU and Western Balkan frameworks; identify policy, legal and institutional gaps; develop evidence-based recommendations; and strengthen cooperation among the actors responsible for digital transformation. Its wider purpose is to support an inclusive, efficient and rights-based digital transition connected to Kosovo's European integration pathway.

The work is organized into desk research and data collection, comparative and regulatory analysis, stakeholder consultation, and policy outputs and dissemination. This methodology provides a comprehensive progress and alignment report and a concise policy brief, supported by communication materials. This report brings together the implementation assessment and the analysis of the evolving European framework.

The Digital Agenda of Kosovo 2030

DAK 2030 is Kosovo's cross-sector strategy for the digital transformation of the economy and society. The Ministry of Economy prepared and proposed it following public consultation and discussions with the information and communication technology sector. The Government adopted it in June 2023. Its direction reflects national development priorities and the European Digital Compass 2030 and related EU policies. [1, 2]

The agenda sets out five strategic objectives. Advanced and secure digital infrastructure concerns high-capacity connectivity and its use. Business digitalisation focuses on adoption of digital technologies and stronger ICT capacity. Digital public services concern accessible online procedures, electronic identity and a capable administration. Digital skills, education and research support participation, specialist competence and innovation. The cybersecurity objective seeks a sustainable ecosystem able to protect users, organisations and essential digital systems. [1]

These objectives depend on one another. Reliable connectivity supports services and enterprise adoption; identity and interoperable registers enable transactions; skills allow people and organisations to use technology effectively; and security and data protection sustain trust. Annex I provides the indicators and, for most of them, intermediate targets for 2025 and final targets for 2030. These form the basis for the implementation assessment in Chapter 2. [1]

Research and stakeholder consultation

During this project, we reviewed DAK 2030, relevant strategies and policy documents, published progress reports and available statistical series. The analysis used data from the Kosovo Agency of Statistics (ASK), Eurostat, regulatory bodies and international and regional organisations. Sources include the European Commission, the Regional Cooperation Council, UNDP and the World Bank.

We compared findings from different sources, distinguishing the period measured from the publication date of the report or response.

We conducted interviews and sent written questions to public institutions, private organisations, NGOs and other organisations involved in Kosovo's digital transformation. Contacts included the Ministry of Economy, the Office of the Prime Minister, the Kosovo Investment and Enterprise Support Agency (KIESA), the Regulatory Authority of Electronic and Postal Communications, the Innovation and Training Park (ITP) Prizren, Venture UP and STIKK, alongside institutions responsible for infrastructure, public administration, education, innovation and cybersecurity. The questions sought information on implementation, results, barriers, institutional responsibilities and priorities. Responses and interview findings informed the assessment where relevant evidence was available. [3, 4, 5, 6, 7, 8]

On 10 September 2026, we held a workshop with stakeholders from the public sector, private sector, civil society and the wider innovation ecosystem to discuss preliminary findings. Participants considered implementation progress, coordination challenges and priorities for the remaining strategy period. Their contributions helped interpret the evidence and identify matters requiring further clarification. Workshop views are treated as qualitative evidence and distinguished from verified statistical measurements and formal institutional decisions. [9]

Scope and interpretation of the evidence

The implementation assessment covers 62 indicator and milestone rows in Annex I and reviews progress primarily against the 2025 targets. Chapter 2 incorporates evidence collected through 16 September 2026, with supplementary clarifications incorporated on 29 September 2026. Its underlying observations mainly concern 2023–2026. Chapter 3 retains a separate policy-review cutoff of 9 September 2026. A publication date or an institutional response date is not necessarily the date on which the reported outcome was measured.

Where a directly comparable measurement is unavailable, the report identifies proxies, qualitative assessments and limitations. Although the use of proxies was discussed and validated by stakeholders, these findings should be interpreted cautiously because they provide a limited representation of reality. Moreover, the absence of a measurement does not demonstrate that no work has been done; an adopted law, completed platform or training participation figure does not by itself demonstrate effective use or competence. The classification rules and exceptions are explained in Chapter 2. The counts describe the evidence for individual indicators and should not be interpreted as a single percentage of DAK implementation.

Structure of the report

The report opens with the executive summary. Chapter 1 presents the project, the objectives of DAK 2030 and the methodology. Chapter 2 assesses implementation and achievement of the objectives. Chapter 3 analyses the EU digital framework and its relevance to Kosovo. Chapter 4 sets out recommendations on governance, indicators, funding and legal approximation. The references are consolidated at the end.

Chapter 2 Implementation progress and achievement of objectives

The assessment identifies clear progress in connectivity, the expansion of e-Kosova and the development of innovation mechanisms. Governance weaknesses, institutional changes, limited research funding and gaps in end-to-end services, digital identity and cybersecurity continue to constrain progress. This chapter reviews implementation against the 2025 targets and identifies priorities for the remaining period to 2030.

Development of the implementation framework

Table 1 Implementation milestones

Period	Development	Implementation significance
June 2023	DAK 2030 adopted after preparation by the Ministry of Economy and stakeholder consultation.	A common framework with five strategic objectives is established.
2023–2024	e-Kosova expands; investment continues in connectivity, KODE/KREN and electronic identity.	Core components of digital government are developed and extended.
2025	DIG-4K, part of ITP Prizren, joins the European Digital Innovation Hubs network; e-Kosova reportedly offers around 230 services; 5G coverage expands.	Infrastructure progress needs to translate into measurable use and benefits.
2025–2026	The electronic identification system is in its final stage; launch is expected before the end of 2026. [78]	Technical completion and nationwide use need separate assessment.
September 2026	The assessment includes institutional responses, the 10 September discussion, the 16 September Eurostat check and supplementary clarifications received on 29 September. [78]	Governance, quality, security and harmonised measurement become priorities through 2030.

The chronology summarises key developments and does not replace measurement of the indicators.

Assessment method and overview of progress

The assessment covers 62 indicator and milestone rows in Annex I. ITS classified them using official sources, harmonised statistics, external reports and institutional responses collected through 16 September 2026, with supplementary clarifications incorporated on 29 September 2026. Sources cover different periods, mainly 2023–2026; publication and response dates are distinguished from measurement dates. [1, 78]

Table 2 Classification of indicators and milestones

Assessment	Classification rule	Count
Achieved	100% or more of the target	20
Mostly achieved	Above 50% and below 100%	9
Partially achieved	20% to 50%	13
Not achieved	Below 20%	4
Insufficient data	A target exists but an appropriate measurement is unavailable	10

Assessment	Classification rule	Count
No target in DAK 2030	Neither a 2025 nor a 2030 target in Annex I	6
Total		62

Distribution by strategic objective

Table 3 Assessment by strategic objective

Area	Achieved	Mostly	Partially	Not achieved	No data	No target	Total
Infrastructure	10	0	3	2	0	0	15
Businesses	2	1	3	0	2	0	8
Public services	1	6	1	1	1	1	11
Skills and research	4	1	3	1	0	3	12
Cybersecurity	2	1	3	0	7	2	15
Infrastructure atlas	1	0	0	0	0	0	1
Total	20	9	13	4	10	6	62

How to read the tables

‘Mostly’ and ‘Partially’ in the detailed tables abbreviate the full classifications above. ‘No data’ means insufficient data, not necessarily an absence of activity. An asterisk (*) identifies a proxy, qualitative judgement or methodological exception. Notes explain where a measurement differs from the DAK indicator.

Rows have equal weight in this count and some overlap. Their distribution is therefore not an overall percentage of agenda implementation. Indicators without targets are not treated as objectives with a value of zero. Percentage thresholds apply where a comparable quantitative measure is available; binary milestones and proxy-based judgements require the accompanying interpretation.

Advanced and secure digital infrastructure

The objective seeks high-capacity fixed and mobile connectivity, coverage in underserved areas and secure use of infrastructure. Of the 15 indicators in this area, 10 are achieved, 3 partially achieved and 2 not achieved. This is the area with the largest number of achieved indicators.

Connectivity coverage and spectrum

Table 4 Connectivity coverage and spectrum indicators

Indicator	2025 target	Evidence and interpretation	Assessment
SO1.1 Households covered by networks capable of 1 Gbps	30%	42% VHCN coverage according to ARKEP; this is not the share of 1 Gbps subscriptions. [3]	Achieved
SO1.2 5G coverage of populated areas	50%	70% of the population in 2024; ARKEP’s latest response: 75%. [3, 10]	Achieved
SO1.1.1 Public programmes for commercially unattractive areas	5	At least one verified programme, KODE; a minimum of 20% of the target*. [11, 12]	Partially*

Indicator	2025 target	Evidence and interpretation	Assessment
SO1.1.2 5G spectrum allocation policy and strategy	Yes	ARKEP confirms adoption of the Frequency Release Plan. [3]	Achieved
SO1.1.3 Available spectrum in 5G pioneer bands	70%	16.7% in 2024, or 23.9% of the target. ARKEP did not provide an updated percentage. [3, 13]	Partially
SO1.1.4 NGA/VHCN territorial coverage	80%	ARKEP confirms coverage of at least 80%, without an exact percentage. [3]	Achieved
SO1.1.5 5G territorial coverage in rural and urban areas	30%	75% of the territory according to the Commission's Kosovo Report 2025. [3, 10]	Achieved
SO1.1.6 Fixed subscriptions at speeds of at least 100 Mbps	70%	83.8% in 2024; ARKEP currently reports over 85%. [3, 13]	Achieved

Household VHCN coverage, population coverage by 5G and territorial coverage measure different things. Their percentages are not interchangeable. Similarly, the availability of a network capable of 1 Gbps does not mean that every covered household subscribes at that speed.

