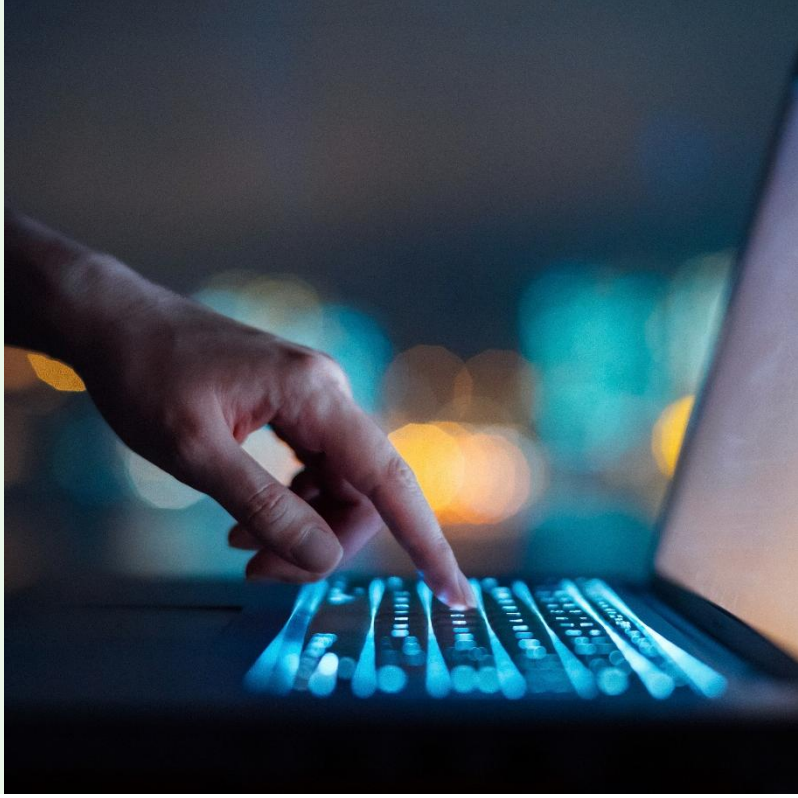
Clifford Chance
Badea Association

BRIEFING



Navigating NIS2: Cybersecurity compliance obligations for Romanian companies

December 2025

The Government Emergency Ordinance no. 155/2024 ("**GEO 155/2024**") on the cybersecurity of networks and information systems, as approved and amended by Law no. 124/2025, fully transposes the NIS2 Directive into Romanian law and significantly expands the cybersecurity related obligations applicable to entities operating in critical sectors (e.g. energy, tech, finance, transportation, healthcare, food, etc).

The National Cybersecurity Directorate's ("**DNSC**") Orders no. 1/2025 and 2/2025, entered into force at the end of August 2025, approved the instruments for concerned entities to register with DNSC, as well as the rules on self-assessment and documenting the cyber risk profile.

At the end of October 2025, DNSC published for consultation a draft order on regulatory control and sanctioning, which has not yet entered into force. The draft order details DNSC's powers and procedures for ad-hoc and planned audits, including the authority to request information, impose and monitor remediation measures, the right to be granted access to premises, hardware and software equipment, as needed for effective oversight.

Key issues

- Concrete obligations under GEO 155/2024 apply mainly to "essential" and "important" entities, generally medium and large organisations meeting specific size and relevance criteria in the sectors listed in the Annexes to GEO 155/2024.
- All qualifying entities must notify DNSC for registration in the Register of Essential and Important Entities following the steps provided under DNSC Order 1/2025.
- Executive management members are required to designate cybersecurity officers and dedicated staff, allocate adequate resources, attend accredited training, approve and supervise cybersecurity risk management measures, and may be held personally liable for breach of their obligations.

- Companies must notify major cyber incidents to DNSC within 24 hours (early warning), follow up with a detailed report within 72 hours, and submit a final report within one month, with a separate 6-hour deadline to notify incidents with potential cross-border impact.
- Non-compliance can attract fines of up to EUR 10 million or 2% of worldwide turnover for essential entities, and up to EUR 7 million or 1.4% of worldwide turnover for important entities.

