

EIT Digital Action Line for Privacy, Security & Trust

Action Line Leader: Jovan Golic

Privacy, Security & Trust action line is about putting into practice innovative privacy-preserving and secure information technologies to protect sensitive data and the privacy of individuals in the Information Age.

EIT Digital is addressing this area in the full Innovation & Entrepreneurship and Entrepreneurial Education framework, through innovation projects-activities, Master and Summer Schools and through Business Development Accelerator and Business Community.



This action line is transversal to other action lines of EIT Digital.

<https://www.eitdigital.eu/innovation-entrepreneurship/privacy-security-trust/>

Privacy

Information technologies have invaded many aspects of people's daily lives, creating new exciting possibilities, but also raising concerns in terms of privacy and trust. Protecting the privacy of individuals in the Information Age is very challenging as they constantly leave digital traces of their lives and habits, often without even being aware of that. Such digital traces, including various identifiers and secrets as well as application data resulting from online services in cyberspace, may be exposed and used for malicious purposes, e.g., fraud, identity theft, defamation, targeted spam as well as illegitimate profiling and espionage. As a response, the European Commission has been putting forward the privacy-by-design principle, which integrates the privacy issues in the design phase of a system or application. However, many existing applicable privacy-preserving or privacy-enhancing technologies are not widely known, accepted and used and are sometimes seen as business obstacles rather than opportunities.

Security and Trust

Data security is about data confidentiality, integrity and availability as well as entity identification. Since data privacy is about the security and users' control of sensitive data, it follows that without data privacy sensitive data would be exposed to cyber attacks and abuses and, hence, one cannot achieve cyber security. On the other hand, authorized exceptional access to sensitive data can help cyber investigation to provide more effective protection against crimes in cyberspace and the physical world. Large scale adoption of digital devices and services, like in e-health and smart cities, requires users' trust both in the technology and the entities involved in the process. This trust and privacy are seriously threatened by growing cyber attacks, which need to be addressed both reactively and proactively. The action line promotes business opportunities in this area by fostering a proactive approach deploying trustworthy and transparent innovative technologies bridging the gaps between available techniques and practice, encouraging the security-by-design and privacy-by-design paradigms and leveraging the recognized expertise and creativity of European players.