

Digital & Telecom Monthly Brief

Raport pregatit de Ana-Maria Anghel



Main Takeaways

Key Developments from the Previous Month

What to Watch in September

Main Takeaways

EU AI & Cloud Regulation Reshapes Digital Infrastructure Rules: The European Commission proposes a sovereign cloud framework with four assurance levels, strict data localisation, mandatory audits for higher tiers, and fast-track permitting for data centres based on sustainability and energy criteria.

EU Delays AI Act Compliance Deadlines: The Digital Omnibus for AI postpones key obligations for high-risk AI systems until 2027–2028, extends transparency deadlines, expands SME exemptions, and strengthens the EU AI Office while banning non-consensual AI-generated intimate content.

Romania Builds National Cybersecurity Governance System: DNSC introduces mandatory risk management and training frameworks under NIS2, requiring essential and important entities to implement structured controls, maturity scoring, audits, and certified cybersecurity training programmes.

Romania Creates Unified Digital State Infrastructure Register: Parliament adopts the PNIDP law, requiring all public institutions to register digital assets in a central platform managed by ADR, with STS infrastructure support and DNSC cybersecurity standards, enforcing interoperability and standardised digital governance.

Key Developments from the Previous Month

(1) New Investment Framework for Next-Generation 112 Emergency System.

Also in June, the Government approved the investment framework for **upgrading Romania's 112 emergency service**. The project aims to modernize emergency communications by enabling voice, real-time text, video, and total conversation services, in line with EU accessibility requirements. It also includes the deployment of AI and machine learning technologies for call analysis, transcription, summarisation, quality monitoring, and operator support, alongside new cybersecurity, interoperability, and digital infrastructure components. The investment is expected to be implemented over 36 months.

***Impact:** The project creates business opportunities for telecom, IT, cybersecurity, AI, and systems integration providers through future public procurement procedures. It does not introduce new compliance obligations for private sector operators but is expected to accelerate investment in Romania's digital emergency communications infrastructure.*

(2) Romania Adopts Framework for Identifying Critical Entities.

According to a recent decision of interim PM Ilie Bolojan, Romania now has the **framework for applying critical thresholds used to identify critical entities** under Law No. 294/2024. The decision establishes the methodology for assessing whether a significant disruption could affect operators in essential sectors, including digital infrastructure and telecommunications. The actual thresholds and assessment criteria remain classified and are contained in a non-public annex, which may be updated by the National Centre for Critical Infrastructure Protection Coordination when necessary.

***Impact:** Telecom and digital infrastructure operators that may qualify as critical entities should expect future assessments based on predefined administrative thresholds, even though the underlying criteria are not publicly available. The new framework supports the implementation of Romania's critical infrastructure protection regime without introducing immediate new compliance obligations.*

(3) Ministry Launches €48.8 Million Innovation Grant Scheme for IT SMEs.

In June, the Ministry of European Investments and Projects adopted and published in the Official Gazette a new state aid and de minimis scheme supporting **the development of innovative digital products, services, and applications**. The scheme provides grants ranging from €200,000 to €3 million for R&D, innovation, and commercialisation projects carried out by SMEs in the ICT sector. Eligible investments cover technologies such as AI, IoT, XR, cloud computing, cybersecurity, advanced communications, microelectronics, and smart hardware, with funding available until 30 June 2027.

***Impact:** The scheme creates significant funding opportunities for Romanian IT SMEs, start-ups, and technology developers investing in innovative digital solutions. It is also expected to benefit suppliers of cloud, cybersecurity, hardware, and consulting services involved in implementing funded projects.*

(4) Ministry Launches €17,000 Training Grant Scheme for SMEs.

The Ministry of Economy and Digitalization has adopted a new **de minimis aid scheme** under Romania's Recovery and Resilience Plan (PNRR) to support the **upskilling and reskilling of SME employees in emerging digital technologies**. Under the programme, eligible SMEs can receive grants of up to €17,000 to cover training costs in areas such as artificial intelligence, cloud computing, IoT, machine learning, blockchain, robotic process automation, and additive manufacturing. The scheme will remain open until 30 June 2026 and has a total budget of €1.7 million.

