Tecnologie per la conservazione della privacy e la gestione dell'identità
Privacy-preserving and identity management technologies

TOPIC ID:
HORIZON-CL3-2023-CS-01-02

Ente finanziatore:
Commissione europea
Programma
Programma quadro Horizon Europe (HORIZON)

Obiettivi ed impatto attesi:
I risultati dei progetti dovrebbero contribuire ad alcuni o a tutti i seguenti risultati:

- Migliori tecnologie scalabili e affidabili per la conservazione della privacy e la gestione delle identità per la condivisione federata e sicura e per l'elaborazione di dati personali e industriali e la loro integrazione in sistemi reali;
- Migliorare le tecnologie che preservano la privacy per le soluzioni di intelligence e condivisione dei dati sulle minacce informatiche;
- Privacy by design;
- Contributo alla promozione di spazi dati europei conformi al GDPR per i servizi digitali e la ricerca (in sinergia con i DATA Topics del Cluster 4 di Horizon Europe). Inoltre, contributo alla promozione di soluzioni europee conformi al regolamento eID;
- Ricerca e sviluppo di tecnologie e soluzioni per la gestione dell'identità auto-sovrana;
- Fornire soluzioni di identità digitale sicure ed efficienti dal punto di vista delle risorse alle piccole e medie imprese (PMI);
- Rafforzamento dell'ecosistema europeo di sviluppatori e ricercatori open-source di soluzioni per la tutela della privacy;
- Usabilità delle tecnologie per la tutela della privacy e la gestione dell'identità.

Ambito di applicazione:
L'utilizzo dei big data per i servizi digitali e la ricerca scientifica comporta nuove opportunità e sfide. Ad esempio, i metodi di apprendimento automatico elaborano dati medici e comportamentali per trovare cause e spiegazioni di malattie o rischi per la salute. Tuttavia, una grande quantità di questi dati è costituita da dati personali. La perdita o l'abuso di questo tipo di dati, i potenziali rischi per la privacy (ad esempio, la divulgazione di attributi o l'inferenza di appartenenza) e la compromissione dell'identità rappresentano minacce per gli individui, la società e l'economia, che ostacolano l'ulteriore sviluppo di spazi di dati che coinvolgono dati personali. Allo stesso modo, esistono sfide simili per lo sfruttamento di asset di dati non personali/industriali che possono compromettere le opportunità offerte dall'economia dei dati. Le tecnologie avanzate per la tutela della privacy, come ad esempio le credenziali anonime crittografiche, la crittografia omomorfa, il calcolo multipartitico sicuro e la privacy differenziale, hanno il potenziale per affrontare queste sfide. Tuttavia, sono necessari ulteriori lavori per garantire e testare la loro applicabilità

in scenari d'uso reali.
La sicurezza di qualsiasi servizio digitale o accesso ai dati si basa su identità digitali sicure. Il Regolamento eID fornisce il quadro giuridico su cui costruire soluzioni tecnologiche che rispondano alle esigenze degli utenti in materia di identità digitale. Per quanto riguarda i dati personali, è anche importante sviluppare soluzioni di identità auto-sovrana che diano agli utenti il controllo completo sui loro dati personali e sul loro utilizzo.
Le proposte devono riguardare l'usabilità, la scalabilità e l'affidabilità delle tecnologie sicure e rispettose della privacy nella catena di approvvigionamento e tenere conto dell'integrazione con le infrastrutture esistenti e le misure di sicurezza tradizionali. Dovrebbero inoltre tenere conto, se necessario, della variazione dei tipi e dei modelli di dati tra le diverse organizzazioni. Le soluzioni proposte devono essere convalidate e sperimentate in infrastrutture di dati realistiche e federate come, ad esempio, gli spazi di dati europei. Dovrebbero garantire la conformità alle normative sui dati ed essere conformi al GDPR per progettazione. Sono incoraggiate le soluzioni open-source.
I consorzi dovrebbero riunire competenze e capacità interdisciplinari che coprano il lato della domanda e dell'offerta, ossia l'industria, i fornitori di servizi e, se del caso, gli utenti finali. Si potrebbe prendere in considerazione l'uso di strumenti quadro per l'infrastruttura di autenticazione e autorizzazione sviluppati per gli spazi dati, in particolare con l'European Open Science Cloud. La partecipazione delle PMI è fortemente incoraggiata. Dovrebbero essere aggiunte anche competenze legali per garantire la conformità dei risultati del progetto alle normative sui dati e al GDPR.
Si incoraggia l'identificazione e l'analisi dei potenziali aspetti normativi e delle barriere per le tecnologie/soluzioni sviluppate, se pertinenti.

Criteri di eleggibilità:
Le condizioni sono descritte nell'Allegato generale B.

Per essere ammissibili, i richiedenti (beneficiari ed enti affiliati) devono:

-essere soggetti giuridici (enti pubblici o privati) avere sede in uno dei Paesi ammissibili, ovvero Stati membri dell'UE (compresi i Paesi e territori d'oltremare (PTOM)) Paesi non UE:

– Paesi SEE elencati e Paesi associati o Paesi che hanno in corso negoziati per un accordo di associazione e in cui l'accordo entra in vigore prima della firma della sovvenzione (elenco dei Paesi partecipanti)

– Paesi in via di adesione,

I beneficiari e gli enti affiliati devono iscriversi al Registro dei partecipanti – prima di presentare la proposta – e dovranno essere convalidati dal Servizio centrale di convalida (REA Validation). Per la convalida, sarà loro richiesto di caricare documenti che dimostrino lo status giuridico e l'origine.

Contributo finanziario:
Le condizioni sono descritte nell'Allegato generale B.

Per essere ammissibili, i richiedenti (beneficiari ed enti affiliati) devono:

-essere soggetti giuridici (enti pubblici o privati) avere sede in uno dei Paesi ammissibili, ovvero Stati membri dell'UE (compresi i Paesi e territori d'oltremare (PTOM)) Paesi non UE:

– Paesi SEE elencati e Paesi associati o Paesi che hanno in corso negoziati per un accordo di associazione e in cui l'accordo entra in vigore prima della firma della sovvenzione (elenco dei Paesi partecipanti)

– Paesi in via di adesione,

I beneficiari e gli enti affiliati devono iscriversi al Registro dei partecipanti – prima di presentare la proposta – e dovranno essere convalidati dal Servizio centrale di convalida (REA Validation). Per la convalida, sarà loro richiesto di caricare documenti che dimostrino lo status giuridico e l'origine.

Scadenza:
23 novembre 2023 17:00:00 ora di Bruxelles

Ulteriori informazioni:
wp-6-civil-security-for-society_horizon-2023-2024_en.pdf (europa.eu)