Verbesserung der Sicherheit, Privatsphäre und Robustheit von KI-Modellen und -Systemen

HORIZON-CL3-2026-02-CS-ECCC-02: Enhancing the Security, Privacy and Robustness of AI Models and Systems (SecureAI)

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1

Für dieses Topic aus **Horizont Europa 2026** beträgt das Fördervolumen insgesamt **21,2 Mio. €**.
Die vorgesehene Projektgröße liegt bei 3 – 4 Mio. €.

2

Art der Maßnahme: Innovation Actions
Förderquote: 100 % (gemeinnützig), 70 % (gewinnorientiert)
Ausschreibungsstart: 03. März 2026
Einreichungsfrist: 15. September 2026
Teilnahmeberechtigt:
Rechtsträger mit Sitz in EU-Mitgliedstaaten oder assoziierten Ländern, die nicht direkt oder indirekt von Drittländern oder deren Einrichtungen kontrolliert werden.

Erwartete Ergebnisse
Gefördert werden robuste KI-Modelle, die Angriffen wie Datenvergiftung, Backdoors oder Fehlklassifikationen standhalten. Zudem sollen neue Abwehrmechanismen und Methoden zur Angriffserkennung entwickelt werden. Ein Schwerpunkt liegt auf datenschutzwahrenden Technologien, die vertrauenswürdige Anwendungen in sensiblen Bereichen wie Verwaltung und Unternehmen ermöglichen.

Umfang
Im Fokus steht die Resilienz von KI-Systemen gegen Manipulationen von Eingaben und Trainingsdaten. Erwartet werden Verfahren zur Echtzeit-Erkennung von Anomalien, zur Abwehr adversarieller Angriffe und zur Absicherung verteilter Lernverfahren. Ergänzend sollen „Private AI“-Ansätze gefördert werden, bei denen Daten und Berechnungen in geschützten Umgebungen bleiben – unterstützt durch Technologien wie föderiertes Lernen, sichere Aggregation oder Verschlüsselung.

NKCS
NATIONALES KOORDINIERUNGSZENTRUM FÜR CYBERSICHERHEIT **DEUTSCHLAND**

Sie haben Fragen? Nehmen Sie Kontakt mit uns auf:
www.nkcs.bund.de/de/kontakt