Essential vs. important entities – classification criteria and regulatory impact

NIS2 obligations apply to entities operating in sectors and subsectors that are considered critical for the national civilian cyberspace, including, among others, energy (e.g. energy producers, suppliers and distributors), digital and telecom infrastructure, banking and financial services, transportation, life sciences, water supply and waste management services, food production and distribution, as well as certain manufacturing sectors (e.g. medical devices, electronics, electrical equipment), as such are listed in Annex 1 and Annex 2 to GEO 155/2024.

Entities in the sectors listed by GEO 155/2024 will be under the umbrella of the NIS2 obligations if they are classified as essential or important entities, based on criteria such as: "International sanction" now expressly covers UN, EU, unilateral measures implemented by Romania, and other international restrictions.

- sector and type of service provided;
- enterprise size (NIS2 obligations mainly apply to medium or large enterprises, based on number of employees, turnover, total assets); and
- risk-level, assessed based on a series of criteria, such as whether the entity is the sole or main provider of a critical service, the potential impact on public safety, national security or public health, as well as cross-border impact of a service disruption.

DNSC may designate entities as essential or important on a case-by-case basis even where criteria such as enterprise size is not fulfilled, if disruption of services would have significant societal or economic consequences (for example, where an entity is the only provider of a particular critical service).

Registration with DNSC and initial compliance milestones

All qualifying entities under GEO 155/2024 have an obligation to register in the **Register of Essential and Important Entities** (the **"Registry**") kept by DNSC.

Key steps of the registration and notification process include:

- **Mandatory notification**: entities must submit to DNSC a detailed notification within the prescribed 30-day deadline (starting as of 20 August 2025, for entities already qualifying under GEO 155/2024 criteria, or as of the date of an entity entering the scope of GEO 155/2024);

- **Notification form**: the form requires comprehensive information about the entity (*i.e.* identification and contact details, size and financial indicators, mapping of services to the list included in the annexes to GEO 155/2024, etc);
- **Preliminary self-assessment**: as part of the filling in of the notification form entities must assess and advance a proposal for their classification as essential or important, based on their own risk assessment and the criteria provided for in the legislation;
- **DNSC decision**: following the review of the notification, DNSC issues a decision within 60 days for essential entities and within 150 days for important entities, either (i) registering the entity as essential or important, as applicable, or (ii) confirming that the entity falls outside the scope of GEO 155/2024 obligations.

Once DNSC has formally designated the entity as essential or important and mandated registration with the Registry, the entity becomes subject to a set of obligations, including clear deadlines, such as:

- appointment of a cybersecurity officer and dedicated staff within **30 days** of notification of the DNSC decision;
- submission to DNSC of a risk-level assessment within **60 days** of notification of the DNSC decision;
- performance of an internal self-assessment of the maturity of the cybersecurity risk-management measures within **60 days** as of submitting with the DNSC the above risk level assessment.

Ongoing risk management, incident reporting and enforcement

Once designated as important or essential and registered with the Register, entities are required to operate an ongoing cybersecurity governance and risk-management framework under the direct oversight of their management bodies, including:

- performing annual internal cybersecurity maturity self-assessments and submitting such to DNSC;
- undergoing periodical external cybersecurity audits with follow-up remediation tracked and reported;
- reporting significant cybersecurity incidents to DNSC within strict deadlines (24-hour early warning, 72-hour detailed report, one-month final report, plus a 6-hour deadline where cross-border impact is suspected).

In the event of non-compliance, entities may be subject to warnings or fines of up to EUR 10 million or 2% of their worldwide annual turnover for essential entities, or up to EUR 7 million or 1.4% of their worldwide annual turnover for important entities, together with remediation measures. When such sanctions are not considered sufficient by DNSC, partial or total suspension of services may be requested by DNSC from competent regulatory authorities.

Specific obligations incumbent upon the executive management (such as obligations to appoint cybersecurity offices and dedicated staff, to appoint a permanent contact point for DNCS, to dedicate resources for and to supervise the implementation of cybersecurity risk management measures

may also result in personal liability of the management members. DNSC may also request temporary prohibition of a management member to exercise a management level position.

Ecaterina Burlacu
Counsel, Bucharest

ecaterina.burlacu@cliffordchancebadea.co
+40 21 6666 144

Filip Marinau
Associate, Bucharest

filip.marinau@cliffordchancebadea.com
+40 21 6666 130

Persida Ciobanu
Associate, Bucharest

persida.ciobanu@cliffordchancebadea.com
+40 21 6666 105