September 5, 2026

HDS's commitment to the EU Cyber Resilience Act

HDS is well prepared for the Cybersecurity Act (CRA), which sets cybersecurity standards for connected digital products sold within the European Union. HDS is constantly working to comply with the CRA's vulnerability reporting obligations, effective from September 11, 2026, and will meet the requirements for the firm's products, which will come into effect on December 11, 2027.

The company shall implement organisational and technical measures to comply with the reporting obligations under Article 14 of Regulation (EU) 2024/2847. The preparation shall include the designation of responsible persons, the provision of access to the CRA Single Reporting Platform and the development of a procedure for assessing and reporting actively exploited vulnerabilities and serious security incidents within the legal deadlines. This statement describes the state of preparation and does not confirm the completion of the implementation of the above measures.

HDS's cybersecurity practices comply with the CRA's obligations regarding basic product requirements, vulnerability resolution, and user guidance. We adhere to the key principles covered by the CRA: Secure by Design, Secure by Default, Lifecycle Management, and Transparency.

HDS adopts a comprehensive lifecycle approach to security and implements stringent risk mitigation measures for products before and after they are sold. The HDS security development model reflects the principle of Secure by Design, guides software development to ensure security integration from the earliest stages of development and minimizes the risk of introducing products with exploitable vulnerabilities. HDS also implements supply chain controls to mitigate the risk of compromised components.

HDS products support the CRA requirement for Secure by Default configurations. No default credentials are used. In addition, support for centralized identity management and step-by-step instructions for our products helps customers deploy and maintain a resilient security posture.

As a member of the Common Vulnerabilities and Exposures Numbering Authority (CNA), HDS adheres to a vulnerability management policy for responsible public disclosure of security incidents and newly discovered software vulnerabilities. Customers can be notified through our notification service and receive software updates on video and device management applications from HDS and our partners.

Transparency is the basis of our operation. In addition to communication, we also document a list of materials (SBOM) products

Cybersecurity is an integral part of HDS's offering. We remain committed to raising the bar for cybersecurity security and responding to the ever-changing threat landscape.

Martin Murín CEO of
HDS a.s.

