GDPR and the relation to IoT – How assessment of ‘technical measures’ required by the GDPR reduces financial risks by applying to Article 25 & 32

IoT Week 2022 – ‘Privacy by Design’
Jacques Kruse Brandao, Global Head of Advocacy, SGS

INFOCLASS: UNCLASSIFIED
TLP: WHITE
PII IS NEARLY EVERYWHERE

Segments:
- Smart Home
- Smart Health
- Industrie 4.0
- Smart City
- Smart Mobility
- Payment
- …

-> Many IoT devices are generating, processing, storing or transferring personal data!
"WORST EXAMPLES OF IOT VULNERABILITIES"

MANY IOT DEVICE HACKS AFFECT PRIVATE DATA!

Source: https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/ and https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/

Armored Games (AG) has confirmed that 100 per cent of its users were caught up in February’s mega-leak that saw the details of 617 million online accounts hacked from 16 hacked websites being sold on the dark web.
controller and the processor shall implement **appropriate technical and organisational measures** to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and **encryption of personal data**;
(b) the ability to ensure the ongoing **confidentiality, integrity, availability and resilience of processing systems and services**;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a **process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures** for ensuring the security of the processing.
Taking into account the **state of the art**, the cost of implementation and the nature, scope, (…) the controller shall, (…), implement appropriate technical and organisational measures, such as pseudonymisation, (…), such as data minimization, (…)
GENERATING TRUST VIA COMPLIANCE
REducing Financial Risks by Applying to Article 25 & 32

- Generate Legal certainty for investors by becoming “GDPR compliant” via proper testing and certification
  - Develop and manufacture GDPR compliant products
  - Become “GDPR compliant” from a holistic point of view via e.g. installing GDPR compliant devices within networks only

- Data Protection Impact Assessment (DPIA): Generate Risk+Impact Assessment for each IoT device

1. What are appropriate technical measures?
2. What is “State-of-the-Art”?
3. What can manufacturer do?

- Up to now there is no technical catalogue or guideline available what exactly needs to be implemented in terms of cybersecurity into IoT devices which are processing (generating, processing, storing or transferring) personal data to fulfil the GDPR requirements

- There are now standards available which include privacy related requirements to protect PII in IoT devices and ancillary services to make them “GDPR-ready/ compliant”.

INFOCLASS: UNCLASSIFIED TLP: WHITE
“State-of-the-Art”: Using a strong governance system / management system based on ISO 27K and 27701 (privacy extension to ISMS) as an essential foundation it is about demonstrating compliance of IoT devices according to existing IoT Cybersecurity standards and certification schemes:

EN 303 645 and TS 103 701 are well placed to provide the foundation for “basic”-level consumer IoT assurance:

IEC 62443-4-2 Technical security requirements for IACS components:

European cybersecurity certification scheme (EUCC) based on common criteria, a voluntary scheme with a set of security requirements for ICT security products

-> SGS is able to support you in generating the right level of trust you want to achieve for your IoT devices and services and support you with the assessment and certification services.
THANK YOU FOR LISTENING!

WWW.SGS.COM