May 2026

HOPE contribution to the public consultation on the Cybersecurity Act revision

HOPE welcomes the proposal for a revised Cybersecurity Act (CSA2) in light of a changed cybersecurity threat landscape characterised by new threats and uncertain future developments hospitals and health services are facing. A needs-focused yet flexible horizontal cybersecurity framework is important at a time when AI-enabled automated attacks and social engineering, refocused ransomware attacks (including state-sponsored) and advances in quantum computing are exploited.

Given the scale and urgency of the threat, which has increased significantly since 2019, and its potential for causing enormous disruption to health systems and harming lives, HOPE supports modernising the Act to take account of novel threats and anchor cybersecurity within a holistic perspective of the geopolitical and digital sovereignty threats Europe is facing.

A prerequisite is to clarify ENISA's role and entrust it with an expanded mandate and financial and human resources. With an evolving EU cybersecurity framework – comprising also the NIS2 Directive, Cyber Resilience Act, Cyber Solidarity Act, and key sectorial initiatives like the Action Plan on the Cybersecurity of Hospitals and Healthcare Providers - ENISA's coordination tasks are pivotal. As a central hub, it is ideally situated to develop an overview of EU and national cybersecurity laws and requirements. The agency is well-positioned to identify gaps and overlaps, and to create mechanisms and conditions that help national stakeholders navigate the regulatory landscape. ENISA should propose solutions and services based on best practices.

HOPE thus agrees with the tasks outlined in Articles 10-16, including the development of cyber threat intelligence repositories, situational awareness actions, issuing early alerts, supporting incidence response by mapping the services of the EU Cybersecurity Reserve, facilitating Union-level cybersecurity exercises and extracting lessons learnt, and providing vulnerability management services. However, a strengthened ENISA should not supplant national CSIRTs or other trusted networks closely working with national authorities and critical entities.

ENISA should maintain steady dialogue with third countries without infringing upon the Member States' national security competences. The proposed mechanism, as part of de-risking ICT supply chain, to identify countries that could pose security risks, could bring added EU value and complement the CER Directive's "all hazards" approach. Considering non-technical risks including geopolitical dependencies is relevant as the threat landscape becomes unpredictable. In healthcare, well-founded restrictions on high-risk suppliers and their products or critical components could avoid harm. However, HOPE appreciates that assessing non-technical risks is complex and the responsibility of national authorities. Following Article 98, an EU mechanism would be created to identify key ICT assets in critical ICT supply chains and set out mitigation measures where protection from designated countries and entities or suppliers is warranted. Clarification is needed to understand the impacts of

measures and exceptions to ensure they are in the public interest. Certain healthcare product components are scarce, and diversification of supply is difficult to achieve.

The relaunch of the EU Cybersecurity Certification Framework to make certification schemes more practical could be useful for hospitals to make informed purchasing decisions and demonstrate their cybersecurity posture. This could build trust in the digitalisation of the sector. However, there are differences between hospitals based on their function and size, ICT budgets, location, expertise, etc. Certification should remain voluntary and not carry negative consequences. Granting ENISA a leading role in preparing schemes and capacity-building should ensure effectiveness.

The implementation of the Cybersecurity Skills Academy should increase the available expertise in the healthcare sector, helping to ensure an even spread of knowledge across the EU and counter fragmentation in digital literacy.

Regarding the single reporting platform pursuant to the Cyber Resilience Act and single entry point for incidence reporting, their development and operation should occur in close collaboration with the Member States and CSIRTs; where feasible, they should redirect to national platforms to avoid disrupting trusted communication flows.

The CSA2 would benefit from clearer definitions to remove inconsistencies with other EU legislation, better explanations of overlapping requirements, and adequate implementation funding.

****

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.