KODE and KREN have supported connectivity in underserved areas, schools and research institutions. The verified evidence identifies one major public programme; the number of beneficiary villages or institutions cannot be counted as the number of programmes. [11, 12, 14]

During the roundtable, stakeholders noted that while Kosovo has high internet coverage, it suffers from slow speeds and frequent coverage gaps in supposedly connected areas.

Advanced network uses

Alongside wider coverage, at least two private 5G networks have been identified: at the University for Business and Technology (UBT) and the Next Gen Networks Institute. The two-network target for SO1.3.1 is therefore assessed as achieved. These networks create opportunities for research, testing and skills development; wider enterprise use requires further monitoring. [78, 79, 80]

Table 5 Advanced network uses and the infrastructure atlas

Indicator	2025 target	Evidence and interpretation	Assessment
SO1.2.1 Implementation of EU 5G security toolbox measures	All	ARKEP Regulation No. 68 represents progress; full implementation of the toolbox is not demonstrated*. [3, 15]	Partially*
SO1.2.2 Rules for cross-sector infrastructure sharing	Yes	A regulatory framework is in force; practical implementation remains incomplete*. [3]	Achieved*
SO1.3.1 Private 5G networks	2	At least 2 private 5G networks: UBT and Next Gen Networks Institute; the target of 2 networks is achieved. [78, 79, 80]	Achieved

Indicator	2025 target	Evidence and interpretation	Assessment
SO1.3.2 5G network slicing models for enterprises	1	Zero models; ARKEP confirms that the service is not offered. [3]	Not achieved
SO1.4.1 5G network for public protection and disaster relief	No	The intermediate target itself was “No”; this status does not demonstrate creation of the network*. [1]	Achieved*
SO1.4.2 5G-based smart city solutions	2	At least two projects identified; a project does not necessarily constitute an operational solution*. [16]	Achieved*
SO1.4.3 Participation in EU cross-border 5G corridors	Yes	Kosovo is not part of such a corridor according to project evidence. [16]	Not achieved
M-2025 Digital atlas of fixed infrastructure	Yes	The atlas exists and contains basic infrastructure information; the creation milestone is assessed as achieved. [16, 78]	Achieved

The M-2025 infrastructure atlas milestone is counted separately from the 15 SO1 indicators. It appears as a cross-cutting row in the overview table. For PPDR, ‘Achieved*’ reflects the wording of the 2025 target (‘No’) and does not indicate a positive infrastructure achievement.

Assessment of the objective

Strengths include near-universal internet access — ASK reports that 99.3% of households had internet access in 2025 — alongside VHCN coverage, fixed broadband speeds, 5G expansion, two private 5G networks and the creation of the atlas. Challenges include uneven service quality, the absence of network slicing and non-participation in EU cross-border 5G corridors. Monitoring through 2030 should address actual speed, stability, latency, affordability, productive use and updates to the atlas. [17, 3, 9, 16, 78, 79, 80]

Digital transformation of businesses

This objective seeks wider adoption of digital technologies, higher digital intensity among SMEs and stronger ICT capacity. The assessment includes two achieved indicators, one mostly achieved, three partially achieved and two with insufficient data.

Table 6 Business digitalisation indicators

Indicator	2025 target	Evidence and interpretation	Assessment
SO2.1 Enterprises using cloud, big data and AI	30%	The combined indicator of 6.7% is used as a proxy, equivalent to 22.3% of the target*. [13]	Partially*
SO2.2 SMEs with at least basic digital intensity	60%	14.3% in 2024, or 23.8% of the target. [13]	Partially
SO2.1.1 Digital innovation hub	Created	DIG-4K, part of ITP Prizren, is Kosovo’s first European Digital Innovation Hub. [18, 19]	Achieved
SO2.2.1 Employed people with specialist ICT skills	20,000	Approximately 7,461, estimated as $1.8\% \times 414,493$ employed people; 37.3% of the target. [13, 20]	Partially

Indicator	2025 target	Evidence and interpretation	Assessment
SO2.2.2 Enterprises providing ICT training for staff	20%	13.6% according to WB DESI 2025, or 68% of the target. [13]	Mostly
SO2.3.2 Enterprises with high digital intensity	20%	No comparable national measurement is available for this level of intensity. [21, 17]	No data
SO2.3.3 Enterprises analysing big data	20%	32.4% used data analytics in 2023, according to WB DESI. [13] This is a proxy figure as there are no data for enterprises analysing big data.	Achieved*
SO2.3.4 Support for new technology adoption by ICT companies	20%	Programmes and beneficiaries identified; the required national denominator is unavailable. [4, 21, 17]	No data

DIG-4K, as part of ITP Prizren, supports businesses and public organisations in digital transformation through an approach based on their needs. This support includes assessing digital maturity, identifying needs, developing digitalisation strategies and providing services for technology testing, skills development and access to finance. Digital maturity assessment (DMA) is the starting point of this wider support process. The dataset used in the analysis contains 43 initial assessments (pre-phase assessments), conducted before interventions and services were delivered: the average score is 41.67/100, while the average for automation and AI is 20.28/100. Further assessments will be conducted during implementation and after services have been received, enabling comparisons of progress and changes in digital maturity. These data should be read as a baseline picture of the sample, not as results following interventions; they are not representative of all businesses in Kosovo. [22]

Assessment of the objective

Strengths include an active ICT sector, ITP Prizren with DIG-4K as part of it, and STIKK programmes providing training, mentoring and access to finance. Weaknesses include the slow spread of digital transformation among traditional SMEs and the lack of national measurements of high digital intensity and advanced technology use. The priority through 2030 should be practical support for enterprises and measurement of its effects on productivity, security and market access. [18, 19, 4]

Digital public services

This objective concerns accessible services that can be completed online, digital identity and a capable administration. Of its 11 indicators, one is achieved, six mostly achieved, one partially achieved, one not achieved, one has insufficient data and one has no target.

Table 7 Digital public service indicators

Indicator	2025 target	Evidence and interpretation	Assessment
SO3.1 Key public services provided online	50%	230/700 $\approx$ 32.9% as a proxy, or 65.8% of the target. The catalogue is broader than key services*. [11, 23]	Mostly*
SO3.2 Citizens with access to electronic health records	50%	The DESI score of 37/100 is used as a proxy; it is not a percentage of citizens*. [13]	Mostly*

Indicator	2025 target	Evidence and interpretation	Assessment
SO3.3 Citizens using digital identity	30%	The system is in its final stage; launch is expected before the end of 2026. Active use against the 30% target is not yet measured*. [24, 25, 78]	Not achieved*
SO3.1.1 Improvement of digital services for citizens	60%	DESI 50/100, or 83.3% of the target as a proxy, not a measure of increased service provision*. [13]	Mostly*
SO3.1.2 Improvement of digital services for businesses	70%	DESI 62/100, or 88.6% of the target as a proxy, not a measure of increased service provision*. [13]	Mostly*
SO3.2.1 Open data	Yes	A national portal exists; 2025 monitoring identifies 205 datasets from 14 organisations. [26]	Achieved
SO3.2.2 Completion of services entirely online	45%	Around 10% according to WB DESI, or 22.2% of the target. [13]	Partially
SO3.3.1 Online submission of completed forms	35%	ASK: 30.8% download or print forms; this activity is used as a proxy*. [17]	Mostly*
SO3.3.2 Online interaction with public authorities	60%	ASK 2025: 33% of people aged 16–74 interacted online with public authorities; 55% of the 60% target. [27]	Mostly
SO3.4.1 Public employees with basic digital skills	55%	IKAP: 387 attendances and 384 certifications; competence measurement and a denominator are missing. [5]	No data
SO3.4.2 Public employees with advanced digital skills	No target	Annex I sets no target for 2025 or 2030. [1]	No target

For interaction with public authorities, the final Eurostat check using ASK data gives a figure of 33% for Kosovo in 2025, covering people aged 16–74 who used the internet to interact with public authorities. This is the closest harmonised measurement to the wording of DAK. A result of 33% against a target of 60% represents 55% of the target and is classified as “Mostly achieved”. The broader figure of 69.17% for the use of e-government services is retained only as context because its definition differs.

Other proxies retain their limitations: DESI scores are not percentages of citizens or increases in service provision; downloading a form is not online submission; and the ratio 230/700 does not measure completion of a procedure. The eID classification is a qualitative assessment of implementation and uptake, rather than a measured national usage percentage.

