HINWEIS: Frei übersetzt aus dem Englischen. Wir empfehlen als Referenz bei der Bewerbung den englischen Text zu nutzen.

Originaltext auf Englisch finden Sie in folgendem Dokument:

“Horizon Europe Work Programme 2025: Civil Security for Society“
14. Mai 2025 herausgegeben vom ECCC / EU-Kommission

https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-3-civil-security-society_en?prefLang=de

Förderbereich: Increased Cybersecurity

Förderthema: HORIZON-CL3-2025-02-ECCC-03: Privacy Enhancing Technologies

Seiten: 99-101

Deutsche Übersetzung des Förderthemas durch das NKCS/ NCC-DE als unterstützendes Informationsangebot erstellt:

HORIZON-CL3-2025-03-ECCC-01: Technologien zur Verbesserung der Privatsphäre

Erwartete Auswirkungen

Vom ECCC eingeleitete Aktion zur Aufnahme der im Abschnitt "Ziel - Erhöhte Cybersicherheit" dieses Teils des Arbeitsprogramms dargelegten Formulierung "erwartete Auswirkungen".

Erwartete Ergebnisse

Es wird erwartet, dass die Ergebnisse der Projekte zu einigen oder allen der folgenden Ergebnisse beitragen:

- Entwicklung robuster, skalierbarer und zuverlässiger Technologien zur Wahrung des Datenschutzes in föderierten und sicheren Systemen zur gemeinsamen Nutzung von Daten sowie bei der Verarbeitung persönlicher und industrieller Daten, die in reale Systeme integriert sind.

- Entwicklung von Ansätzen zur Wahrung der Privatsphäre bei Lösungen für die gemeinsame Nutzung von Daten, einschließlich der gemeinsamen Nutzung von Informationen über Cyber-Bedrohungen unter Wahrung der Privatsphäre, und bei kollaborativen Berechnungen mit sensiblen Daten.

- Integration von Privacy-by-Design in den Kern von Software- und Protokollentwicklungsprozessen. Dabei ist darauf zu achten, dass kryptographische Bausteine und Implementierungen von datenschutzfreundlichen digitalen Signaturen und

Benutzerauthentifizierungssystemen kryptoagil und modular sind, um den Übergang zu post-quantum kryptographischen Algorithmen zu erleichtern.

- Entwicklung von Technologien zur Verbesserung des Datenschutzes für die Benutzer von eingeschränkten Geräten

- Beitrag zur Förderung von GDPR-konformen europäischen Datenräumen für digitale Dienste und Forschung, z.B. für Gesundheitsdaten, in Übereinstimmung mit den DATA Topics von Horizon Europe Cluster 4.

- Entwicklung von Technologien und Lösungen zur Verbesserung des Datenschutzes, die den Bedürfnissen von Bürgern und Unternehmen, einschließlich kleiner und mittlerer Unternehmen (KMU), entsprechen.

- Entwicklung von Blockchain-basierten und dezentralen Technologien zur Verbesserung der Privatsphäre, um die Vertraulichkeit und Integrität von Daten sowie die Authentizität von Transaktionen und digitalen Vermögenswerten zu wahren. Eine mögliche Kombination von Blockchain mit anderen Technologien, wie z.B. föderiertes Lernen, muss die Sicherheit und den Datenschutz der über solche Netzwerke ausgetauschten Daten gewährleisten und gleichzeitig sicherstellen, dass die angeschlossenen Geräte vertrauenswürdig sind.

- Untersuchung der Benutzerfreundlichkeit und der Benutzererfahrung von Technologien zur Verbesserung der Privatsphäre und Erkundung von Möglichkeiten zur Entwicklung von Systemen, die sowohl sicher als auch benutzerfreundlich sind.

Umfang

Der Schutz der persönlichen Daten von Einzelpersonen und die Gewährleistung der Privatsphäre bei gleichzeitiger Ermöglichung der Datenverarbeitung und -analyse ist für unsere Gesellschaft von grundlegender Bedeutung. Techniken zur Wahrung der Privatsphäre ermöglichen es, die Menge der gesammelten und verarbeiteten persönlichen Daten zu minimieren und diese Daten durch fortschrittliche kryptografische Methoden zu schützen. So werden beispielsweise Methoden des maschinellen Lernens eingesetzt, um medizinische und verhaltensbezogene Daten zu analysieren, um Ursachen und Erkenntnisse über Cyberangriffe oder Bedrohungen zu gewinnen. Ein erheblicher Teil dieser Daten besteht jedoch aus persönlichen Informationen (z. B. sensible Gesundheitsdaten), was Bedenken hinsichtlich möglicher Verstöße oder Missbrauchs aufkommen lässt und somit die Privatsphäre des Einzelnen, das gesellschaftliche Wohlergehen und die wirtschaftliche Stabilität gefährdet.

