Input: Privacy by Design – defaults, information and users’ rights

Marit Hansen
Data Protection Commissioner
Schleswig-Holstein, Germany

Annual Privacy Forum – Rome, 13 June 2019

Data Protection by Design & by Default

• Art. 25 GDPR

• Targeted at controllers

• Producers of IT systems “should be encouraged” (Rec. 78)

• Objective: to design systems + services from early on, for the full lifecycle …
  a) … in a data-minimising way
  b) … with the most data protection-friendly pre-settings

Art. 25 Data Protection by Design and by Default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, […]
Data Protection by Design & by Default

- Art. 25 GDPR
- Targeted at controllers
- Producers of IT systems “should be encouraged” (Rec. 78)
- Objective: to design systems + services from early on, for the full lifecycle …
  a) … in a data-minimising way
  b) … with the most data protection-friendly pre-settings

Art. 25 Data Protection by Design and by Default

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. […]

Protection Goals: from IT security to privacy

- Confidentiality
- Unlinkability
- Integrity
- Intervenability
- Transparency
- Availability

classical IT security protection goals*)

Data minimisation

*) From the data subject’s perspective
How to implement?

Unlinkability

- Separation of domains, separation of power, purpose binding

Transparency

- Objective: awareness, understanding and control; different media, support by technology

Intervenability

- E.g. opt-out, complaints, judicial relief, reversing decisions ...
- Deactivating sensors and data processing, defined help desk ...

Objective: risk mitigation – i.e. of the risk for the rights and freedoms of natural persons

Enhancing transparency

Clear and simple language
“Layered Policies”
Standardised icons (Art 12(7) GDPR)
Machine readable

Privacy by Design – defaults, information and users’ rights
Call for machine-reability – finally!?

History: P3P as one of the early proposals + follow-up work (e.g. policy languages)
But by now not very successful!
Now: Call for GDPR-tailored machine-readable solutions that work in specific or several contexts

Privacy by Design – defaults, information and users’ rights

E.g. for consent management

EU Project
SPECIAL – Scalable Policy-aware linked data architecture for privacy, transparency and compliance

Beware!
Self-protection tools not sufficient:
We must not put the burden on the user!

Forbrukerrådet (Norway 2018): Report „Deceived by Design“, https://www.forbrukerradet.no/dark-patterns/