Electronic identity and administrative skills

From the technical platform to sustained use

The electronic identification system is in its final stage and is expected to launch before the end of 2026, according to supplementary clarifications for the report. The Ministry of Economy announced the start of piloting in November 2025; the 2026 concept document addresses further legal and institutional harmonisation. This progress does not yet establish the share of citizens actively using eID. SO3.3 therefore retains its qualitative assessment against the uptake target, rather than an assessment of system completion. [24, 25, 78]

Article 32 of Law No. 08/L-022 on Electronic Identification and Trust Services in Electronic Transactions provides that an electronic signature cannot be denied validity or evidential weight solely because it is electronic or does not meet the requirements for a qualified signature. A qualified electronic signature has the same legal effect as a handwritten signature. The Ministry of Economy lists two licensed providers of electronic signatures, electronic seals and website authentication certificates: PBC Sh.P.K. (rTrust) and Evrotrust Technologies JSC & IT Vision. Services from providers authorised in the EU may be used in Kosovo subject to the law's conditions for the relevant service; Articles 33, 41 and 58 address the recognition and use of services from abroad. The priority is practical integration and use in procedures, alongside measurement of completed transactions. [81, 82]

Evidence from IKAP training

Table 8 Public administration training reported by IKAP

Training	Courses	Attendances	Certifications
SPSS	1	16	16
PowerPoint and Outlook	1	12	12
Visio and Publisher	1	55	55
Cyber hygiene	1	158	157
Excel	1	59	59
Artificial intelligence	1	57	56
WordPress	1	12	12
Project	1	18	17
Total	8	387	384 [5]

The Moodle course on cybersecurity fundamentals separately reports 1,980 invitees, 220 starters and 149 completions. Attendance figures in the table do not necessarily represent unique individuals and do not establish the share of all public employees with basic competence. [5]

Assessment of the objective

Strengths include the expansion of e-Kosova, increased use of online public services, the final stage of the eID system and the existence of a legal framework and licensed trust-service providers. Challenges remain in completing procedures entirely online, integrating eID and electronic signatures in practice, and measuring uptake and digital competence across the administration. Service development should be measured through actual transactions, avoided visits, time saved and user experience. [11, 27, 24, 25, 5, 78, 81, 82]

Digital skills education and research

This area connects population skills with ICT specialists, education, research and innovative technologies. Of its 12 indicators, four are achieved, one mostly achieved, three partially achieved, one not achieved and three have no target.

Table 9 Digital skills education and research indicators

Indicator	2025 target	Evidence and interpretation	Assessment
SO4.1 Adults with at least basic digital skills	40%	ASK: 76% of people aged 16–74 in 2025; 190% of the target. This differs from the WB DESI figure of 37.7%. [28]	Achieved*

Indicator	2025 target	Evidence and interpretation	Assessment
SO4.2 Growth in ICT specialists and gender convergence	4,000	The estimate of approximately 7,461 is used for the numerical target; gender convergence is not measured*. [13, 20]	Achieved*
SO4.1.1 Above-basic digital skills	25%	9.8% in 2025, or 39.2% of the target. [13]	Partially
SO4.1.2 At least basic digital skills	40%	ASK: 76% in 2025; *the same evidence as SO4.1. Discrepancy with WB DESI.	Achieved*
SO4.2.1 Science and technology graduates	No target	Annex I sets no target for 2025 or 2030. [1]	No target
SO4.2.2 STEM graduates	No target	Annex I sets no target for 2025 or 2030. [1]	No target
SO4.2.3 ICT specialists as a share of employment	3.5%	1.8% in 2024, or 51.4% of the target. [13]	Mostly
SO4.3.1 Programmes in innovative technologies	2	The Ministry of Education and Science (MASH) identifies more than two accredited programmes in AI, cloud, cybersecurity and related fields. [6]	Achieved
SO4.4.1 National AI strategy	100%	No national strategy has been adopted, according to project confirmation. [9]	Not achieved
SO4.4.2 Legal framework for the innovative ecosystem	100%	The Ministry of Economy reports two of eight listed instruments, or 25%; terminology and scope require clarification. [7]	Partially
SO4.5.1 ICT business expenditure on research and development	No target	Annex I sets no target for 2025 or 2030. [1]	No target
SO4.5.2 Public expenditure on ICT research	€1.5m	General R&I allocation: €1.05m, below the €1.5m target for ICT research. Around 60% was spent (approximately €0.63m, or 42% of the target as a proxy). The ICT-specific amount is not established*. [29]	Partially*

For SO4.4.2, ‘two of eight’ is a Ministry of Economy statement and does not establish full legal alignment. The list contains terms requiring clarification. For SO4.5.2, the general research and innovation allocation is not actual ICT-specific research expenditure. The partial classification reflects incomplete execution of a general allocation below the target; it is not a verified measurement of ICT-specific research spending.

Assessment of the objective

ASK reports that 76% of people aged 16–74 had at least basic digital skills in 2025, exceeding the 40% target. This differs substantially from the estimate of 37.7% in Western Balkans DESI 2025. Above-basic skills and research funding remain considerably weaker. [28, 13]

The cybersecurity ecosystem

This objective covers harm, user behaviour, business practices and institutional capacity. The assessment identifies two achieved indicators, one mostly achieved, three partially achieved, seven with insufficient data and two with no target.

Table 10 Cybersecurity indicators

Indicator	2025 target	Evidence and interpretation	Assessment
SO5.1 Main provisions of the EU Cybersecurity Strategy	50%	8/14 implementing acts =57.1%, used as a proxy; this does not directly measure the EU strategy's provisions*. [30, 10]	Achieved*
SO5.1.1 Individuals suffering financial losses from cyber incidents	0.3%	No new comparable national measurement. [21, 17]	No data
SO5.1.2 Misuse of personal data or privacy violations	No target	No 2025 or 2030 target in Annex I. [1]	No target
SO5.1.3 Computer infections causing loss of data or time	7.5%	No new comparable national measurement. [21, 17]	No data
SO5.1.4 Avoiding online purchases for security reasons	37%	No new comparable national measurement. [21, 17]	No data
SO5.1.5 Awareness that cookies can track online activity	55%	No new comparable national measurement. [21, 17]	No data
SO5.1.6 Use of anti-tracking software	25%	ASK reports 6.75%, equivalent to 27% of the 25% target. [77]	Partially
SO5.1.7 Refusal of personal data use for advertising	No target	No 2025 or 2030 target in Annex I. [1]	No target
SO5.1.8 Enterprises advertising by geolocation	15%	No new comparable national measurement. [21, 17]	No data
SO5.1.9 Enterprises tracking users for targeted advertising	25%	No new comparable national measurement. [21, 17]	No data
SO5.1.10 Enterprises with a formal ICT security policy	45%	No comparable national percentage. [21, 17]	No data
SO5.2.1 Cybersecurity awareness programmes	5	At least two identifiable IKAP offerings; a minimum 40% proxy*. [5]	Partially*
SO5.3.1 Public protection and disaster relief network	No	The 2025 target was "No"; this status does not demonstrate construction of the network*. [1]	Achieved*
SO5.4.1 Implementation of the cybersecurity regulatory framework	Yes	Commission 2025: eight of 14 implementing acts, or 57.1%. Operational institutional capacity remained necessary. [10, 30]	Mostly

Indicator	2025 target	Evidence and interpretation	Assessment
SO5.4.2 Implementation of the international security risk assessment standard	Yes	Preparatory and risk management measures; implementation of the required standard is not confirmed*. [30, 10]	Partially*

Assessment of the objective

Strengths include the Cybersecurity Law, some implementing acts, CERT and initial training activities. Weaknesses concern operational capacity, staffing and funding: workshop participants considered that cybersecurity structures still lacked the capacity required for full implementation. The absence of regular data on incidents and business security practices makes progress difficult to measure. [30, 10, 5, 9]

Main implementation challenges

Progress in individual components does not automatically secure shared outcomes. The assessment identifies six challenges that require a coordinated response during the remaining DAK 2030 period. [9, 14]

Dispersed responsibility and coordination

The implementation evidence and the 10 September discussion describe unclear mandates, irregular coordination and a lack of detailed public reporting. DAK spans multiple institutions; without central responsibility, dependencies among identity, registers, services, education and security may remain unresolved. Participants' views constitute qualitative evidence and should be connected to documented institutional decisions. [9, 14]

Continuity and financing throughout the lifecycle

Projects require maintenance, updates, support and staff beyond initial funding. The institutional changes and instability described in the implementation evidence threaten continuity. Investment in platforms, identity and security should be accompanied by stable responsibilities, multi-year funding, and handover and maintenance plans. [9, 14]

From system creation to functional services

Around 230 services on e-Kosova do not demonstrate that most procedures can be completed online. Similarly, a technical eID platform, licensed trust service providers and a cybersecurity law do not establish widespread use or operational readiness. Measurement should cover transactions, institutional acceptance, service time, accessibility and recovery after disruption. [11, 23, 24, 25]

Human capacity and the distribution of benefits

According to Eurostat's harmonised measurement, based on ASK data, at least basic digital skills exceed the 2025 target, but above-basic skills remain substantially lower, and there is a large discrepancy between Eurostat and WB DESI for the basic level. SMEs also have limited digital intensity. Training participation does not automatically provide a measure of competence; support should be linked to employees' specific tasks, enterprise productivity and access for groups that need assistance. [28, 13, 4, 5]

