Tempora mutantur et nos mutamur in illis

Datenschutzbehörden und
Privacy-Enhancing Technologies (PETs)

Dr. John Borking

(Folien ins Deutsche übersetzt)

Die Zeiten ändern sich, und wir ändern uns in ihnen

- Haben PETs die Arbeit von Datenschutz-Aufsichtsbehörden verändert?
- Blick zurück:
  Das Technology Assessment zu PETs in 1994 wäre nicht möglich gewesen, wenn die niederländische Datenschutzbehörde sich nicht zu einer proaktiven Organisation entwickelt hätte.

1994: SWOT der Datenschutzbehörde NL

- SWOT-Analyse:
  - 1. eigene Stärken und Schwächen
  - 2. Chancen und Risiken in der Umgebung der Behörde

- Ergebnis:
  Die Datenschutzbehörde muss sich zu einer proaktiven, kundenorientierten Organisation wandeln

Eine proaktive Auffassung erreichen

- Die Datenschutzbehörde NL hat wegen der Unabhängigkeit einen erheblichen Spielraum, um Ausrichtung und Inhalt ihrer Aktivitäten zu bestimmen.
- Die Transformation der Datenschutzbehörde NL folgte einer Vision (eine eindeutige Vorstellung der gewünschten Zukunft, wohin gehen wir?) und einem Leitbild (wieso gibt es uns, was sind unsere Aufgaben, wer sind unsere Kunden, welche Produkte oder Dienste stellen wir bereit?)
- Ergebnisse unseres Brainstormings:
  - durch Technology Assessments das relevante Wissen erhöhen &
  - das Datenschutzrecht durch gezielte EDV-Audits durchsetzen

Frage: Können Informationssysteme weiterhin funktionieren, wenn sie weniger personenbezogene Daten verarbeiten?

- Ja, durch einen „Identity Protector (IP)“ und den Einsatz von Techniken zum Anonymisieren und Pseudonymisieren, um getrennte Identitäts-Domänen zu schaffen, in denen die Identität der Nutzenden des Systems jeweils bekannt oder unbekannt ist
- Theoretische Basis ist valide.
  Also Entwicklung von PET-Innovationstechnologien
- Notwendig: ein funktionierendes PET-System als Referenz (erstes Krankenhaus-Informationssystem in einem psychiatrischen Krankenhaus 1997)
- Widerlegen des Datensicherheitsarguments:
  1995: Datenschutz-Risikoklassen der Datenschutzbehörde
- Veröffentlichung der Ergebnisse auf Niederländisch und Englisch

Lücke zwischen Offline- und Online-Privacy

- Auch im Internet müssen Betroffene sich selbst schützen können, ohne von der Gnade der Website-Anbieter abhängig zu sein
- EU-geförderte PET-Studie (1999) zur Entwicklung eines „Privacy incorporated Software Agent (PISA)“ zum Aushandeln der Bedingungen, unter denen personenbezogene Daten herausgegeben werden – das ist machbar
- Online- und Offline-Privacy lässt sich durch geschickte Gestaltung erreichen [Hoepman: „Privacy is hard and seven other myths”, 2021]

Das „PET Adoption Problem“

- Organisatorische und ökonomische Hindernisse für das Verwenden von PETs [siehe Rogers: „Diffusion of Innovations“, 1962]
- Organisationen werden von einer Vielzahl von Faktoren in ihrer Entscheidung, ob sie PETs implementieren, beeinflusst [Forschungsergebnisse im PRIME-Projekt]
- Wichtiger Faktor für die Implementation von PETs: aktive Beratungsrolle der Datenschutzbehörden [Forschungsergebnisse, siehe Borking 2010].
  Um PETs in die Praxis zu bringen, proaktiver Druck von Datenschutzbehörden auf Organisationen nötig [Bos 2006, Hosein 2007]
- Würden die positiven Umsetzungsfaktoren genutzt, könnten Organisationen PETs in ihren Informationssystemen viel schneller im großen Rahmen implementieren
- Entscheidender Faktor: ein von Datenschutzbehörden unterstütztes Datenschutz-Gütesiegel, das Datenschutzkonformität für ein PET-System bestätigt

Fazit

- Datenschutzfreundliche Informationssysteme für jede Umgebung
- Techniken, Architekturen (Privacy by Design) und Datenschutzmanagementsysteme sind verfügbar
- Jedoch suboptimaler Einsatz von PETs
- Aktives Fördern und Durchsetzen von PETs nötig
- Als Aufgabe der Datenschutzbehörden
- Schutz vor der Entwicklung der Menschen zu einem „digitalen Proletariat“, das sich von Technik steuern lässt