CMS | Romania implements public platform for digital infrastructure

On 3 July 2026, Romania published Law No. 119/2026 on the recording, administration, use and security of public digital infrastructure in Romania and the establishment of the National Platform for Public Digital Infrastructure (PNIDP). The law will enter into force on 3 January 2027 and introduces a centralised inventory of public digital resources used by Romanian public authorities and institutions.

The law is part of a broader trend towards strengthening digital governance, cyber resilience and interoperability across the Romanian public sector.

The timing is not accidental. Over the past few years, Romania has implemented the Government Cloud project, expanded the national interoperability framework and transposed the NIS2 Directive through the national cybersecurity framework. Yet one fundamental challenge has remained: public authorities often operate hundreds of digital assets, software systems, websites, databases and licences without a unified mechanism for inventory, oversight and verification. According to the law's explanatory memorandum, this fragmentation creates cyber risks, duplication of costs, limited interoperability and reduced transparency. Law 119 seeks to address precisely this gap.

What is the PNIDP?

The PNIDP is designed as the primary information system and the official inventory of public digital resources used, administered or owned by public entities.

The platform is expected to include information relating to institutional domains and subdomains, official email addresses, official phone numbers, websites and digital portals, software applications and digital platforms, software licences, hardware assets and public digital projects.

The PNIDP consists of specialised registries designed to catalogue the categories of public digital resources, which are in turn recorded in the National Interoperability Platform.

The Authority for the Digitalisation of Romania (ADR) is designated to monitor compliance, implement up-to-date technical standards and collaborate with competent authorities in the cybersecurity sector for the efficient functioning of the platform.

Why does the law matter from a NIS2 perspective?

Although Law 119 is not formally part of Romania's NIS2 transposition package, the two frameworks are closely interconnected. Law 119 expressly provides that public digital resources registered in the PNIDP are subject to the provisions of Government Emergency Ordinance No. 155/2024, Romania's NIS2 implementing framework. As a result, public authorities must inventory their digital resources and ensure that these resources are governed and protected according to the cybersecurity requirements applicable under the NIS2 regime.

From a cybersecurity perspective, asset management is the foundation of any effective cyber risk management programme. Organisations cannot meaningfully protect assets they have not identified, inventoried or classified. Public authorities may struggle to assess vulnerabilities, manage supplier dependencies, implement appropriate security controls or respond effectively to incidents where they lack a complete overview of the systems, applications and digital resources under their control.

In this context, PNIDP goes beyond a simple administrative register. By creating a centralised inventory of public digital resources across the Romanian public sector, the platform may provide authorities with greater visibility over the digital assets supporting public services. This is particularly relevant in an environment where cybersecurity risks increasingly affect interconnected systems rather than isolated entities. A consolidated picture of public digital infrastructure may facilitate the identification of systemic vulnerabilities, improve coordination between authorities and support the development of cybersecurity strategies and remediation measures at a national level, rather than on a purely institution-by-institution basis.

Law 119 addresses this issue by requiring the registration and continuous updating of public digital resources while also linking cybersecurity responsibilities to designated digital representatives.

The law therefore introduces an additional governance layer that supports the practical implementation of cybersecurity obligations under the NIS2 framework. While NIS2 focuses on risk management, incident reporting and resilience measures, Law 119 seeks to ensure that public authorities establish and maintain a reliable inventory of digital resources to which those obligations apply.

Key obligations for public entities

Public entities will face the following obligations:

→ They must appoint a digital representative to manage information recorded in PNIDP. Where no such representative is appointed, liability falls on the head of the institution.
→ Within six months after the law enters into force, public entities must register all public digital resources they own, use or administer. Changes must be recorded within 15 days or within five days in urgent situations.
→ Any breach or cybersecurity incident must be reported to the National Directorate for Cybersecurity (DNSC) via the national cybersecurity incident reporting platform, as part of public entities' obligations under the NIS2 legal framework.

Software reuse and procurement efficiency

Law 119 allows the redistribution of unused software licences between public entities, subject to ADR approval and contractual limitations. The law also requires certain publicly funded digital resources to be made available for reuse by other public entities where appropriate.

For technology suppliers, software vendors and public procurement contractors, these provisions may influence future contracting models, licensing structures and intellectual property arrangements.

Categorisation of information available on the PNIDP Platform

The data included on the PNIDP will be classified into three categories:

→ "public data" pertains to identification and purpose information about public digital resources, which is openly accessible to anyone;
→ "internal data" refers to technical information about the internal structure of digital resources, which is accessible only to designated authorities;
→ "sensitive data" pertains to critical cybersecurity information accessible only to the ADR and other specific organisations on a need-to-know basis.

Public data registered in the PNIDP is made publicly available through the national open data portal at https://data.gov.ro/ where any person can verify the authenticity of a public digital resource and confirm the public entity it belongs to. In case of discrepancies between the data recorded in the PNIDP and data contained in any other public records, PNIDP data prevails until proven otherwise.

Sanctions

Law 119 imposes fines ranging from RON 5,000 to 10,000 on digital representatives or heads of public entities for non-compliance with registration deadlines, corrective measures and resource-sharing obligations. Repeat offences occurring within six months may trigger suspension of access to PNIDP functions until compliance is restored.

Beyond administrative fines, the law provides that unregistered public digital resources cannot benefit from financing or modernisation projects. In practice, this means that authorities seeking funding for upgrades, migrations or digital transformation initiatives may first need to demonstrate that the relevant assets have been appropriately recorded in PNIDP.

Looking ahead

Many practical aspects remain unclear and will depend on the methodological norms and technical standards to be adopted after the law enters into force.

The direction, however, is clear. Law 119 moves Romania away from a fragmented model of digital administration towards a framework based on visibility, accountability, interoperability and cyber resilience.

Law 119 should be viewed as part of a wider effort to strengthen the resilience of Romania's public-sector digital infrastructure. Recently, public authorities have become targets of sophisticated cyberattacks capable of disrupting essential public services, affecting the availability of critical systems and exposing sensitive information. Against this backdrop, greater visibility over public digital assets, clearer governance structures and stronger accountability mechanisms are becoming cybersecurity necessities rather than mere administrative requirements.

Law 119 is expected to be complemented by additional technical and organisational measures to enhance the cybersecurity posture of public authorities.

Cybersecurity can no longer be treated as a purely technical matter delegated to IT departments. As digital public services become increasingly interconnected and essential to the functioning of the state, authorities will need to strengthen governance, improve oversight of digital assets and ensure that resilience considerations are embedded into day-to-day operations. Doing so is not only necessary for compliance purposes, but also for ensuring the continuity of public services, protecting public-sector data and maintaining citizens' trust in digital government services.

For more information on recent legislative developments affecting the Romanian cybersecurity framework, contact your usual CMS contact or the authors of this article, **Cristina Popescu**, **Florentin Giurgea** and **Carmen Turcu**. This article was written with the support of student **Vanessa Chioaru**.