Data and the quality of the indicator framework

Ten rows lack sufficient data and six have no target. Some headline and detailed indicators overlap; different numerical targets are used for ICT specialists. Proxies support monitoring, but differences in population, period and definition limit the conclusions. Measurements of harm and actual practices are particularly lacking in cybersecurity. [1, 21, 17]

Legal approximation and responsible use of technology

Adoption of legislation should be accompanied by implementation, oversight and technical capability. AI requires clarity on use cases, sensitive data, procurement, human oversight and responsibility for errors. Intellectual property, licensing and copyright should be linked to innovation support. Chapter 3 examines the relationship between these issues and EU developments. [7, 30, 10, 9]

Chapter 3 The changing European digital framework and Kosovo's Digital Agenda 2030

Purpose and European context

Kosovo adopted its Digital Agenda 2030 in 2023 as the main policy framework for digital infrastructure, business digitalisation, public services, skills and cybersecurity. Its broad objectives remain relevant. The setting in which they must be implemented, however, has changed substantially. In the intervening period, the European Union has adopted or begun applying major rules on artificial intelligence, data, online platforms, digital identity, interoperability, health data, cybersecurity and infrastructure. It has also linked digital policy more closely to competitiveness, investment and technological dependence. [1]

This chapter explains how that European framework now operates, what has changed since DAK was prepared and why those changes matter for its implementation through 2030. It does not assess every activity undertaken under DAK, nor does it assume that each EU initiative requires a corresponding Kosovo institution or law. The concern is whether Kosovo's existing priorities, governance arrangements and implementation capacity can respond to a more detailed and more demanding European policy environment.

EU regulations do not become Kosovo domestic law automatically. Their relevance arises through approximation, economic relations with the EU market, programme participation and Kosovo's wider European integration process. Directives may require transposition as part of approximation with the *acquis*. In both cases, formal legal alignment is only one part of implementation. Regulators, public bodies and businesses also need the authority, skills, systems and resources to apply the rules in practice.

How European digital policy is organised

There is no single EU document that serves as a direct counterpart to DAK 2030. European digital policy is organised through several connected layers. The Digital Decade Policy Programme provides the common direction. It sets targets for 2030 in skills, infrastructure, business and public services, while requiring national roadmaps, annual monitoring and cooperation on projects that no single country can readily deliver alone. The programme is due for review in 2027, and the Commission's 2026 assessment reports continuing fragmentation and uneven implementation across the Union. [31, 32]

A second layer consists of binding legislation. Regulations such as the AI Act, the Digital Services Act, the Digital Markets Act, the Data Act, the revised European digital identity framework and the Interoperable Europe Act allocate responsibilities and define rights, safeguards or technical requirements. Directives, including NIS2, require Member States to establish national rules and supervisory arrangements. These instruments differ in scope and legal form. Together, they increasingly determine how digital systems are designed, procured, connected and supervised, rather than merely setting general ambitions. [33, 34, 35, 36, 37, 38, 39]

The third layer combines policy programmes, funding and shared infrastructure. The Digital Europe Programme supports advanced digital capacity and deployment; the AI Continent Action Plan

promotes computing capacity and AI adoption; European data spaces and identity infrastructure are intended to support exchange across borders and sectors. These initiatives are not equivalent to legal obligations, and an announced investment or pilot does not prove that a service is operational. They nevertheless matter because the EU now treats computing capacity, data access, cybersecurity and specialised skills as conditions for achieving its regulatory and economic objectives. [40, 41, 42]

The fourth layer is implementation and enforcement. National authorities, the European Commission, the AI Office and European networks of regulators monitor compliance in different fields. Digital Decade reports track progress against roadmaps, while enforcement under the DSA and DMA has moved from designation and preparation to investigations and formal decisions. The European approach therefore combines target setting with institutional responsibility, investment and review. For Kosovo, this architecture is more useful as an analytical reference than as a template to reproduce in full. [31, 36, 43]

What has changed since 2023

The most visible change is the move from broad digital targets to rules and implementation mechanisms. The Data Governance Act began applying in September 2023, the DSA became generally applicable in February 2024 and the first DMA gatekeepers reached their principal compliance deadline the following month. During 2024 the EU adopted the AI Act, the Interoperable Europe Act and the revised digital identity framework. The European Health Data Space entered into force in 2025, while the Data Act and the European Accessibility Act began applying that year. Cybersecurity policy also expanded from the protection of networks and essential organisations toward the resilience of products, financial services and supply chains. [44, 35, 36, 37, 45, 46, 47, 48, 49]

The substance of digital policy has widened at the same time. Digital government is increasingly assessed through interoperability and the completion of end-to-end transactions, not the number of portals alone. Business digitalisation now raises questions about access to data, platform power, privacy, intellectual property and dependence on cloud or AI providers. Connectivity policy encompasses deployment procedures, cloud, edge and computing capacity alongside fibre and 5G coverage. Skills policy now includes AI literacy and specialised capability as well as basic participation.

The EU has also placed greater emphasis on competitiveness and technological sovereignty. Its adoption policies seek to expand the use of AI while its regulatory framework addresses risks, market conduct and fundamental rights. Proposals presented in 2026 on digital networks and cloud and AI capacity reinforce this direction, but they were not adopted law at this chapter's cutoff. This distinction matters for Kosovo: policy direction can inform planning, but pending proposals should not be treated as settled requirements. [50, 51]

These developments explain why a review of DAK is warranted even if its five objectives remain broadly sound. The strategy was designed before many of these instruments entered their implementation phase. A review can therefore test the assumptions beneath the objectives: whether institutional responsibilities remain clear, whether planned investments include recurring costs, whether legal approximation is matched by enforcement capacity, and whether monitoring provides evidence about outcomes rather than activities. The point is to update the delivery model where necessary, not to replace the agenda with a catalogue of recent EU legislation.

AI data markets privacy and intellectual property

AI illustrates both the expansion and the instability of the European framework. The AI Act entered into force on 1 August 2024, with phased application. Prohibitions and the original AI-literacy provisions began applying in February 2025; general-purpose AI obligations and governance provisions followed in August 2025. General application in August 2026 did not mean that every obligation applied to every system. Amendments entering into force in July 2026 moved the main high-risk deadlines to December 2027 for Annex III systems and August 2028 for systems associated with Annex I product legislation. [33, 52]

The July 2026 changes also revised the treatment of AI literacy and strengthened parts of EU-level oversight. The AI Office's role in relation to general-purpose models differs from the responsibilities attached to downstream systems, while the general-purpose AI Code of Practice remains a voluntary compliance instrument. Alignment therefore requires attention to the use being governed and the responsible actor. For DAK, this applies both to business support and public administration. A public body acquiring an AI-enabled service still needs to understand its purpose, data and limitations, provide a route to challenge errors and ensure that staff can exercise judgement. These considerations do not mean that a Kosovo institution is automatically subject to a particular AI Act obligation. [52, 53]

Alongside regulation, the AI Continent Action Plan and the Apply AI Strategy developed a stronger European adoption agenda in 2025. Computing infrastructure, AI factories, testing facilities and support for business and public-sector use form part of this policy approach. These are programmes and investment initiatives, not evidence that all announced capacity is operational. Their relevance to DAK lies in the conditions for useful adoption. For a smaller economy, access to suitable services, capable intermediaries and sector expertise may matter more than reproducing the infrastructure ambitions of larger Member States. [40, 54]

Data policy addresses another constraint on adoption. The Data Governance Act, adopted before DAK, began applying in September 2023; the subsequently adopted Data Act generally began applying in September 2025. The former establishes arrangements for protected public-data reuse, data intermediaries and data altruism. The latter addresses, among other matters, access to connected-product data and switching between data-processing services. Their significance is not that all data become openly available. It is that access and reuse depend on defined rights, responsibilities and safeguards. [44, 34]

Research by Coche, Kolk and Dekker on financial-sector data sharing identifies tensions involving privacy, security, control and business incentives; it does not evaluate the subsequent effects of the Data Act. The relevant point for Kosovo is that formal access does not make data economically useful. Quality, contractual conditions and compatibility with business processes influence whether smaller firms can benefit. [55]

Personal-data protection has become more closely intertwined with AI and data use. The GDPR predates DAK, but principles such as purpose limitation, data minimisation and accountability are harder to apply to generative AI, outsourced analytics and linked records. The European Data Protection Board concluded in Opinion 28/2024 that the anonymity of an AI model must be assessed case by case; training on personal data does not make a model automatically anonymous. Public bodies and businesses still need to assess identification risks, legal basis and the exercise of individual rights. [56, 57]

Intellectual property presents a related business-capacity issue. A 2025 EUIPO and European Patent Office study found that 9.74 per cent of SMEs in its EU sample owned a registered patent, trade mark or design, compared with 49.01 per cent of large firms. The panel covers 2013–2022, excludes copyright and does not describe Kosovo. It nevertheless illustrates why firms adopting digital tools need practical support to protect brands, designs, software and original content, and to respect licences and third-party rights. [58]

