Cybersecurity: Romania transposes the NIS2 Directive. What's next?

Directive (EU) 2022/2555 (NIS2) aims to further strengthen the cyber resilience of the EU by requiring entities in various sectors to dial up their cybersecurity efforts. NIS2 replaces the former NIS1 Directive (EU) 2016/1148, expands the range of entities falling under its provisions, and introduces stricter requirements for these entities.

On 31 December 2024, the Romanian government passed Government Emergency Ordinance no. 155/2024 (GEO 155/2024) transposing NIS2 into national legislation.

Whom does it concern?

NIS2 and GEO 155/2024 target entities across various industry sectors and categorises them into essential and important entities. Entities active in the following areas should check whether NIS2 and GEO 155/2024 apply to them:

(i) essential entities: energy (electricity, district heating and cooling, oil, gas, hydrogen); transport (air, rail, water, road); banking; financial market infrastructures; health; drinking water; wastewater; and public administration and space. Even stricter obligations apply to digital infrastructure and ICT service management;

(ii) important entities: postal and courier services; waste management; manufacture, production and distribution of chemicals; production, processing and distribution of food; manufacturing of medical devices; computer, electronic and optical products; electrical equipment; machinery and equipment; motor vehicles, trailers and semi-trailers and other transport equipment; digital providers of online marketplaces, search engines, and social networking.

Even though size thresholds are in place (NIS2 and GEO 155/2024 apply mainly to medium and large enterprises), an entity falling under these thresholds can still be subject to these legal provisions due to its critical role in a specific sector. Some obligations extend to suppliers of such entities, as NIS2 also aims to raise the cyber preparedness of supply chains.

What must be done?

If an entity has determined that it falls under NIS2 and GEO 155/2024, it must comply with all obligations and

requirements laid down in this legislation for the respective type of entity.

GEO 155/2024 outlines several obligations for the entities subject to its provisions, including, but not limited to, the following:

→ Implement appropriate and proportional technical, operational, and organisational measures to manage security risks and minimise the impact of incidents on information systems, adhering also to sector-specific requirements;
→ Register with the Romanian National Cybersecurity Directorate ("DNSC"), the authority responsible for enforcing GEO 155/2024 provisions;
→ Conduct audits at regular intervals and communicate their results to the DNSC;
→ Ensure management undergoes cybersecurity training and that the individual responsible for cybersecurity decisions operates independently from the operational Head of IT;
→ In the event of a cybersecurity incident, notify authorities within six and 24 hours, and—depending on the circumstances—inform affected individuals or contractual partners when necessary.

Sanctions

GEO 155/2024 establishes a framework of multiple obligations in which each breach of an individual type of obligation is sanctioned with a fine (e.g., failure to register with the DNSC, not performing the required audits, or not communicating their results to the DNSC). Fines can reach up to EUR 10 million or 2% of annual worldwide turnover, whichever is higher, for essential entities, and EUR 7 million or 1.4% of annual worldwide turnover, whichever is higher, for important entities.

In addition, NIS2 and GEO 155/2024 legislate the personal liability of individuals from management for non-compliance.

Next step?

GEO 155/2024 established a deadline for registering with the DNSC that elapsed on 30 January 2025. However, at present, the DNSC has not yet issued the application norms required to perform the registration of essential and important entities.

According to a press release available on the DNSC website, registrations will be performed based on the application norms that the DNSC commits to issue in Q1 2025. After the necessary application norms will be issued, relevant entities will have to register with the DNSC in the prescribed manner and deadlines.

As non-observance of regulatory cybersecurity obligations could lead not only to fines for both the company and management, but also to damage claims from contractual partners (if the latter suffer losses following an incident that could have been prevented or mitigated if the prescribed measures would have been in place), relevant entities should take the necessary actions to comply with these legal requirements as soon as possible.