***Impact:** The scheme provides SMEs with financial support to develop advanced digital skills while reducing employee training costs. It is particularly relevant for companies investing in digital transformation and for training providers delivering courses in emerging technologies.*

(5) Government Sets Up Coordination Bodies for Black Sea AI Gigafactory Project.

Romania now has a Strategic Coordination Council for the **Black Sea AI Gigafactory** project, a flagship initiative aimed at developing one of Europe's largest AI computing infrastructures. Designed to host more than 100,000 AI chips and powered by up to 1.5 GW of clean energy, the project seeks to strengthen Europe's technological sovereignty and is currently looking for a consortium leader. The Council, together with the newly created Technical Implementation Committee, will oversee the project's strategic direction, technical implementation, and cooperation with the future consortium that will develop and operate the facility.

***Impact:** The measure is relevant for companies seeking to participate in the future consortium, as well as providers of AI, cloud, infrastructure, engineering, legal, financial, and consulting services. Businesses involved in the project will need to operate within the new governance framework, including confidentiality, coordination, and information-sharing requirements.*

(6) DNSC Proposes Authorization Scheme for Cybersecurity Training Providers.

Changing the register, the National Directorate for Cybersecurity (DNSC) launched a draft order establishing a **new authorisation framework for cybersecurity training providers**. The proposal would introduce mandatory DNSC authorisation for organisations delivering NIS2-related training, alongside rules on verification, supervision, suspension, and revocation of authorisations. It also sets standardised curriculum requirements, record-keeping obligations, and certification validity periods for training programmes aimed at management, auditors, CSIRT members, NIS2 points of contact, IT personnel, and internal trainers within essential and important entities.

***Impact:** The new rules would introduce significant compliance requirements for cybersecurity training providers, including mandatory authorisation, curriculum alignment with DNSC standards, audits, and ongoing record-keeping obligations. Essential and important entities subject to NIS2 would also need to ensure that relevant personnel receive training through recognised programmes delivered by authorised providers.*

(7) DNSC Proposes Cybersecurity Risk Management Rules for NIS2 Entities.

The second draft order issued by DNSC sets out the **cybersecurity risk management measures that essential and important entities must implement under Romania's NIS2 framework**. It requires affected organisations to adopt technical, organisational, and procedural controls based on their risk profile and assurance level. It also introduces a maturity self-assessment process through the NIS2@RO platform, minimum compliance scores, and mandatory remediation plans where the required security levels are not met. Entities already subject to the EU's DORA framework, including certain financial institutions and critical ICT service providers, are exempt from the DNSC risk assessment methodology.

***Impact:** This would require essential and important entities to translate NIS2 requirements into comprehensive cybersecurity governance, technical controls, supplier management processes, and documented compliance measures. It is expected to increase investment in cybersecurity, internal governance, audits, and resilience across the telecom and digital sectors.*

(8) Parliament Adopts Law Creating National Register of Public Digital Infrastructure.

In June, Parliament adopted a USR-signed law establishing Romania's first **unified legal framework for managing and securing public digital infrastructure**. The legislation creates the **National Public Digital Infrastructure Platform (PNIDP)**, a central register covering all digital assets used by public authorities, including domains, websites, software applications, licences, IT equipment, and publicly funded digital projects. Managed by the Romanian Digitalisation Authority (ADR), with technical support from STS and cybersecurity standards overseen by DNSC, the platform will require public institutions to register all digital resources within six months of the law's entry into force. The law is yet to be signed by the President and published in the Official Gazette.

***Impact:** This would require essential and important entities to translate NIS2 requirements into comprehensive cybersecurity governance, technical controls, supplier management processes, and documented compliance measures. It is expected to increase investment in cybersecurity, internal governance, audits, and resilience across the telecom and digital sectors.*

(9) Parliament Adopts Law on Coordinated Cybersecurity Governance and Vulnerability Disclosure.

