Privacy by design

Christoph Isele

Gmds Workshop

9.Oktober 2017

Zusammenfassung

- Datenschutz durch Technikgestaltung wendet sich zunächst an den Verantwortlichen, der den gesamten Prozess betrachten und absichern muss.
- Das „Schlagwort“ Privacy by Design wurde von Ann Cavoukian geprägt, die mit der Resolution der Datenschutzbeauftragen 2010 in Jerusalem 7 Prinzipien zur Diskussion stellte.
- Die abstrakten Prinzipien führten zu den konkreten Weiterentwicklung wie Privacy Enhancing Technology oder Privacy Engineering, die nur teilweise im Alltag umgesetzt wurden.

Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen **trifft der Verantwortliche** sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung **geeignete technische und organisatorische Maßnahmen** … die Rechte der betroffenen Personen zu schützen.

(2) **Der Verantwortliche** trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. …

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 ...

Erwägungsgrund 78

- … **Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen**, …
- In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, **sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden,** das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen.

PbD: Ann Cavoukian (2010)

“As the Information and Privacy Commissioner of Ontario, Canada, my mandate is to raise awareness of privacy-related issues involved in emerging technologies …”

32nd International Conference of Data Protection and Privacy Commissioners
Jerusalem, Israel
27-29 October, 2010
Resolution on Privacy by Design

Privacy by Design: The Foundational Principles

- **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**

Privacy by Design: The Foundational Principles

- 1. ***Proactive*** not Reactive; ***Preventative*** not Remedial
  The *Privacy by Design* approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. *Privacy by Design* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.
- 2. Privacy as the ***Default Setting***
  We can all be certain of one thing — the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.

Privacy by Design: The Foundational Principles (2)

- 3. Privacy ***Embedded*** into Design
  Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.
- 4. Full Functionality — ***Positive-Sum***, not Zero-Sum
  Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum win-win manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy vs. security – demonstrating that it is possible to have both.

Privacy by Design: The Foundational Principles (3)

- 5. End-to-End Security — ***Full Lifecycle Protection***
  Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, secure lifecycle management of information, end-to-end.
- 6. ***Visibility*** and ***Transparency*** — Keep it ***Open***
  Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

Privacy by Design: The Foundational Principles (4)

- 7. ***Respect*** for User Privacy — Keep it ***User-Centric***
  Above all, *Privacy by Design* requires architects and operators to protect the interests of the individual by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Federal Trade Commission: Fair Information Practices

1. Notice / Awareness
2. Choice / Consent
3. Access / Participation
4. Integrity / Security
5. Enforcement / Redress

OECD: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle

- Privacy enhancing technology
- Privacy engineering
- Privacy design framework

Privacy Enhancing Technology

- enisa 2014: Privacy and Data Protection by Design – from policy to engineering
  - This report shall promote the discussion on how privacy by design can be implemented with the help of engineering methods. It provides a basis for better understanding of the current state of the art concerning privacy by design with a focus on the technological side.

  - Engineering Privacy
  - Privacy Design Strategies
  - Privacy Techniques

https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

enisa 2014: privacy design strategies

- #1: MINIMISE
- #2: HIDE
- #3: SEPARATE
- #4: AGGREGATE
- #5: INFORM
- #6: CONTROL
- #7: ENFORCE
- #8: DEMONSTRATE

in Anlehnung an J-H Hoepmann, 2014

- Technisch
  - Minimise: Nur notwendige Daten speichern und verarbeiten
  - Separate: Daten verteilt verarbeiten und speichern
  - Aggregate: Daten auf das notwendige Maß zusammenfassen
  - Hide: Daten nicht in offener Form speichern
- Organisatorisch
  - Enforce: Durchsetzung einer Datenschutz-Policy (access control)
  - Inform: Betroffene über Datenverwendung informieren (P3P)
  - Control: Eingriffsmöglichkeit der Betroffenen (informed consent)
  - Demonstrate: Überprüfbarkeit (privacy management, logging)

Diskussion

DANKESCHÖN!