



## PRESS RELEASE

### **In the context of Russian Federation's invasion against Ukraine, Romania adopted the law that forbids procurement or use by any public body of cyber or information security products and services coming directly or indirectly from the Russian Federation**

**Bucharest, 14<sup>th</sup> of December 2022**

Today, December 14, 2022, the [Law on the Protection of Information Systems of Public Authorities and Institutions in the Context of the Russian Federation's Invasion against Ukraine](#) was published in the Official Gazette, and therefore enters into force. The law was initiated by the Romanian Ministry of Research, Innovation and Digitalization (MCID) and was voted by the Parliament on 23.11.2022.

The law establishes the legal and institutional framework for prohibiting the acquisition and use by public authorities and institutions of cybersecurity and information security software products and services coming directly or indirectly:

- from the Russian Federation;
- from an economic operator under the direct or indirect control of a natural or legal person in the Russian Federation;
- from an economic operator whose capital is constituted with a shareholding coming directly or through interposed firms from the Russian Federation, or whose administrative bodies include persons from the Russian Federation.

The law covers all networks and information systems that manage classified information, owned by public or private entities, located on the territory of Romania, with the exception of those owned by public authorities and institutions with responsibilities in the domain of national security, cybersecurity, defense or public order.

The security of hardware and software products and the level of trust in them are vital for ensuring the resilience of networks and information systems at national level. In the context of Russia's war in Ukraine and of the related cyber-attacks, some of which targeting and impacting Romanian governmental bodies, organizations and users, it is also necessary to secure the supply chain by establishing trust criteria for equipment and service providers alike.

The Romanian National Cyber Security Directorate (DNSC), together with the Romanian Digitalization Authority (ADR), the Romanian Intelligence Service (SRI), the Ministry of National Defense (MapN), the Ministry of Internal Affairs (MAI), the Special Telecommunications Service (STS), the Protection and Guard Service (SPP) and the Office of the National Register of State Secret Information (ORNISS), have a mandate and an active role in identifying the products and services covered by this law.

The law has a direct impact only on certain categories of stakeholders, however the Directorate recommends to all impacted Romanian users and decision to carefully assess the security solutions they use, in the context of the hybrid conflict between Russia and Ukraine.

The Directorate's team will provide assistance to entities or users who need support in this case, as usual. You can contact us via phone, at the national cyber emergency number 1911, or at [office@dnsc.ro](mailto:office@dnsc.ro).

**Press Contact: Mihai Rotariu | [mihai.rotariu@dnsc.ro](mailto:mihai.rotariu@dnsc.ro) | 0740 066 866**