Human Centric Approach in IoT

ETSI STF 547

Presented by: **Olajumoke Ogunbekun**
STF 547 Member

For: **IoT Week Aarhus**

20.06.2019

ETSI STF 547 Technical Reports Regarding Privacy

ETSI TR 103 591 V0.0.6(2018-09)

**SmartM2M;
Privacy study report;
Standards Landscape
and best practices**

ETSI TR 103 534-2 V0.6.4 (2018-09)

**SmartM2M;
Teaching material;
Part 2: IoT Privacy**

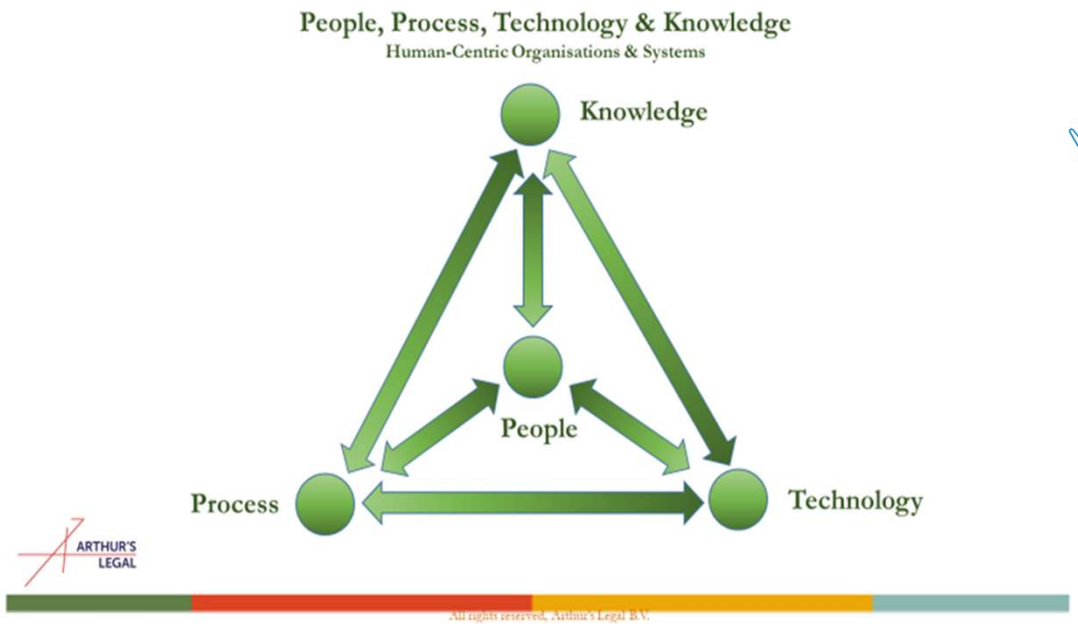
Privacy

- The concept of privacy overlaps, but does not coincide, with the concept of data protection. The right to privacy is enshrined in the Universal Declaration of Human Rights (Article 12) as well as in the European Convention of Human Rights (Article 8).
- Personal Data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
- Privacy and security are separate concepts in the sense, for example, that privacy can be perceived independently of security. But they are complementary, given that in reality security is an enabler of privacy. It can be stressed that security is a basic requirement for the effective protection of privacy.

