April 2026

HOPE contribution to the "Draft Commission guidance on the Cyber Resilience Act"

HOPE welcomes the publication of the draft Commission guidance on the application of the Cyber Resilience Act (CRA) as an indispensable reference document addressed to economic operators and supporting the activities of market surveillance authorities, notifying authorities and notified bodies. At the same time, the document holds value for critical entities as purchasers and deployers of products with digital elements.

In particular, HOPE appreciates the clear examples provided in the guidance, which help to illuminate and clarify key CRA provisions and concepts, from the types of products subject to the act to their "placing on the market", the distinction between "important" and "critical" products, rules pertaining to free and open-source software (FOSS), clarifications on what constitutes substantial modifications, as well as remote data processing.

From a hospital perspective, given the sheer diversity of products covered and their uses within and outside different healthcare settings, it is important to establish the right balance between stipulating robust, forward-looking cybersecurity requirements covering all reasonably conceivable risks and ensuring that deployers and providers can harness their practical and innovation value.

However, HOPE is concerned that certain provisions of the Commission's CRA guidance, which sets an EU-level baseline, could compromise the Member States' ability to maintain established cybersecurity rules and processes for critical infrastructure which, although aligned with the CRA, allow for interpretations in line with national preferences. Several are more advanced and rigorous than those described in the draft Communication. Examples include national implementation practices based on more detailed technical guidelines on essential requirements; cybersecurity risk assessment and vulnerability handling regimes involving independent third parties; incident reporting portals closely tied to national CSIRTs, placing higher pressure on manufacturers than a single-reporting platform; and more solid certification schemes and security standards as part of national cybersecurity strategies.

Hence, it is vital that the CRA guidance does not inadvertently weaken regulatory frameworks for products with digital elements. Notably, the CRA gives manufacturers greater self-assessment powers for conducting cybersecurity risk assessments and demonstrating compliance with vulnerability handling requirements than is currently the case in some Member States. This could lead to loss of control over the demonstrability of security and privacy by design, in turn eroding hard-won trust in national cybersecurity authorities and processes.

Regarding substantial modifications, HOPE supports issuing more detailed guidance on CRA rules pertaining to certain security updates, given the need to enable brisk incident responses to fast-moving cybersecurity threats. Similarly, the interplay between NIS2 and CRA reporting obligations (which

involves different systems for manufacturers and hospitals), and compliance with MDR/IVMR and CRA requirements warrants further clarification given the multitude of digital products in hospitals and their context-specific uses. Overall, the CRA must neither cause unnecessary delays nor result in an under-reporting of incidents.

Since the lifespans of hospital systems and equipment differ from the short product cycles of the CRA, HOPE thinks it is necessary to define "reasonable" support periods in the guidance. Manufacturers' obligations to provide security updates throughout the promised lifecycle must be clear.

A strong EU cybersecurity regulatory framework does not contradict commercial objectives: if designed well, it can be a powerful incentive to increase patient safety and stimulate the profitable development of secure and sovereign technology that meets the everyday needs of health system stakeholders and reflects the value- and rights-based EU approach.

****

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.