Generative AI makes that need more immediate. The AI Act requires providers of general-purpose models to maintain a policy for compliance with EU copyright law and publish a sufficiently detailed summary of training content. EUIPO also identifies rights reservation, licensing and identification of generated content as central questions. The rules do not settle ownership of every AI-assisted output. For DAK, they support combining SME technical assistance with accessible advice on licences, contracts, training inputs and commercial use. [59, 60]

The platform framework has also moved into enforcement. The DSA became generally applicable in February 2024, and the first DMA gatekeepers reached their principal compliance deadline in March 2024. The Commission’s April 2025 decisions against Apple and Meta show enforcement moving beyond designation, although they do not establish final judicial outcomes or economy-wide benefits. Research on DSA codes of conduct also raises questions about participation and accountability. Kosovo should distinguish adoption of comparable rules from the capacity to investigate complaints and sustain oversight. [35, 36, 43, 61]

Competitiveness, strategic dependence and regulatory simplification now sit alongside these concerns. The proposed Digital Networks Act and Cloud and AI Development Act remain proposals, as does the broader digital omnibus. They indicate policy direction, not settled requirements or the removal of existing safeguards. Kosovo nevertheless needs the capacity to follow amendments and address dependence on suppliers where it limits switching, control over data or long-term affordability. [50, 51, 62]

Interoperable public services identity and health

DAK’s public-service objective already contains the once-only principle. The European developments since adoption make its organisational implications more concrete. Under the Interoperable Europe Act, mandatory assessments began in January 2025 for specified binding requirements affecting trans-European digital public services. This is not a requirement to assess every local technology purchase. It reflects the recognition that legal and organisational choices, as well as technical design, can create barriers to exchange. [63, 37]

The Once-Only Technical System provides a related example. Its core infrastructure was launched in December 2023 to support cross-border exchange of evidence for relevant procedures. Launching that infrastructure did not establish that every competent authority was connected or every procedure worked end to end. For Kosovo, the distinction is particularly useful. A citizen should not have to compensate for institutional fragmentation by moving the same information between offices, but eliminating that burden requires reliable source registers and an agreed legal basis for exchange. An interface cannot resolve contradictory records or unclear authority over data. [41]

Estonia’s cooperation with its Nordic neighbours illustrates these dependencies. Hardy’s interview-based study finds that cross-border interoperability requires sustained institutional and diplomatic work

even where the technology is mature. The example does not suggest that Kosovo can reproduce the same result by adopting an Estonian platform. National law, administrative practice, resources and cooperation arrangements remain decisive. [64]

Digital identity adds a shared component. The revised EU framework entered into force in May 2024, with Member States expected to provide European Digital Identity Wallets by the end of 2026. Implementing regulations specify requirements for functionality, interfaces and certification. For DAK, identity should be assessed through transactions: whether services accept the credential, source data are reliable, users can recover access and redress is available. Technical similarity would not itself secure European recognition, which depends on applicable legal and cooperation arrangements. [45, 38, 65]

The European Health Data Space entered into force in March 2025, but its requirements are phased. Priority categories for primary use, including patient summaries and electronic prescriptions, and most secondary-use provisions are scheduled for 2029; further categories follow in 2031. It is not yet a fully operational system that Kosovo can simply join. Its relevance lies in the preparation required: structured records, consistent terminology, reliable patient identification, secure access and clear responsibility. DAK's health-record ambition therefore concerns clinical and data-governance arrangements as well as an online account. [46, 1]

Finland's Findata offers a bounded example. Its 2024 annual report describes an authority that manages permits and coordinates secure access to health and social data under national law. This institutional self-assessment is not evidence of completed EHDS implementation, but it shows the functions and resources behind a health-data space. It is not an automatic case for creating an identical authority in Kosovo. [66]

These developments place greater weight on shared administrative foundations. Applications can be procured faster than institutions can reconcile records, assign responsibility or change procedures. Once-only administration also has a public-interest boundary: data reuse does not authorise unrestricted circulation across government. The purpose and authority for an exchange, and the record of access, remain material. Interoperability and privacy must be assessed together.

Cyber resilience and digital infrastructure

European cybersecurity policy now addresses several connected layers. The Network and Information Systems Directive (EU) 2022/2555 (NIS2), adopted before DAK, reached its EU transposition deadline in October 2024. The Cyber Resilience Act, adopted afterwards, introduces product-security requirements, including lifecycle responsibilities. Its reporting obligations begin on 11 September 2026, two days after this chapter's cutoff, while its main requirements apply from December 2027. Treating either future stage as already operational would distort the benchmark. [39, 47]

The distinction between organisational and product security matters for DAK. Incident-response arrangements cannot compensate for unsupported software, while secure products cannot compensate for weak access controls or absent recovery procedures. Procurement connects these layers: the choice of a supplier also determines access to updates, vulnerability information and support. Cybersecurity expenditure is therefore part of the cost of delivering a digital service, not only the budget of a specialised authority.

The Cyber Solidarity Act, in force since February 2025, adds arrangements for preparedness and coordinated response. The Digital Operational Resilience Act (DORA), applicable in the EU since January 2025, addresses operational resilience in finance, including ICT third-party risk. Neither creates an automatic entitlement to EU assistance or a general domestic obligation for Kosovo. Financial-sector relevance may arise through EU group relationships, service provision or contracts; the precise obligations require a case-specific assessment. These instruments nonetheless broaden the questions that can be asked about supply-chain dependence and recovery capacity. [67, 48]

Kosovo's own institutional evidence remains important. The Commission's 2025 report called for stronger operational cybersecurity arrangements and identified outstanding implementing measures. It also described resource constraints affecting the telecommunications regulator. These are dated findings, not proof that the same gaps persisted unchanged in September 2026. They identify issues for validation: staffing, operational procedures and the ability to use legal powers, rather than only the existence of legislation. [10]

Connectivity policy presents a parallel implementation challenge. The Gigabit Infrastructure Act, fully applicable from 12 May 2026, addresses deployment costs, access to physical infrastructure and administrative coordination. For DAK's fixed and mobile infrastructure objectives, this draws attention to obstacles that are not solved by coverage targets alone. Permissions, infrastructure information and coordination between public bodies can influence how efficiently networks are extended. [68]

Fibre, 5G, cloud and edge capacity are also inputs whose value depends on service quality and use. Coverage does not by itself establish affordability, reliability or business adoption. Larger computing projects raise further questions about electricity, connectivity and operating expenditure. In assessing DAK, infrastructure ambition and institutional capacity therefore belong in the same analysis, including the capacity to manage contracts and maintain services after initial investment.

Skills inclusion and trust

European evidence continues to show that technical availability is an incomplete measure of digital inclusion. Eurostat data for 2025, published in 2026, indicate that 60% of people aged 16–74 had at least basic digital skills. The share was 82% among those with a high level of formal education and 38% among those with a low level. This indicator is derived from reported digital activities rather than a direct competence examination. It describes the EU, not Kosovo, but shows why widespread connectivity can coexist with considerable inequalities in use. [69]

The Union of Skills, launched in 2025, places skills development within the wider competitiveness agenda. Gender inequality remains relevant within the specialist workforce: women accounted for 19.5% of EU ICT specialists in 2025. For DAK, the distinction between general digital participation and specialist labour supply is consequential. More ICT graduates would not, by itself, establish that people with limited education can use essential services or that women have equal access to digital employment. [70, 71]

AI literacy adds a further dimension, despite changes to its regulatory treatment in 2026. Training attendance is not evidence that a worker can recognise an unreliable output or decide when human review is needed. For public administration, competence also includes understanding the limits of a tool and the responsibility attached to its use. The relevant assessment concerns the relationship

between learning and actual tasks, rather than a presumption that every employee requires the same course. [52]

Accessibility and child protection make service quality more explicit. The European Accessibility Act began applying to covered products and services in June 2025. The Commission's July 2025 guidelines on protecting minors provide a reference for implementing DSA duties; they do not constitute a separate generally binding law or automatic proof of compliance. These developments strengthen the analytical case for examining design, usability and safeguards alongside access. They do not establish identical domestic obligations in Kosovo. [49, 72]

For DAK's population-skills and public-service objectives, inclusion is therefore a practical test of implementation. An online procedure can reduce burdens for one group while increasing them for people who need assistance, use another language or cannot navigate its interface. Trust depends on whether users can understand a decision, correct inaccurate information, obtain human assistance and know how their data are being used. Service counts and registration figures do not capture these outcomes.

