Disclaimer: This content is an extract from a draft version of the Horizon Europe Security Cluster work programme

CS5.1.2021 (RIA) – Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data

Expected Outcomes: *Projects' results are expected to contribute to one or more the following outcomes:*

- Improved scalable and reliable privacy-preserving technologies for federated processing of personal data and their integration in real-world systems
- More user-friendly solutions for privacy-preserving processing of federated personal data registries by researchers
- Improving privacy-preserving technologies for cyber threat intelligence and data sharing solution
- Contribution to promotion of GDPR compliant European data spaces for digital services and research (in synergy with topic DATA-01-2021 of Horizon Europe Cluster 4)
- Strengthened European ecosystem of open source developers and researchers of privacy-preserving solutions

Scope: Using big data for digital services and scientific research brings about new opportunities and challenges. For example, machine learning methods process medical and behavioural data for finding causes and explanations for diseases or health risks. However, a large amount of this data is personal data. Leakage or abuse of this kind of data and potential privacy infringement (e.g. attribute disclosure or membership inference) risks are a cybersecurity threat to individuals, society and economy and an impediment for further developing data spaces involving personal data. Vice versa, adequate protection of this data according to the GDPR can also prevent its full utilization for society. Advanced privacy-preserving computation techniques such as homomorphic encryption, secure multiparty computation, and differential privacy are being researched and have proven promising to address these challenges. However, further research is required to ensure their applicability in real-world use case scenarios. For example, fully homomorphic encryption is not practically applicable in many cases and secure multi-party computation often imposes special infrastructural requirements.

Building on research and innovation in the area of privacy-preserving computation, proposals should address scalability and reliability of privacy-preserving technologies in realistic problem areas and take integration with existing infrastructures and traditional security measures (e.g. access control) into account. They should respond to users' needs, e.g. for research and digital services in access and data management for citizens geared towards their own profiles (incl. dynamic personalised recommendations for improved cybersecurity)

or in personalised medicine. They should further address the legacy variation in personal data types and data models across different organisations in the same business sector and/or across different potential application sectors. A proposed solution should include validation or piloting of privacy-preserving computation in realistic federated data infrastructures and more specifically European data spaces involving personal data (e.g. the EU heath data space). It should be guided by the EU's high standards concerning the right to privacy, protection of personal data, and the protection of fundamental rights in the digital age. It should ensure, by-design, compliance with data regulations and specifically the GDPR.

Consortia should bring together interdisciplinary expertise and capacity covering the supply and the demand side, i.e. industry, service providers and end-users. Participation of SMEs is strongly encouraged. . Legal expertise should also be incorporated to assess and ensure compliance of the technical project results with data regulations and the GDPR.

The proposal should provide appropriate indicators to measure its progress and specific impact.