

**CYBERFORT CONSORTIUM WILL ORGANIZE THE 2<sup>nd</sup> GENERAL ASSEMBLY MEETING**  
24<sup>th</sup> of February 2026, Carina Ioana NITA

The CYBERFORT Consortium will convene the 2<sup>nd</sup> General Assembly Meeting on 3<sup>rd</sup> of February 2026, taking place in Bucharest, Romania, with the option to participate online. The objectives of the *Strengthening Cyber Defenses of SMEs for Cyber Resilience Act (CRA) Compliance Project* are: aiming to simplify the process of CRA compliance for Small and Medium Enterprises (SMEs); enhancing the efficiency of compliance documentation processes through automation. The Project is delivering training to elevate the cybersecurity knowledge and practices among SMEs; ensuring the tools evolve in response to new cybersecurity challenges and feedback from users; and fostering collaborations with cybersecurity networks and initiatives across Europe.

The Agenda of the 2<sup>nd</sup> General Assembly Meeting highlights very important topics: CYBERFORT Project Objectives & Guidelines; the Progress of the Management and Coordination of the Project; Amendment regarding the 2 months extension; Use Cases Definitions, Scenarios and CRA Analysis and compliance; CRA Compliance Automated Tool Development; CYBERFORT GRC Platform presentation and Requirements, Design, Architecture and Integration Plan; and CYBERFORT Platform Evaluation through Pilots Execution.

Furthermore, Dissemination, Exploitation and Stakeholders Involvement will also be presented, providing an overview of actions implemented to date, tools and channels used, and results achieved so far. Planned future activities will be outlined, alongside key messages and target audiences, creating space for coordination and alignment to maximise the project's visibility, impact, and long-term uptake of its outcomes. Business Modelling and Exploitation Activities, Replicability and Market Analysis will be discussed as well.

Moreover, dedicated Cybersecurity CRA-specific training sessions will be organized, alongside targeted outreach to SMEs, with the aim of developing tailored training modules that simulate real-world cybersecurity scenarios and strengthen practical compliance capabilities.

CYBERFORT presents a comprehensive approach designed to strengthen the cybersecurity defenses of SMEs. It offers an integrated strategy to improve SMEs' cybersecurity by implementing the CRA requirements. The project emphasizes creating and sharing tailored compliance tools, best practices, and educational resources to help SMEs tackle the challenges posed by cybersecurity threats. CYBERFORT will develop free, open-source tools to support the internal compliance process in line with the CRA. Throughout the project's implementation, workshops, hackathons, and conferences will be organized to share results and outcomes.

The Project aims to introduce innovative ideas for various energy stakeholders across Europe, particularly in Southeastern Europe. CYBERFORT will develop free, open-source tools to support the internal compliance process in line with the CRA. Throughout the project's implementation, workshops, hackathons, and conferences will be organized to share results and outcomes.

The Project's development is driven by an International Consortium that is both complementary in expertise and united in its objectives. The CYBERFORT Project funded by the European Cybersecurity Competence Centre (ECCC), under the Digital Europe Programme, started its implementation on 1<sup>st</sup> December 2024.

The Project gathers experts from Cyprus and Romania - 8 Consortium Partners Organizations. The European Consortium Partners is coordinated by I-ENERGYLINK (RO) working together with BOLTON TECHNOLOGIES (CY), CLONE SYSTEMS (CY), COLUMBIA SHIPMANAGEMENT (CY), DEALIO LIMITED (CY), ROMANIAN NATIONAL CYBERSECURITY DIRECTORATE (RO), ELIAS NEOCLEOUS (CY) and EXIMPROD ENGINEERING (RO).