Kosovo European and regional integration

The Western Balkans Growth Plan, adopted in November 2023, connects closer economic integration with reforms and financial support. Kosovo's Reform Agenda was approved by the Commission in October 2024. Its published milestones include digital public services, identity, connectivity and cybersecurity. These commitments create a more specific implementation context for DAK, but approval of an agenda is not confirmation that its milestones have been met or associated funds disbursed. [73, 23]

Digital Europe participation offers another channel. Kosovo is associated with the programme, while access to particular actions remains subject to call conditions and, for certain capacities, security-related restrictions. Association can create opportunities for cooperation; it does not establish eligibility for every project or the resources to prepare and sustain participation. Administrative capacity, partnerships and any required co-financing affect the practical value of access. [42]

The Common Regional Market Action Plan for 2025–2028, signed in October 2024, supplies a further regional policy context. Cooperation can offer a useful scale for shared learning and compatible approaches, but regional commitments, EU programme participation and domestic implementation are distinct processes. Their value for DAK depends on whether they connect to the same responsible institutions and delivery priorities, rather than generate parallel commitments with separate reporting and no clear operational relationship. [74]

The Commission's latest country assessment available for this review, published in November 2025, identified alignment and implementation work across electronic communications, platform regulation, interoperability, AI and cybersecurity. Its reporting period ended in September 2025. The June 2026 OECD profile provides additional assessment material, but its publication date does not turn all underlying observations into measurements taken that month. Neither source supports a blanket judgement about Kosovo's position at the chapter's September 2026 cutoff. They provide a documented basis for testing subsequent progress with institutions and service users. [10, 75]

Conclusion

DAK's five objectives remain broad enough to accommodate the main European developments examined in this chapter. The need for review arises because the content and conditions of implementation have become more specific. Public-service digitalisation now depends on interoperable registers, trusted identity and effective data governance. Business digitalisation increasingly involves access to data, responsible AI adoption, privacy, intellectual property and the terms on which firms depend on platform, cloud and software providers. Cybersecurity extends across institutions, products, suppliers and essential services. Inclusion must be assessed through people's ability to complete transactions and exercise their rights, rather than through access or service counts alone.

Governance is the immediate condition for responding to these changes coherently. DAK envisages central monitoring, annual reporting and periodic evaluation. Preliminary evidence gathered for this assessment indicates that the central coordination mechanism has not remained operational as a regular forum for direction and accountability. If this is confirmed, the problem is not simply the absence of another committee. Without an active body that can review evidence, assign responsibility and resolve dependencies between institutions, separate projects may advance without producing the combined outcomes that the agenda requires. A credible review should therefore address how political oversight, technical coordination and public reporting will operate for the remainder of the strategy period. [1, 9]

Legal approximation also needs a more adaptive process. Kosovo will need to track recently adopted EU legislation, implementation standards and subsequent amendments, deciding what should be transposed, approximated or addressed through sectoral practice. This work cannot be measured only by the number of legal acts adopted. Regulators and implementing institutions need staff, procedures, technical knowledge and enforcement tools. The pace of change in AI and data policy also argues for institutions that can revise guidance and implementation plans without waiting for another full strategy cycle.

Skills form part of the same implementation capacity. General digital literacy remains important, but the European framework now requires more specialised competence in AI assessment, cybersecurity, data protection, interoperability, procurement and intellectual property. Public institutions must be able to act as informed purchasers and supervisors of technology, while businesses and citizens need accessible support to use digital systems safely and productively. Training should therefore be connected to actual functions and measured through changes in practice, not participation figures alone.

Finally, technological sovereignty should be understood in practical rather than absolute terms. Kosovo cannot and need not produce every component of its digital infrastructure. It can, however, reduce avoidable dependence by maintaining control over critical data, avoiding unnecessary supplier lock-in, applying open and interoperable standards where appropriate, diversifying essential providers and retaining the capacity to operate and secure public systems. These considerations link competitiveness to resilience and public accountability.

The review should not replace DAK with a list of new EU instruments. Its purpose is to preserve the agenda's useful direction while updating the arrangements that make delivery possible: governance, legal and regulatory capacity, skills, financing, secure infrastructure and measurable outcomes. That

would keep the strategy connected to Kosovo's European integration pathway without treating formal alignment as evidence of implementation.

Chapter 4 Recommendations for implementing and updating DAK 2030

The assessment findings show that DAK 2030 has made progress in digital infrastructure, the expansion of electronic services and the development of the innovation ecosystem. However, achieving the objectives by 2030 requires clearer governance, sustained funding and a regular system of measurement and reporting. The priorities identified during the discussion of preliminary findings and in the report's analysis should be translated into concrete measures, with responsible institutions and verifiable results.

It is recommended that DAK's five strategic objectives be retained, while the specific objectives, indicators and action plan are updated for the remaining period through 2030. The update should address identified implementation gaps and developments in EU digital legislation, adapting them to Kosovo's capacity and needs.

4.1 Improving governance and accountability

The Government should explicitly designate the lead institution for DAK implementation and allocate responsibilities among ministries, agencies and regulators. This is particularly important following institutional changes and transfers of responsibilities. Each objective and indicator should have an institution accountable for the result, alongside institutions that contribute to implementation or provide data. Ideally, given the number of actors involved, DAK 2030 should be governed by the Office of the Prime Minister.

DAK's steering structure should function as a regular decision-making mechanism. Quarterly meetings are recommended to review progress, obstacles and budget execution. Decisions should specify corrective measures, the responsible institution and the implementation deadline. Issues that cannot be resolved at the technical level should be referred to the Government.

Consultation with the private sector, universities and civil society should become part of the annual monitoring cycle. Organisations such as STIKK, ITP Prizren (including DIG-4K) and Venture UP can contribute evidence from businesses, training programmes and innovation projects. Responsibility for national statistics and official reporting should remain with the competent public institutions.

4.2 Mandatory measurement and publication of all indicators

The lack of data should be treated as a weakness in the implementation system. Institutions should be designated and required to ensure that data for every indicator under their responsibility are measured, submitted and published.

This obligation should cover all existing indicators and those added during the review. Where an indicator requires a national survey, the responsible institution should work with the Kosovo Agency of Statistics (ASK) on methodology and funding. Where data already exist in administrative registers, institutions should organise their regular extraction and validation.

A methodology sheet should be approved for each indicator, containing:

- the definition, unit of measurement and calculation formula;

- the population covered, numerator and denominator;
- the baseline value and its reference year;
- the 2030 target and intermediate milestones;
- the data source and responsible institution;
- the frequency of measurement and publication deadline;
- methodological limitations and the procedure for correcting data.

ASK should coordinate statistical harmonisation with European methodologies, while ARKEP, the institutions responsible for digital services, IKAP and sectoral institutions should provide measurements within their respective remits. Data from projects or limited samples should be clearly identified and should not be presented as representative results for Kosovo as a whole.

Results should be available on a shared monitoring webpage, with historical series, methodological explanations and downloadable files in open formats. Publication should protect personal data, statistical confidentiality and sensitive security information.

For indicators without measurements, the responsible institution should submit a data collection plan with a deadline and budget. A “No data” status should be accompanied by this explanation. The aim should be to establish methodologies for all indicators and complete the first measurements for existing gaps by the end of 2027.

4.3 Filling gaps in targets and objectives

Six indicators identified in the assessment have no target for 2025 or 2030. The review of Annex I should address these indicators specifically. Targets should be based on baseline measurements, sectoral needs and the resources required to achieve them.

Indicator	Recommended addition
SO3.4.2 – Public employees with advanced digital skills	Define the required level of competence and measure the percentage of employees who demonstrate it. Link the 2030 target to the administration’s needs, with a sub-indicator for positions that necessarily require advanced skills.
SO4.2.1 – Science and technology graduates	Define the fields and levels of education covered, the baseline and the growth target through 2030, taking labour market demand into account.
SO4.2.2 – STEM graduates	Set a measurable target with breakdowns by gender and field of study. Clarify the overlap with SO4.2.1 so that results are not counted twice as separate achievements.
SO4.5.1 – ICT businesses’ expenditure on research and development	Establish a regular statistical series for actual expenditure. Express the 2030 target in monetary terms and, in accordance with the approved methodology, as a share of the sector’s economic activity.
SO5.1.2 – Individuals who have experienced misuse of personal data or a breach of privacy	Set a target for reducing the prevalence of harm, measured through comparable surveys. Report the number of administrative complaints separately, since increased reporting may reflect greater awareness and better access to remedies.
SO5.1.7 – Individuals who do not allow their personal data to be used for advertising	Review the desired direction of the indicator. The objective should concern informed choice and the actual ability to exercise rights. The percentage refusing advertising should be interpreted as user behaviour, not automatically as success or failure.

In addition to filling gaps in targets, it is recommended that specific objectives be added or made more concrete for:

- **the responsible use of artificial intelligence**, with risk assessment, human oversight and institutional capacity;
- **data governance and interoperability**, including register quality and practical implementation of the once-only principle;
- **accessibility and digital inclusion**, measuring different groups' actual ability to complete services;
- **operational resilience and supplier security**, including recovery after incidents and maintenance of digital products;
- **the protection of rights in the digital environment**, including privacy, complaints about online services and the lawful use of content and software.

These objectives should be integrated within DAK's five existing areas and accompanied by defined measures, funding and indicators.

4.4 Linking funding to results

The updated action plan should specify the cost of each measure, its funding source and the responsible institution. Budgeting should include maintenance, security updates, licences and staff throughout the systems' lifecycle.

For research and innovation, planned funding, allocated funding and actual expenditure should be reported separately. The amount attributable to ICT research should be identified within each. The classification of SO4.5.2 as partially achieved reinforces this need: the overall research and innovation allocation and its partial execution do not provide an accurate measurement of expenditure on ICT research.

