HORIZON-CL3-2026-02-CS-ECCC-02 (SecureAI)	
Program	Horizon Europe
Program de lucru	Horizon Europe Work Programme 2026-2027 – Cluster 3: Civil Security for Society
Autoritate implementare	European Commission (implementare indirectă prin ECCC)
Cod apel	HORIZON-CL3-2026-02-CS-ECCC-02
Titlu apel	Enhancing the Security, Privacy and Robustness of AI Models and Systems (SecureAI)
Domeniu / Topic	Cybersecurity – securitatea, confidențialitatea și robustețea modelelor și sistemelor de IA
Tip acțiune	Innovation Action (IA)
Tip acord de finanțare	Horizon Lump Sum MGA
Rata de finanțare	70 % (până la 100 % pentru entități non-profit)
Data deschiderii apelului	03 martie 2026
Data limită de depunere	15 septembrie 2026, ora 17:00 (ora Bruxelles-ului)
Obiectivul apelului	Consolidarea rezilienței sistemelor de inteligență artificială împotriva diferitelor tipuri de amenințări și atacuri, în conformitate cu Regulamentul IA (AI Act).
Rezultate așteptate	• Modele și sisteme de IA robuste capabile să reziste diferitelor clase de manipulare ostilă; • Mecanisme inovatoare de apărare pentru modelele și sistemele de IA împotriva noilor familii de atacuri; • Metodologii pentru detectarea și atenuarea atacurilor, cum ar fi otrăvirea datelor (data poisoning), exploatarea backdoor-urilor și clasificarea eronată; • Sisteme de IA care utilizează tehnologii de îmbunătățire a confidențialității (PET), menținând confidențialitatea datelor și conformitatea cu reglementările.
Tipuri de beneficiari	Universități, institute de cercetare, industrie, IMM-uri și alte organizații din state membre UE sau țări asociate
Structura consorțiului	Minimum 3 entități independente din 3 state membre sau asociate
Buget total al topicului	21,2 milioane EUR
Buget estimat per proiect	aprox. 4,2 milioane EUR
Număr estimat de proiecte	aprox. 5
Restricții de participare	Participare limitată la entități din state membre UE sau țări asociate. Entitățile stabilite în China nu sunt eligibile să participe la această Acțiune de Inovare.
Domeniu de aplicare detaliat	
Descriere generală	Dependența crescândă de IA în securitatea cibernetică, infrastructurile critice și procesele decizionale ridică preocupări cu privire la securitatea și robustețea sistemelor de IA. Propunerile ar trebui să abordeze:
Modele IA robuste	Explorarea tehnicilor de consolidare a modelelor împotriva perturbărilor adversariale: antrenament adversarial, optimizare robustă, mecanisme de apărare.

Detectare date compromise	Avansarea metodologiilor pentru identificarea și atenuarea seturilor de date manipulate sau otrăvite: detectarea anomaliilor, urmărirea proveniență, validare automată.
IA privată (Private AI)	Dezvoltarea de mecanisme pentru antrenarea și operarea modelelor de IA în medii care protejează confidențialitatea: învățare federată, agregare securizată, calcul pe date criptate, criptare homomorfă rezistentă la amenințări cuantice, inferență securizată în deep learning.
Evaluare și condiții	
Model depunere	Etapă unică (single-stage)
Limita de pagini	45 pagini (lump sum IA)
Criterii de evaluare	Propunerile vor fi evaluate pe baza a trei criterii: Excelență, Impact și Calitatea și eficiența implementării. Fiecare criteriu se notează cu un punctaj de la 1 la 5. Pragul minim per criteriu este 3, iar pragul minim cumulat al celor trei criterii este 10. Pentru Acțiunile de Inovare, criteriul Impact beneficiază de o pondere de 1,5 în stabilirea clasamentului.
Observație securitate	Unele activități pot implica informații clasificate sau rezultate sensibile (EUCI/SEN).
Context	
Program	Horizon Europe – principalul program de finanțare al UE pentru cercetare și inovare 2021-2027 (95,5 miliarde EUR). Clusterul 3, Destinația „Securitate cibernetică sporită”.
Implementare	ECCC implementează acțiunile gestionate indirect, conform Regulamentului (UE) 2021/887.
Linkuri utile	
Funding & Tenders Portal	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2026-02-cs-eccc-02
Programme Guide	https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/programme-guide_horizon_en.pdf
General Annexes 2026-2027	https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2026-2027/wp-15-general-annexes_horizon-2026-2027_en.pdf