Another law adopted by Parliament ensures that **cybersecurity research carried out in good faith, without causing harm or gaining unauthorised access, does not constitute a criminal offence**. Reported vulnerabilities must be notified within 48 hours and handled in accordance with strict confidentiality and system protection requirements. In this case as well, the law is yet to be signed by the President and published in the Official Gazette.

***Impact:** The law provides greater legal certainty for cybersecurity researchers and organisations involved in vulnerability disclosure, while strengthening cooperation between public authorities on cyber risk management. It is expected to encourage responsible security testing and improve cyber resilience across Romania's telecom and digital sectors.*

(10) EU Adopts AI Omnibus to Delay Key AI Act Obligations.

The EU will soon have a simplified AI environment after the EU Council adopted the **Digital Omnibus for AI**. For example, it postpones key compliance deadlines for high-risk AI systems until December 2027 for standalone systems and August 2028 for AI embedded in regulated products, while delaying watermarking obligations for AI-generated content until December 2026. It also introduces simplified compliance rules for SMEs, expands access to AI regulatory sandboxes, strengthens the supervisory role of the EU AI Office, clarifies the use of sensitive personal data for AI bias mitigation, and bans AI systems designed to generate non-consensual intimate or sexually explicit content. The regulation will soon be signed and published in the Official Journal of the European Union.

***Impact:** The regulation gives AI developers and deployers, including telecom and digital companies, additional time to comply with the AI Act's most demanding requirements. It also reduces the compliance burden for SMEs, expands opportunities to test AI systems in regulatory sandboxes, and provides greater legal certainty for providers of high-risk AI solutions.*

(11) European Commission Proposes EU Sovereign Cloud Framework.

The European Commission has proposed a new regulation establishing a **common EU framework for sovereign cloud services and AI infrastructure**. The proposal introduces four EU assurance levels for cloud services used by EU institutions and the public sector, requiring cloud providers to obtain the appropriate certification before supplying these customers. It also sets new rules on data localisation, operational control, software supply chain security, and independent audits for higher assurance levels. In parallel, the proposal aims to accelerate the development of AI infrastructure by introducing fast-track permitting procedures for data centres, subject to energy efficiency and sustainability requirements.

***Impact:** Cloud service providers seeking to serve the public sector would face new requirements on data governance, infrastructure location, technical support, software supply chain security, and compliance audits. The proposal would also create faster permitting opportunities for data centre operators while encouraging investment in secure and sustainable cloud and AI infrastructure across the EU.*

What to Watch in September

Disclaimer: Since the Parliament begins its summer vacation period today, its activity will be resumed in September, when the debate on pending bills will commence.

(1) Deputies to Reject Tightened EU Cookie Consent Rules for Telecom Providers.

A legislative proposal expected for final vote in the Chamber of Deputies in September introduces **new rules on how telecom operators and digital service providers obtain user consent for cookies and similar technologies**. The proposal has already been rejected by the Senate and is unlikely to pass. It requires equal visibility for accept and reject options, bans pre-checked boxes, and ensures users can easily withdraw consent. Providers must also be able to prove when and how consent was given.

***Impact:** Telecom and digital companies would need to redesign consent banners and user interfaces. They would also need stronger systems to record and prove user consent.*

(2) Unified Registry for Public Digital Infrastructure, Possible Adoption.

Instead, the deputies could adopt a USR legislative proposal that creates Romania's first **unified legal framework for managing public digital infrastructure**. The law establishes the National Public Digital Infrastructure Platform (PNIDP), a central registry covering all digital assets used by public institutions, including websites, applications, software licences, IT equipment, and publicly funded digital projects. The platform will be managed by the Romanian Digitalisation Authority (ADR), with technical support from STS and cybersecurity standards set by DNSC.

***Impact:** The law would significantly increase requirements for public sector digital governance and IT system integration. Technology providers working with public authorities would need to align with new interoperability, security, and registration requirements under the PNIDP framework.*