Support for SMEs should focus on practical technology use through grants, digital service vouchers and technical assistance. Programmes with ITP Prizren (including DIG-4K), STIKK, Venture UP and other actors should measure changes in beneficiary enterprises, including productivity, security and technology use. The number of beneficiaries and training participations should be supplemented by assessments after support has been completed.

In public services, priority should be given to procedures with high usage and a heavy administrative burden. Completing them entirely online requires procedural changes, reliable registers, acceptance of electronic identity and user support.

4.5 Proposed additional indicators for 2030

The analysis of EU legislation demonstrates the need to measure the quality, security and use of digital systems. The AI Act, the European Digital Identity framework, the Interoperable Europe Act and the instruments on data and cybersecurity provide reference points for this update.

The table below proposes supplementary indicators. The numerical targets are proposals for discussion and institutional approval; they are neither adopted DAK targets nor numerical obligations imposed on Kosovo by the EU. A baseline should be established for each indicator during 2027 and the cost of achievement assessed. The list of services, systems or entities included in the denominator should be approved in advance and documented.

Proposed indicator and link to the EU	Measurement method	Proposed 2030 target	Responsibility and data source
Implementation of the once-only principle – European interoperability	Percentage of key services that lawfully obtain the necessary data from registers without requiring users to resubmit them.	90% of key services to which the principle applies.	The institution responsible for digitalisation, the Information Society Agency (ASHI) and service-providing institutions; transaction logs and annual testing.
Functional acceptance of electronic identity – EUDI/eIDAS framework	Percentage of key services requiring identification that accept the national eID in a successfully completed transaction.	100%.	Institutions responsible for eID and services; documented testing and usage data.
Interoperability of health data – EHDS	Percentage of public healthcare institutions within scope that exchange structured patient summaries in accordance with approved national specifications.	90%.	The Ministry of Health and healthcare institutions; technical testing and annual reporting.
Accessibility of digital public services – European accessibility framework	Percentage of key services that pass an assessment against the applicable requirements of EN 301 549, using the version adopted in the national framework.	100%.	Service-providing institutions; accessibility audits and user testing.
AI risk management in the public sector – AI Act	Percentage of public-sector systems classified as high-risk that have a documented risk assessment, safeguards and human oversight in place before use.	100%.	User institutions and the competent authority designated in the domestic framework; a systems inventory and periodic checks.
Data protection impact assessment – GDPR principles	Percentage of new or changed processing operations requiring an impact assessment for which it has been completed before processing begins.	100%.	Data controller institutions, supervised by the Information and Privacy Agency (AIP); registers and documentation checks.
Data portability and exit from cloud services – Data Act	Percentage of critical public cloud services with an exit plan and a documented test of data export and reuse.	100%.	Contracting institutions and ASHI; contracts, a service inventory and periodic tests.
Readiness for incident recovery – NIS2 and, for the financial sector, DORA	Percentage of entities within the national scope that meet approved recovery objectives in a documented annual test. Results are reported separately by sector.	100%.	The competent cybersecurity authority and sectoral regulators, including the Central Bank of Kosovo; test reports.

Proposed indicator and link to the EU	Measurement method	Proposed 2030 target	Responsibility and data source
Timely reporting of significant incidents – NIS2	Percentage of incidents identified as reportable for which notification was submitted within the applicable deadline in the domestic framework.	100%.	The competent authority and response teams; incident registers, with publication of aggregated results.
Security throughout the lifecycle of digital products – Cyber Resilience Act	Percentage of new public contracts for products with digital elements that specify the support period, security updates and vulnerability-handling procedure.	100% of contracts within the defined scope.	Contracting authorities and the competent procurement and security bodies; annual contract review.
Handling complaints about digital services – DSA	Percentage of complaints within the competence of domestic authorities that receive a reasoned response within the deadline set by the national framework.	At least 90%, with an annual public report.	The competent authorities for digital services and consumer protection; complaint registers.
Efficiency of network deployment procedures – Gigabit Infrastructure Act	Percentage of complete permit applications whose review deadline falls within the year that receive a decision within the statutory deadline. Overdue applications still awaiting a decision are included.	At least 95%.	Permit-issuing authorities, municipalities and the institutions responsible for connectivity; an electronic application register.

The supplementary indicators should be linked to existing ones without creating double counting. For example, acceptance of eID by services complements the measurement of its use by citizens, while health data interoperability complements the indicator on access to electronic records.

For indicators based on complaints or incidents, the absence of reported cases should not automatically be interpreted as a positive result. Where the denominator is zero, the result should be recorded as “Not applicable for the period”, together with the number of cases and the relevant explanation.

4.6 Legal approximation and sequencing of actions

Alignment with the EU should be based on a plan identifying the European instrument, the gap in the domestic framework, the action required and the responsible institution. The plan should distinguish the adoption of legislation from the development of capacity for implementation and supervision. This applies to AI, data, the DSA, the DMA, digital identity and cybersecurity.

EU regulations do not automatically become part of domestic law. Approximation should take account of each instrument’s scope and the powers Kosovo can exercise. Similarly, technical compatibility with European systems does not by itself ensure recognition or participation in EU mechanisms.

The following sequence of actions is recommended:

- **Within six months of adopting the recommendations:** clarify the lead institution, establish an operational technical secretariat and assign responsibility for every indicator.

- **During 2027:** update the action plan and Annex I, fill the gaps in targets and conduct baseline measurements for the new indicators.
- **During 2028–2029:** expand measures that demonstrate results, conduct an independent assessment of progress and adjust interventions with weak implementation.
- **For 2030:** carry out the final measurement against the approved targets. Publish the final assessment once complete data for the year are available.
- **In early 2031:** publish the full DAK implementation report.

References

Numbered citations throughout the report refer to this consolidated list. Unpublished institutional responses and project research are identified separately from public sources. Publication dates and the periods measured are distinguished in the analysis.

1. Ministry of Economy, Kosovo (May 2023), Digital Agenda of Kosovo 2030, Annex I and sections 5.2–5.3. Original title: Agjenda Digjitale e Kosovës 2030. [Online source](#) [Additional source](#)
2. Ministry of Economy (30 June 2023), Government adopts the Digital Agenda of Kosovo 2030. [Online source](#)
3. ARKEP (August 2026), institutional response to ITS on DAK 2030 indicators. Unpublished primary communication.
4. STIKK (August 2026), institutional response to ITS on startup and SME support, training, employment and investment. Unpublished primary communication.
5. Kosovo Institute for Public Administration (IKAP) (September 2026), institutional response to ITS on public employee training and cybersecurity. Unpublished primary communication.
6. Ministry of Education and Science (MASH), institutional response to ITS on higher education programmes in innovative technologies, August 2026. Unpublished primary communication.
7. Ministry of Economy (September 2026), institutional response to ITS on the indicator “Legal and regulatory framework for intelligent/innovative ecosystem developed”. Unpublished primary communication.
8. Institute for Technology and Society (2026), project interviews and written questions to public institutions, private organisations, NGOs and innovation organisations, including ITP Prizren, Venture UP and STIKK. Primary research undertaken for this assessment.
9. Institute for Technology and Society (10 September 2026), notes from the stakeholder workshop on DAK 2030 implementation. Unpublished project record.
10. European Commission (4 November 2025), Kosovo Report 2025, especially Chapter 10, pp. 73–74. [Online source](#) [Additional source](#)
11. UNDP Kosovo (24 June 2025), Digital Development Profile. [Online source](#)
12. World Bank (21 March 2023), Every village in Kosovo now connected to high-speed broadband internet with World Bank support. [Online source](#)
13. Regional Cooperation Council (April 2026), Western Balkans Digital Economy and Society Index 2025. [Online source](#)
14. Digital Inclusion Initiative / Kosovo Education Center (June 2025), National Report for Kosovo. [Online source](#)
15. ARKEP (2025), Regulation No. 68 on the security and proper functioning of electronic communications networks and services. [Online source](#)
16. ITS (August–September 2026), additional institutional and project information collected on SO1. Unpublished primary evidence.
17. Kosovo Agency of Statistics, Survey on ICT Use in Households, 2024 and 2025. [Online source](#)
18. ITP Prizren – DIG-4K (30 June 2026), Deliverable D3.1 - Assessment of Training Needs and Requirements. [Online source](#)
19. ITP Prizren – DIG-4K (30 June 2026), Deliverable D3.2 - Digital Skills Curriculum for MSMEs, education and public sector. [Online source](#)
20. Kosovo Agency of Statistics (22 May 2025), Labour Force Survey results for 2024. [Online source](#)
21. Eurostat, Digital Economy and Society — Information Society and enterprise ICT datasets, checked in September 2026. [Online source](#)
22. Evidence from DIG-4K, part of ITP Prizren, used for this assessment: the digital maturity assessment (DMA) dataset containing 43 initial assessments conducted before interventions and services were delivered. Unpublished data.
23. Government of Kosovo (2024), Reform Agenda of Kosovo, policy area 2a — Digitalisation; Annex 1 reform milestones, p. 4. [Online source](#) [Additional source](#)
24. Ministry of Economy (18 November 2025), Ministry of Economy begins the first pilot phase for electronic identity enrolment. [Online source](#)
25. Government of Kosovo (2026), Concept Document on electronic identification, trust services and the Digital Identity Wallet. [Online source](#)

