pharaon posts

> *«Appropriate cybersecurity mechanisms and procedures have no alternative when delivering solutions for ICT-enabled independence and improved quality of life.»*

Andrej Grgurić, Ericsson Nikola Tesla d.d.

Importance of cybersecurity and privacy for Pharaon

The goal of the Pharaon project is to realize smart and active living for Europe's ageing population by integrating different digital services, platforms, and devices to deliver personalised and user-friendly fit-for-purpose solutions. On this path, appropriate cybersecurity and privacy mechanisms are of pivotal importance. Pharaon services will mostly be delivered from the Cloud, which offers some benefits but also introduces challenges when ensuring confidentiality, integrity and availability.

Cybersecurity threats are growing in frequency and severity

As cybersecurity threats are growing both in frequency and severity, cybersecurity aspects become one of the most critical points to address before delivering solutions to end-users. Any violations in terms of data security can compromise the entire system and thus ultimately erode the fragile trust of the users. For this reason, clear identification and prioritisation of cybersecurity threats and vulnerabilities is the first step towards establishing effective countermeasures and ensuring the highest cybersecurity standards are met.

Adoption of cybersecurity standards is a must

Six pilot sites in five countries are to deliver different services, so providers of technologies and services must comply with the EU and national regulations that concern privacy, such as the General Data Protection Regulation (GDPR) and other national laws. In this respect, standards such as the ISO/IEC 27000 series on information security and standards on health informatics security are being consulted alongside recommendations from leading cybersecurity organizations such as NIST (U.S. National Institute of Standards and Technology) and ENISA (European Union Agency for Cybersecurity).

Cybersecurity and privacy concerns addressed end-to-end

Cybersecurity concerns (such as malicious attacks detection and prevention, quick recovery from failure, fine-grained access control, insider attack detection, device heterogeneity) and privacy concerns (such as profiling and tracking, localization, secure data transmission) have to be addressed on different levels. In order to provide end-to-end cybersecurity, the cybersecurity dimensions (such as access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability) have to be applied to all infrastructure, service and application layers.

Pharaon cybersecurity governance

Pharaon cybersecurity governance aims towards ensuring cybersecurity strategies are aligned with the Pharaon objectives and regulations. This type of oversight makes sure the right things are done, that resources are properly allocated, and that policies are correctly implemented. Strategic planning, organisational setups (including project-wide and pilot-specific cybersecurity measures overseen by local managers), regulation and law conformance, and continuous monitoring are in place to ensure adoption of identified cybersecurity requirements throughout the project and after.

www.pharaon.eu contact@pharaon.eu @PharaonProject fb.me/pharaon.project Pharaon Project Pharaon - Pilots for Healthy and Active Ageing