

CYBERSECURITY ACT 2

LAST UPDATE 05 | 2026

1. OVERVIEW AND SCOPE

- Official name of the initiative: **Cybersecurity Act 2 (CSA2) - Regulation EU 2019/881**
- Type: **Regulation** (a "regulation" is a binding legislative act. It must be applied in its entirety across the EU).

The Cybersecurity Act 1 (Regulation 2019/881) has as main subject matter and scope: a. ENISA (the European Union Agency for Cybersecurity); b. a framework for establishing European cybersecurity certification schemes.

The Cybersecurity Act 2 proposal has two objectives: increase cybersecurity capabilities and resilience and prevent fragmentation across the single market. It includes enhanced security on the ICT supply-chain and reinforced ENISA role.

The regulation aims to tackle: (i) the misalignment between the Union's cybersecurity policy framework and stakeholders' needs in an increasingly hostile threat landscape; (ii) the stalled implementation of the European cybersecurity certification framework (ECCF); (iii) the complexity and diversity of the cybersecurity-related policies impacting the Union's cyber posture; and (iv) increasing ICT supply chains security risks.

2. WHAT DOES IT APPLY TO?

Manufacturers and providers of ICT products, ICT services, ICT processes or managed security services, or entities the cyber posture of which is certified.

Subject to the final text, companies should consider mapping in-scope suppliers, reviewing contractual arrangements, and assessing data transfer and remote data processing practices to prepare mitigation strategies and compliance processes.

3. HOW IS THE EVENTS INDUSTRY DIRECTLY AFFECTED?

In-scope companies will need to comply with the provisions of the Regulation.

To be noted that, according to the implementation timing, some European Exhibition Centres have already been requested to comply with NIS2 directive.

Overall, companies should perform a mapping and assessment of ICT suppliers, and adopt necessary measures.

4. MAIN PROVISIONS OF THE LEGISLATION

The Regulation lays down:

- a. the mission, objectives, tasks and organisational matters relating to the European Union Agency for Cybersecurity (ENISA);
- b. a framework for establishing European cybersecurity certification (including changes to the European Cybersecurity Certification Framework);
- c. a trusted ICT supply chain framework.

5. STATE OF THE LEGISLATIVE PROCESS

Proposal. In February the proposal has entered the Parliament's preparatory phase.

7. LINKS

Communication of the European Commission: <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act>

Proposal for Regulation:

[file:///C:/Users/giulia.corino00000/Downloads/COM_2026_11_1_EN_ACT_part1_v81_gVB5aSbD9VXgCvXjk9kiarOw9Q_123727%20\(1\).pdf](file:///C:/Users/giulia.corino00000/Downloads/COM_2026_11_1_EN_ACT_part1_v81_gVB5aSbD9VXgCvXjk9kiarOw9Q_123727%20(1).pdf)