Cybersecurity in Romania: New obligations for companies

by Sonia Benga, Avocat (Attorney at Law RO)

Emergency Ordinance 155/2024 establishing a framework for the cybersecurity of networks and information systems in the civilian national cyberspace ("**EO 155**") was adopted at the end of last year and came into force on December 31. The basics can be found in our last report:

https://stalfort.ro/wp-content/uploads/2025/03/NIS-2_implemented_in_Romania_extended_obligations_on_cyber_and_information_security.pdf

Six months later, Law 124/2025 approving EO 155 ("**the Law**") was passed. This law not only approves EO 155 but also partially amends it. Key aspects of the EO were clarified, tightened, or expanded, and vague provisions were improved.

The law, which came into force on July 10, 2025, must be taken into account by many companies operating in Romania, as the current changes are relevant to their practices.

Expansion and clarification of scope

Perhaps one of the most important changes brought by the law is the expansion of EO 155's scope by including certain institutions in the public health and food sectors among the entities classified as critical.

Annex 1 to the EO, which lists the entities classified as critical, is expanded to include those that:

- hold a wholesale distribution license for pharmaceuticals;
- engage in wholesale and retail trade of pharmaceutical and medical products (CAEN codes 4646 and 4773 according to CAEN Rev. 3.).

Furthermore, it is now explicitly clarified that companies involved in the production, processing, and/**or** distribution of foodstuffs are generally subject to EO 155.

These clarifications are significant for companies that were previously unsure whether they were affected by the law or not. This applies, for example, to medium-sized and large companies involved in the distribution of food. Arguments previously made that this activity was not covered by EO 155—unless it was combined with production or processing—are no longer valid.

Deadlines and appointment of an NIS officer

According to EO 155, affected companies were already required to appoint a person responsible for the security of network and information systems. However, no specific deadline was set for when essential and important entities had to make this appointment. The law now sets a clear timeframe; the responsible person must be appointed within 30 days of receiving the DNSC Director's decision on entry in the official register.

Another change concerns deadlines for implementing corrective measures to remedy deficiencies identified during inspections. Previously, the EO only required entities to prepare an action plan within 15 days of receiving a request, with self-set deadlines for implementation.

The new version now includes the obligation to comply with these self-imposed deadlines and to submit evidence of implementation within 5 days of their expiry.

Clarifications regarding security incidents

Since EO 155 was unclear in its definition of the term “significant event,” the law now defines it more precisely. An event or its impact is considered significant if it:

- **has** caused or may cause serious operational disruptions to the services or financial losses for the company concerned;
- **or** other natural or legal persons who have caused or may cause significant material or immaterial damage.

In anticipation of new regulations

Secondary legislation is still required to fully implement EO 155. This includes criteria and methods for risk assessment, rules for reporting incidents, requirements for notification and information transfer, measures for risk management, and regulations for the organization of cybersecurity bodies.

Since April 30, several draft regulations have been published outlining these criteria and methods. However, these regulations remain in draft form and have not yet been adopted, despite the public consultation process having been completed.

Conclusion

Although secondary legislation on cybersecurity is still pending, Law 124 introduces several necessary and welcome clarifications. By combining its provisions with the draft regulations published by the DNSC, companies can better prepare for their obligations in this area.

Contact and further information:

STALFORT Legal. Tax. Audit.
Bucharest – Bistrița – Sibiu

Office Bucharest:
T.: +40 – 21 – 301 03 53
F: +40 – 21 – 315 78 36
M: bukarest@stalfort.ro
www.stalfort.ro