Darüber hinaus sind die Herausforderungen im Zusammenhang mit der Nutzung von nicht-personenbezogenen/industriellen Datenbeständen, die die vollständige Verwirklichung der datengesteuerten Wirtschaft behindern könnten, ebenfalls Gegenstand der Arbeit, die unter diesem Thema vorgeschlagen werden kann. Lösungen, die Sicherheit gegen Quanten-Angreifer bieten, sind ebenfalls erwünscht.

Technologien zur Verbesserung des Schutzes der Privatsphäre (Privacy Enhancing Technologies, PETs) wie kryptografische anonyme Berechtigungsnachweise, differentieller Datenschutz, sichere Mehrparteienberechnungen, homomorphe Verschlüsselung, fortgeschrittene digitale Signaturen wie Ringsignaturen, blinde Signaturen und attributbasierte Berechtigungsnachweise sind vielversprechend, um diese Herausforderungen zu mildern, doch ihre praktische Anwendung erfordert weitere Verfeinerung und strenge Tests. Konsortien sind aufgefordert, Lösungen

vorzuschlagen, die die Nutzbarkeit und Wirksamkeit verschiedener Technologien zum Schutz der Privatsphäre in einer realistischen Umgebung verbessern können, und ihre Integration in gemeinsame europäische Datenräume zu untersuchen. Angesichts der Fortschritte der Quantentechnologien ist die Einbeziehung flexibler, modularer Systeme zur Unterstützung des Übergangs zu Post-Quantum-PETs sowie die Entwicklung, Verbesserung und Sicherheitsanalyse von quantenresistenten PETs zu begrüßen.

Die Vorschläge sollten sich auch darauf konzentrieren, die Nutzbarkeit, Skalierbarkeit und Zuverlässigkeit von sicheren und Technologien zum Schutz der Privatsphäre innerhalb von Lieferketten zu verbessern und sich dabei nahtlos in bestehende Infrastrukturen und herkömmliche Sicherheitsprotokolle zu integrieren. Sie sollten auch der Vielfalt an Datentypen und -modellen in verschiedenen Organisationen Rechnung tragen und in authentischen Datenumgebungen validiert und getestet werden. Die Einhaltung von Datenvorschriften, insbesondere der GDPR, ist von größter Bedeutung.

Konsortien sollten versuchen, interdisziplinäres Fachwissen und Ressourcen von Interessenvertretern der Industrie, Dienstleistern und Endnutzern miteinander zu verbinden. Die Einbindung von KMUs wird ebenso gefördert wie die Einbeziehung juristischer Fachkräfte, um die Einhaltung von Vorschriften, einschließlich der Datenschutzgrundverordnung, sicherzustellen. Darüber hinaus wird die proaktive Identifizierung und Bewertung potenzieller regulatorischer Hürden und Beschränkungen für die entwickelten Technologien/Lösungen nachdrücklich empfohlen.

Art der Maßnahme	Research and Innovation Actions
Vorläufiges Budget	*11 Mio. EUR*
Vorläufiges Budget pro Projekt	*3-4 Mio. EUR*
Ausschreibungsstart	12.06.2025
Implementierung	ECCC
Zuwendungsberechtigt	Rechtsträger mit Sitz in EU-Mitgliedstaaten und assoziierten Länder, die nicht direkt oder indirekt von Drittländern kontrolliert werden
Technologiereifegrad	Projektstart mindestens TRL 4, Projektende mindestens TRL 7
Abrechnung	Förderfähige Kosten werden als Lump Sums (Pauschalbeträge) gewährt
Sicherheit	Einige Aktivitäten, die sich aus diesem Thema ergeben, können die Verwendung von als Verschlusssache eingestuften Hintergrundinformationen und/oder die Erstellung von sicherheitsempfindlichen Ergebnissen (EU-Verschlusssachen und SEN) beinhalten. Bitte beachten Sie die entsprechenden Bestimmungen in Abschnitt B Sicherheit - EU-Verschlusssachen und sensible Informationen der Allgemeinen Anhänge.

HINWEIS: Frei übersetzt aus dem Englischen. Wir empfehlen als Referenz bei der Bewerbung den englischen Text zu nutzen.

Das **Nationale Koordinierungszentrum für Cybersicherheit (NKCS/ NCC-DE)**

berät zu **EU-Fördermöglichkeiten in der Cybersicherheit**

und hilft bei der **Vernetzung mit EU-Partnern**.

Sie erreichen uns unter **nkcs@bsi.bund.de**