May 2026

HOPE contribution to the public consultation on the targeted NIS2 amendment Directive

HOPE acknowledges the Commission proposal for a Directive amending Directive (EU) 2022/2555 ("NIS2") as regards simplification measures and alignment with the proposal for the Cybersecurity Act 2. The delays experienced in the national NIS2 transposition demonstrated that its implementation is challenging for entities regulated by it, including in the hospital sector where financial, human, and operational resources are insufficient in many places for adapting to fast-evolving digital policy frameworks. Hence, the clarifications on the scope and mechanisms facilitating compliance with NIS2 contained in the targeted amendment are timely and appreciated.

As highlighted by HOPE also in relation to the Digital Omnibus and Cybersecurity Act 2 proposals, a robust and forward-looking EU regulatory framework is crucial for ensuring the security of increasingly data-rich systems, equipment, devices, and processes deployed in healthcare. As part of patient care, the implementation of NIS2 and the Action Plan on the Cybersecurity of Hospitals and Healthcare Providers are essential for safeguarding the effective day-to-day operations of this critical sector, protecting individuals' safety, privacy, and fundamental rights, and supporting the knowledge and actions of staff. Cybersecurity measures must include clear guidelines and tailored training to ensure that staff at all levels, as well as external partners, are able to assume responsibility according to their respective roles.

HOPE therefore supports cyber measures that raise the standard across the EU and provide concrete additional support to national authorities and entities in scope of NIS2, in particular the guidelines on the application of supply chain security requirements (ensuring they benefit entities as much as their suppliers), the requirement for Member States to include the migration to post-quantum cryptography in national cybersecurity strategies, and the purposeful relaunch of cybersecurity certification schemes that could enable hospitals operating in a cross-border context to attest their cyber posture.

HOPE is also in favour of an enlarged mandate and budget for ENISA, which will further expand its coordination activities including supporting the Member States in supervising entities providing services or cooperating cross-border, facilitating mutual assistance, and conducting a comprehensive mapping of entities in scope of NIS2. While remaining subject to NIS2 requirements, HOPE understands that clinics falling in the new small mid-caps category will no longer be considered as "essential" but as "important" entities, subject to a lighter supervision and compliance regime. The consequences of this shift should be clarified.

Regarding the single-entry point for incident reporting to be developed and maintained by ENISA, already introduced in the Digital Omnibus, HOPE is generally in favour of streamlined reporting, as long as such a mechanism does not disrupt the maintenance of effective and trusted communication flows in place at national level, the precise workings of which, and networks involved, differ between Member States.

Similarly, HOPE is generally in favour of a maximum harmonisation of Implementing Acts specifying cybersecurity risk-management measures, but this should not prevent national authorities to continue to apply tried-and-tested measures meeting national needs, in line with Article 5 that leaves room for higher levels of cybersecurity where appropriate.

Finally, HOPE supports the introduction of harmonised collection of data on ransomware attacks as presented in the proposal, i.e. information about actual ransom payments should be restricted to requests of national CSIRTs or competent authorities, which should only be issued if necessary and for transparent reasons. There is a difference between collecting information about ransomware attack incidents and about payments; the latter is a lot more sensitive given the dynamic and complex cyber threat landscape. The "no ransom payments" policy of the International Counter Ransomware Initiative may not always be a viable option for critical entities. Depending on the precise nature and disruptive impacts of the threats they are faced with, hospitals may be forced to negotiate in certain cases. Obtaining a better overview of the ransomware problem in the EU would be useful, but caution must be taken regarding entities' liability and drawing conclusions from such information, which could be incomplete or skewed.

****

HOPE, the European Hospital and Healthcare Federation, is a European non-profit organisation, created in 1966. HOPE represents national public and private hospitals associations and hospitals owners either federations of local and regional authorities or national health services. Today, HOPE is made up of 36 organisations coming from the 27 Member States of the European Union, as well as from the United Kingdom, Switzerland and Serbia as observer members. HOPE mission is to promote improvements in the health of citizens throughout Europe, high standard of hospital care and to foster efficiency with humanity in the organisation and operation of hospital and healthcare services.