Privacy by Design

Dr. Moritz Karg
Referent bei der Dienststelle des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit
Concept

“The current challenges to privacy are driven by the synergy between the fundamentally positive forces of innovation, competition, and the worldwide adoption of new information technologies. The solution, therefore, must be woven or baked into these synergetic forces. Privacy must become the default mode of design and operation.

This is precisely the aim of Privacy by Design (PbD) – the philosophy and methodology of embedding privacy into the design specifications of information technologies, business practices, and networked infrastructures as a core functionality. Privacy by Design means building in privacy right up front, directly into the design specifications and architecture of new systems and processes.”

1
Definition

“In brief, PbD offers a framework for ensuring that privacy is embedded directly into the design specifications of information technologies, business practices and operational processes. When applied, PbD allows for greater privacy and personal control over one’s information, while enabling organizations to gain a competitive advantage, that is sustainable over time.” ²
Examples

- smart metering
- design of protection profile (technical specifications)
- legal basis (EnWG & Gesetz zur Digitalisierung der Energiewende 29.08.2016)
Core Characteristics and Incentives

- part of system of privacy enhancing technologies (PET)
- synergy between development of privacy friendly technology and competitive advantage
- fostering sustainable privacy protection
The Foundational Principles recognized by the 32. Conference of Data Protection and Privacy Commissioners, 2010³

- Proactive not Reactive; Preventative not Remedial
- Privacy as the Default
- Privacy Embedded into Design
- Full Functionality: Positive-Sum, not Zero-Sum
- End-to-End Lifecycle Protection
- Visibility and Transparency
- Respect for User Privacy
Regulatory Claims for Implementation by Art-29-Group

“First, the principle of ‘privacy by design’ should be introduced in the new framework; second, as the need arises, regulations for specific technological contexts should be adopted which require embedding data protection and privacy principles into such contexts.”

 […]

This principle [PbD] should be binding for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of ICT. They should be obliged to take technological data protection into account already at the planning stage of information-technological procedures and systems.”

4
Challenges for Data Protection Authorities

- identification and regulatory implementation of relevant substantive principles
- enforcement of privacy by design
Privacy by Design is a Procedural Framework

- necessity for substantive principles
- characteristics
  - technologically neutral but specific requirements for high-risk technology (e.g. processing of health data, biometric data)
  - flexible to allow case-by-case-implementation
  - substantive requirements (objectives of data protection and security)
    - secrecy and security
    - integrity (incl. Accountability)
    - availability
    - purpose limitation (appropriation and avoidance of chaining personal data) and necessity
    - Transparency and information
    - intervenability (controllability and accountability)
„Solution“ of GDPR

Art. 25 para 1:

„[…] implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.“
„Solution“ of GDPR

- substantive requirements of PbD by GDPR
  - general
    - requirements of regulation – reference to Art. 5 GDPR
  - explicit
    - pseudonymisation - protection of identity and reduction of depth of information
    - data minimisation – enforcement of necessity-principle
    - recital 78
      - transparency
      - monitoring by the data subject
      - ability of controller to create and improve security features (data security)
temporal aspects

- cradle-to-grave-principle
- consideration shall start already in the context of public tenders
- technical design and organisation must allow adjustment to changing technical and legal environment
- foreseeing and anticipation of terminal point of processing – retention periods and deletion routine
Do privacy by design and talk about it!
Office of the Hamburg Commissioner for Data Protection and Freedom of Information

Dr. Moritz Karg
Senior Legal Adviser, Department of Telemedia, Telecommunication, Media and E-Government
E-mail: moritz.karg@datenschutz.hamburg.de

Sources

2. Ibid, p. III