26. Interoperable Europe, Kosovo 2025 monitoring — Open Data Portal and public-sector interoperability indicators. [Online source](#)
27. Eurostat, isoc_ciegi_ac — Individuals interacting online with public authorities, Kosovo, 2025 observations. [Online source](#)
28. Eurostat (2026 edition), sdg_04_70 / isoc_sk_dskl_i21 — Share of adults with at least basic digital skills, 2025 observations. [Online source](#)
29. Riinvest Institute / POLICY ANSWERS (4 April 2026), Developments in the R&I Sector in Kosovo 2023-2025. [Online source](#)
30. Official Gazette of the Republic of Kosovo, Law No. 08/L-173 on Cybersecurity and implementing acts. [Online source](#)
31. European Commission, Digital Decade Policy Programme, live implementation/governance overview; planned review in 2027. [Online source](#)
32. European Commission (2026), 2026 State of the Digital Decade package. Exact publication day not established; overview rather than all underlying reports. [Online source](#)
33. European Commission, AI Act: regulatory framework and implementation timeline, live page reflecting July 2026 amendments. [Online source](#)
34. European Commission, Data Act, implementation and application overview for Regulation 2023/2854. [Online source](#)
35. European Parliament, Committee on Petitions (Commission reply received 12 August 2025), Communication to Members, PE776.785, p.2, DSA entry and general application dates. [Online source](#)
36. European Commission (7 March 2024), Designated gatekeepers must now comply. [Online source](#)
37. Council of the European Union, Interoperable Europe legislative text, PE-CONS 73/23, 21 February 2024 document version, adopted by Council 4 March. Pre-publication text, not the final numbered OJ edition; Article 3 and governance provisions. [Online source](#)
38. European Commission, European Digital Identity Regulation, updated 22 June 2026; “Next steps”. [Online source](#)
39. European Commission, NIS2 Directive, scope, implementation and EU transposition deadline. [Online source](#)
40. European Commission (9 April 2025), AI Continent Action Plan. [Online source](#)
41. European Commission, DG GROW (12 December 2023), Online cross-border procedures to be simplified through the Once-Only Technical System. [Online source](#)
42. European Commission, Digital Europe Programme — Questions & Answers, association and Article 12 security conditions. [Online source](#)
43. European Commission (23 April 2025), Commission finds Apple and Meta in breach of the Digital Markets Act. [Online source](#)
44. European Commission, European Data Governance Act, and DGA becomes applicable (25 September 2023 announcement; application 24 September). [Online source](#) [Additional source](#)
45. European Commission (2 September 2025), The legal and technical road to EU Digital Identity Wallets, opening paragraph confirms entry on 20 May 2024. [Online source](#)
46. European Commission, DG SANTE, European Health Data Space Regulation, implementation timeline and primary/secondary-use distinctions. [Online source](#)
47. European Commission, Cyber Resilience Act, entry/application dates and 27 July 2026 guidance. [Online source](#)
48. EIOPA, Digital Operational Resilience Act, 17 January 2025 application; legal provisions and third-party oversight. [Online source](#)
49. European Commission (27 June 2025), The EU becomes more accessible for all, application on 28 June. [Online source](#)
50. European Commission (21 January 2026), Proposal for a Digital Networks Act. [Online source](#)
51. European Commission (3 June 2026), Proposal for the Cloud and AI Development Act. [Online source](#)
52. European Commission (27 July 2026; updated 31 July), AI Omnibus enters into force. [Online source](#)
53. European Commission, General-Purpose AI Models in the AI Act — Questions & Answers; final code publication 10 July 2025; model/provider/system distinctions. [Online source](#)
54. European Commission, Apply AI Strategy, launched 8 October 2025; opened page updated 21 August 2026. [Online source](#)

55. Coche, Eugénie, Ans Kolk and Martijn Dekker (12 February 2024), “Navigating the EU data governance labyrinth: A business perspective on data sharing in the financial sector,” *Internet Policy Review*, 13(1), doi:10.14763/2024.1.1738. Full text. Exploratory analysis; the article discloses ABN AMRO funding of the first author’s PhD without content/publication restrictions. [Online source](#)
56. European Commission, Data protection explained, GDPR principles, scope and individual rights; live institutional guidance. [Online source](#)
57. European Data Protection Board (18 December 2024), Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, especially paras. 34 and 38–43 on case-specific assessment of anonymity and identification risk. [Online source](#)
58. European Union Intellectual Property Office and European Patent Office (January 2025), Intellectual property rights and firm performance in the European Union, executive summary, Table E1, printed p.8 (PDF p.3). [Online source](#)
59. European Commission, Guidelines on obligations for general-purpose AI providers, copyright-policy and training-content-summary obligations applicable from 2 August 2025. [Online source](#)
60. European Union Intellectual Property Office (May 2025), The development of generative artificial intelligence from a copyright perspective, executive brief, pp.3–5. [Online source](#)
61. Griffin, Rachel (2 September 2024), “Codes of Conduct in the Digital Services Act: Functions, Benefits & Concerns,” *Technology and Regulation*, 2024, 167–187. Full text. [Online source](#)
62. European Commission, Simplification tracker, section “Omnibus VII: digital”; distinguishes adopted Regulation 2026/1744 from pending COM(2025)837. [Online source](#)
63. European Commission / Interoperable Europe (13 January 2025; updated 18 February), Interoperability assessments are now mandatory. [Online source](#)
64. Hardy, Alex (22 July 2024), “Estonia’s digital diplomacy: Nordic interoperability and the challenges of cross-border e-governance,” *Internet Policy Review*, 13(3), doi:10.14763/2024.3.1785. Full text. Qualitative interview-based research. [Online source](#)
65. European Commission (4 December 2024), Implementing regulations for European Digital Identity Wallets. [Online source](#)
66. Findata, Annual report 2024, national health/social-data permit authority; reporting year 2024, live page updated in 2026. Implementation self-report. [Online source](#)
67. European Commission, EU Cyber Solidarity Act, entry into force, reserve and participation conditions. [Online source](#)
68. European Commission, Gigabit Infrastructure Act, phased application and implementation monitoring. [Online source](#)
69. Eurostat (2 June 2026 version), Skills for the digital age, 2025 observations, pp.1–3; Digital Skills Indicator methodology. [Online source](#)
70. European Commission (5 March 2025 initiative), Union of Skills. [Online source](#)
71. Eurostat (27 May 2026), Number of ICT specialists in the EU continues to grow, 2025 observations. [Online source](#)
72. European Commission (14 July 2025; updated 22 April 2026), Guidelines on the protection of minors, relationship to DSA Article 28(1). [Online source](#)
73. European Commission, Growth Plan for the Western Balkans, adopted 8 November 2023; Reform Agenda approval and financing conditions. [Online source](#)
74. Regional Cooperation Council (14 October 2024), Common Regional Market Action Plan 2025–2028. [Online source](#)
75. OECD (June 2026), SME Policy Index for Western Balkans and Türkiye 2026 — Economy Profile for Kosovo, doi:10.1787/5737889a-en; table 1.9 and digital-government discussion, PDF pp.49–51. [Online source](#)
76. Ministry of Digitalisation and Public Administration (2026), Draft Law on Electronic Communications; public consultation from 17 August to 4 September 2026. [Online source](#)
77. Email response from the Kosovo Agency of Statistics.
78. Supplementary comments received during the report review (29 September 2026), on the final stage of eID and its expected launch by the end of 2026, private 5G networks at UBT and Next Gen Networks Institute, and the existence and basic information of the atlas. Unpublished.
79. University for Business and Technology (UBT), “UBT Ranks Kosovo First in the Region for the Deployment of the 5G Network”. Announcement on deployment of the private 5G network. [Online source](#)

80. ARKEP / Ilir Imeri (2023), Current status of national broadband infrastructure in Kosovo, p. 17: private 5G authorisation for Next Generation Network Institute and campus testing authorisations. [Online source](#)
81. Official Gazette of the Republic of Kosovo (23 December 2021), Law No. 08/L-022 on Electronic Identification and Trust Services in Electronic Transactions, Articles 32, 33, 41 and 58. [Online source](#)
82. Ministry of Economy, Trusted Service Providers: PBC Sh.P.K. and Evrotrust Technologies JSC & IT Vision. Official list, accessed 29 September 2026. [Online source](#)

The background of the image is a deep blue gradient. A stylized map of Europe is visible, with its borders and major cities highlighted by a network of glowing white and yellow dots connected by thin, curved lines. Several bright, glowing arcs sweep across the lower half of the image, adding a sense of motion and technology. The text 'ITS INSTITUTE FOR TECHNOLOGY AND SOCIETY' is centered in the middle of the image.

ITS INSTITUTE FOR
TECHNOLOGY
AND SOCIETY