Privacy by Design - Principles

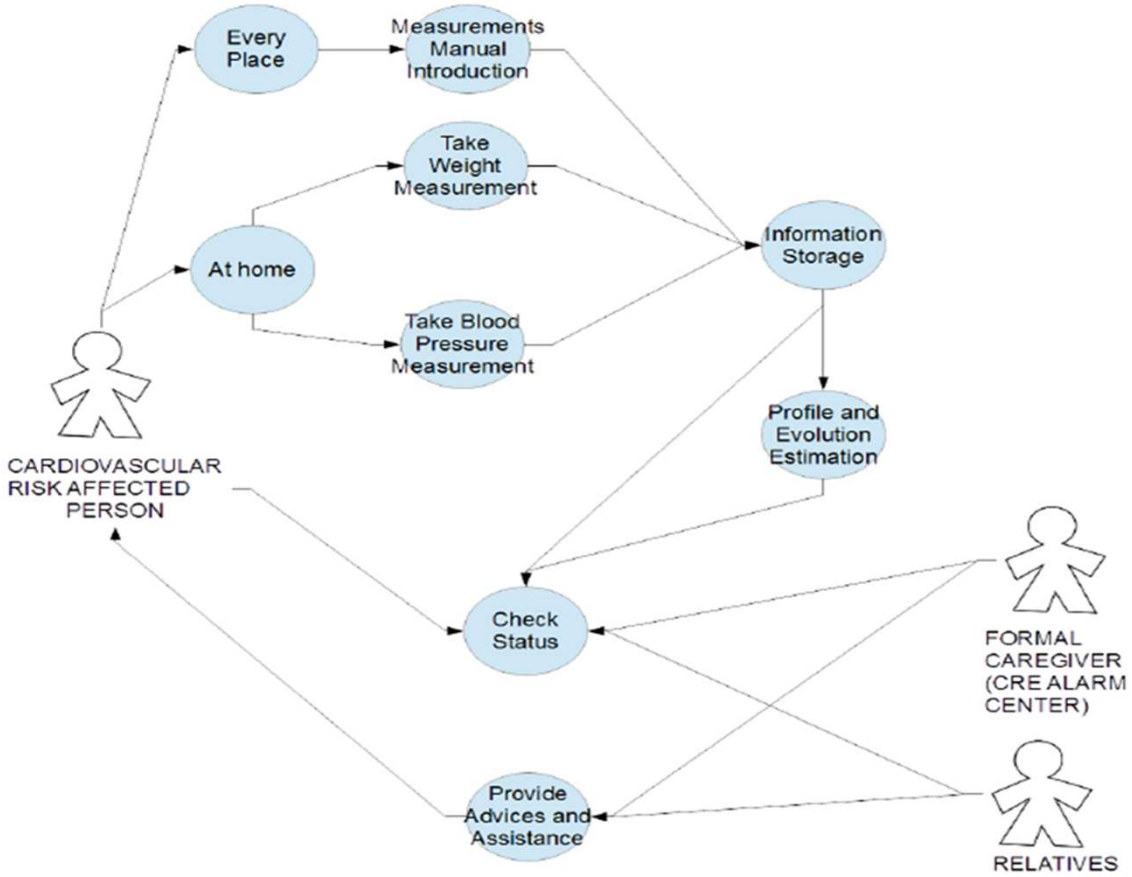
- Privacy by design, established under Article 25 of the GDPR, could be broken down into the following set of principles:
  - No personal data by default principle: avoid personal data collection or creation by default, except where, when and to the extent required.
  - 'As-If' principle: design and engineer IoT ecosystems as-if these will process personal data, now or in a later phase.
  - De-Identification by default principle: de-identify, sanitise or delete personal data as soon as there is valid legal basis anymore.
  - Data minimization by default: only process data where, when and to the extent required, and delete or de-identity other data.
  - Encryption by default principle: encrypt personal data by default and include digital rights and digital rights management thereto.

Privacy in the context of IoT – How it affects you



- Suggest reinforcing the role of human users
- Putting privacy concerns at the heart of IoT and as the users and beneficiaries of IoT.

Use case examples
Ambient assisted living in smart homes, older people - illustration



Use case examples
Ambient assisted living in smart homes, older people - stakeholders

- Main actors
  - Beneficiary: elderly person (Angela, 84 years-old) with raised cardiovascular risk
  - Family caregiver: the relatives (Alba) or family caregiver with interest and with permission to check the status of the beneficiary
  - Formal caregiver: in this case, the Spanish Red Cross that provides the 24/7 telecare and assistance service
- Data Subject: Angela
- Data Controller: CCTV camera manufacturer; Blood pressure device manufacturer
- Data Processor
  - Location service provider (provides Angela's location service to Alba)
  - Caregiver -Spanish Red cross company (provides staff that reviews Angela medical record)
  - Relative; Blood Pressure device manufacturer

Challenge of Privacy in IoT

- IoT forms a clear example of hyper connectivity and distributed control
- Appropriate safeguards are needed to ensure that individuals' right to privacy is effectively protected
- The following are some of the challenges in identifying:
  - the stakeholders that are impacted by Privacy
  - the personal data and who is responsible for the data
  - privacy in various domains in IoT
  - how stakeholders need to think of Privacy as part of design not an afterthought
  - the implication of non-compliance with Regulation not just standards.

Addressing Privacy Gaps

- The STF547 work showed that there does not appear to be any new standards or regulations needed with respect to privacy.
- The effective use of existing standards and regulation in a circular manner would seem to be sufficient to maximize the possible resulting benefits.
- What is suggested by this report is the need for new codes of conduct and certification, as they are clearly embraced as accountability tools under the GDPR and they are, of course, highly relevant, also, for the IoT environment.

Key Takeaways (1/2)

- The requirements set under the GDPR are mandatory.
- The effective protection of privacy and (personal) data protection, within the IoT environment requires appropriate technical and organizational measures.
- The implementation, monitoring and optimisation of measures are to be planned and taken in advance during related data collecting, data processing and data management pertaining to the life cycle of the respective IoT ecosystem.
- The GDPR further requires organizations not only to be able to ensure, but also to deliver documented and continuous proof of appropriate levels of compliance – defined in the GDPR as: accountability on a continuous basis.
- A holistic approach of IoT would presume the engagement of all IoT stakeholders and would, therefore, possibly, increase the likelihood of their wide adoption and actual implementation.

Key Takeaways (2/2)

- GDPR strengthens the role of standards without necessarily dictating the creation of new standards.
- If at all new standards arise in relation to the GDPR, they should take into account how they will interoperate with other legislative instruments.
- Compliance with GDPR should not be a mere a ''box-ticking exercise'' but should aim at the effective protection of personal information in reality.
- According to EDPS Opinion, technology organisation should not only bear in mind progress of technology and its endless capabilities but also the fundamental rights at stake, among which there are privacy and the protection of personal data.

Thank you for your attention!

Contact Details: Olajumoke Ogunbekun
EX2 Management Consulting Ltd.
jogunbekun@yahoo.com

STF547 Homepage:

https://portal.etsi.org/STF/STFs/STFHomePages/STF547