Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises

Proposals are invited against one of the following sub-topics:

(a): Protecting citizens' security, privacy and personal data

Proposals should bring innovative solutions to personal data protection, develop new applications and technologies in order to help citizens to better monitor and audit their security, privacy and personal data protection, enabling them to become more engaged and active in the fight against cyber, privacy and personal data protection risks.

These solutions should include innovative approaches, techniques and user-friendly tools for: (1) improving resilience against privacy and personal data protection risks (e.g. personal data breaches[[Notification of a personal data breach to the supervisory authority and communication of a personal data breach to the data subject are regulated respectively under articles 33 and 34 of the GDPR.]] and cyber threats (e.g. profiling, eavesdropping, data misuse); (2) identifying, removing and reporting potential harmful content (e.g. apology of criminal acts, unhealthy or self-harming habits) and abusive interactions (e.g. harassment, unsolicited communications); (3) exercising citizens' right to erasure ("right-to-be-forgotten") [[See article 17 of the GDPR.]] and data portability[[See article 20 of the GDPR.]]; (4) providing citizens with transparent information about their privacy and personal data protection[[See article 12 of the GDPR.]] level and empowering them to modulate it at any moment of their digital activities (e.g. by activating encryption); (5) protecting or
providing rights for any access/audit/interference with citizens’ "smart terminals" or their Internet-based communications in a data protection compliant way; (6) developing on-line help-desks services or "one-stop-shop" informing, helping citizens in dealing with any security and/or privacy incident and data (including personal data) protection breach, and enabling them in reporting any cyber or privacy related incident and data (including personal data) protection breach. Such approaches need to build bridges/synergies with data protection authorities and CERTs/CSIRTs. To better respond to the needs and expectations of the end-users, proposals should engage the end-users by involving them in the design and implementation, in order to ensure the usability and acceptability of the proposed solutions. In addition, assurance and transparency about the digital security, privacy and personal data protection levels embedded in products and services should be easily accessed, identified and monitored by all citizens, independently of their physical condition or ICT skills, by developing appropriate innovative solutions.

The outcome of the proposal is expected to lead to development up to Technology Readiness level (TRL) 7; please see Annex G of the General Annexes.

The Commission considers that proposals requesting a contribution from the EU of between EUR 4 and 5 million would allow this specific challenge under sub-topic (a) to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

(b): Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs): defenders of security, privacy and personal data protection

Proposals should deliver innovative solutions to increase the knowledge sharing in digital security across SMEs&MEs and between SMEs&MEs and larger providers. The user SMEs&MEs should be supported by democratizing access to tools and solutions of varied sophistication level, to allow SMEs&MEs benefitting from innovative targeted solutions addressing their specific needs and available resources (currently reserved to larger organisations, due to their cost and availability of internal expertise).

The proposals should develop targeted, user-friendly and cost-effective solutions enabling SMEs&MEs to: (1) dynamically monitor, forecast and assess their security, privacy and personal data protection risks[[Data protection impact assessments are required in situation enumerated in article 35 of the GDPR.]]; (2) become more aware of vulnerabilities, attacks and risks that influence their business; (3) manage and forecast their security, privacy and personal data protection risks in an easy and affordable way; (4) build on-line collaboration between SMEs&MEs associations and with CERTs/CSIRTs, enabling thus individual SMEs&MEs to report any incident.
Citizens and SMEs&MEs are better protected and become active players in the Digital Single Market, including implementation of the NIS directive and the application of the General Data Protection Regulation.

In addition, tools and processes should be proposed to facilitate the participation of user SMEs&MEs in cyber ranges for cybersecurity.

The outcome of the proposal is expected to lead to development up to Technology Readiness level (TRL) 7; please see Annex G of the General Annexes.

The Commission considers that proposals requesting a contribution from the EU of between EUR 3 and 4 million would allow this specific challenge under sub-topic (b) to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Projects should also foresee activities and envisage resources for clustering with other projects funded under this topic and with other relevant projects in the field funded by H2020.

Some members of the digital society in the EU are more vulnerable as they are less prepared to confront with cyber-attacks. The scale, value and sensitivity of personal data in the cyberspace are significantly increasing and citizens are typically uncertain about who monitors, accesses and modifies their personal data. Personal data breach may facilitate abuse by third parties, including cyber-thrreats such as coercion, extortion and corruption.

In order to protect the freedom, security and privacy, and ensure personal data protection of the citizens in Europe, citizens should be enabled to assess the risk involved in their digital activities and configure their own security, privacy and personal data protection settings and controls across these services. Citizens need to be fully aware that their informed consent is necessary in many situations and become capable in providing their permission/consent for allowing accessing their personal data/devices/terminals with an increased level of granularity. Additionally there is a need for increased citizens’ capacity to modulate the level and accuracy of the monitoring tools used by services (e.g. via cookies, positioning, tokens).

Most Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs) lack sufficient awareness and can only allocate limited resources - both technical and human - to counter cyber risks, hence they are an easier target (e.g. of ransomware attacks) compared to large organizations. Security professionals and experts working for SMEs&MEs need to be in a constant learning process since cybersecurity is a significantly complex and fast-evolving field. Taking into account the significant economic role of SMEs&MEs in the EU, tailored research to innovation should support cybersecurity for SMEs&MEs.

- Citizens and SMEs&MEs are better protected and become active players in the Digital Single Market, including implementation of the NIS directive and the application of the General Data Protection Regulation.
Regulation.

- Security, privacy and personal data protection are strengthened as shared responsibility along all layers in the digital economy, including citizens and SMEs&MEs.
- Reduced economic damage caused by harmful cyber-attacks and privacy incidents and data (including personal data) protection breaches.
- Pave the way for a trustworthy EU digital environment benefitting all economic and social actors.

Last update: 16 April 2019


European Union, 2024