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

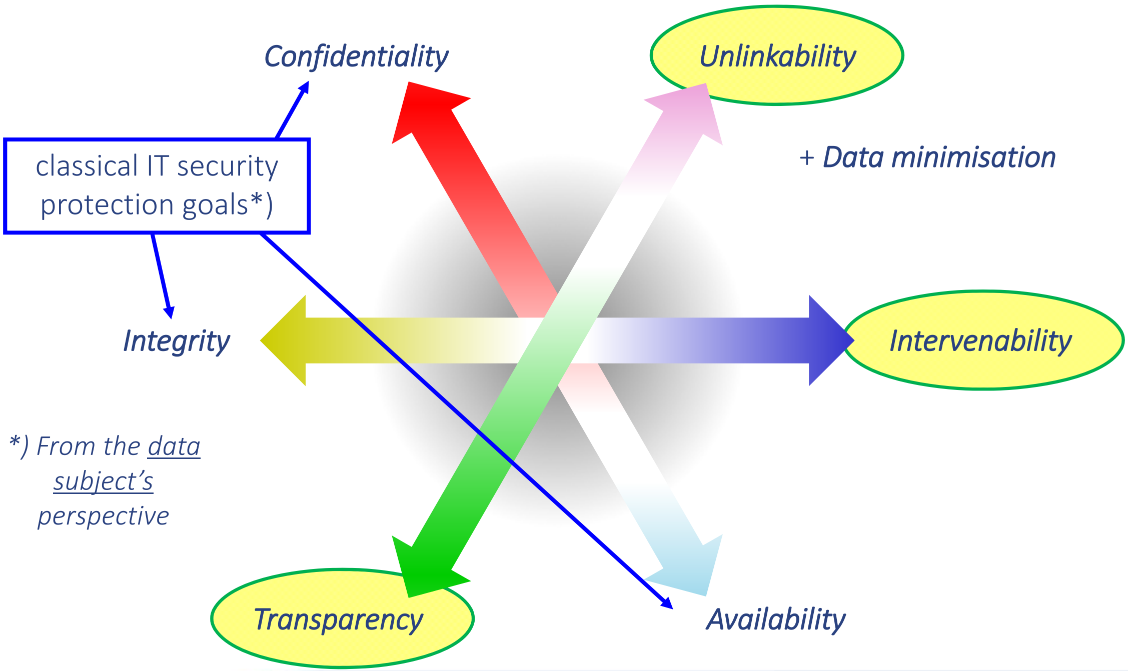
- Art. 25 GDPR
- Targeted at controllers
- Producers of IT systems “should be encouraged” (Rec. 78)
- Objective: to design systems + services from early on, for the full lifecycle …
  a) … in a data-minimising way
  b) … with the most data protection-friendly pre-settings

Art. 25 Data Protection by Design and <u>by Default</u>

No excuse!

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



*) From the <u>data subject’s</u> perspective

How to implement?

Unlinkability

Separation of domains, separation of power, purpose binding

Photo: ivanacoi via Pixabay

Transparency

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

Photo: geralt via Pixabay

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

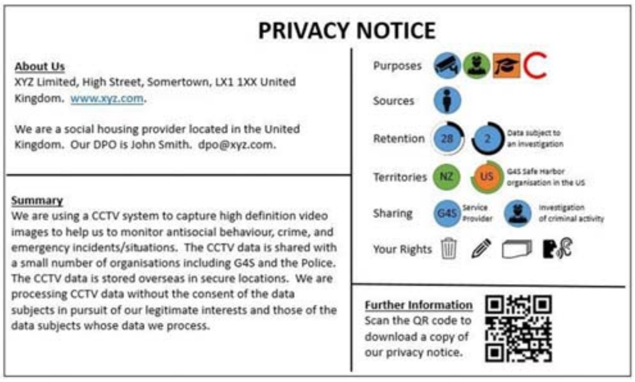
Photo: geralt via Pixabay

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

Intervenability

Enhancing transparency

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



PRIVACY NOTICE

About Us
XYZ Limited, High Street, Somertown, LX1 1XX United Kingdom. www.xyz.com.

We are a social housing provider located in the United Kingdom. Our DPO is John Smith. dpo@xyz.com.

Summary
We are using a CCTV system to capture high definition video images to help us to monitor antisocial behaviour, crime, and emergency incidents/situations. The CCTV data is shared with a small number of organisations including G4S and the Police. The CCTV data is stored overseas in secure locations. We are processing CCTV data without the consent of the data subjects in pursuit of our legitimate interests and those of the data subjects whose data we process.

Purposes

Sources

Retention 28 2 Data subject to an investigation

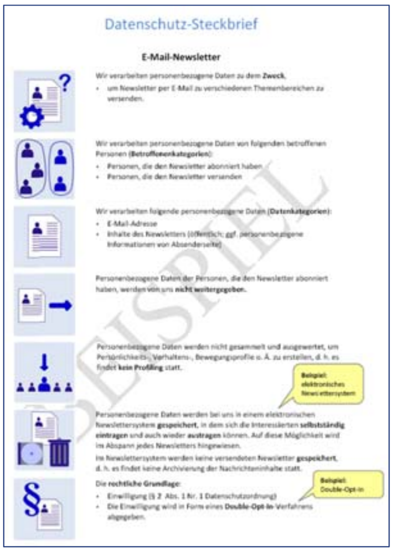
Territories NZ US G4S Safe Harbor organisation in the US

Sharing G4S Service Provider Investigation of criminal activity

Your Rights

Further Information
Scan the QR code to download a copy of our privacy notice.

http://www.dataprotectionpeople.com/5918-2/ (January 2016)



Datenschutz-Steckbrief

E-Mail-Newsletter

Wir verarbeiten personenbezogene Daten zu dem **Zweck**,
- um Newsletter per E-Mail zu verschiedenen Themenbereichen zu versenden.

Wir verarbeiten personenbezogene Daten von folgenden betroffenen Personen (**Betroffenenkategorien**):
- Personen, die den Newsletter abonniert haben
- Personen, die den Newsletter versenden

Wir verarbeiten folgende personenbezogene Daten (**Datenkategorien**):
- E-Mail-Adresse
- Inhalte des Newsletters (öffentlich; ggf. personenbezogene Informationen von Absenderseite)

Personenbezogene Daten der Personen, die den Newsletter abonniert haben, werden von uns **nicht weitergegeben**.

Personenbezogene Daten werden nicht gesammelt und ausgewertet, um Persönlichkeits-, Verhaltens-, Bewegungsprofile o. Ä. zu erstellen, d. h. es findet **kein Profiling** statt.

Beispiel: elektronisches Newslettersystem

Personenbezogene Daten werden bei uns in einem elektronischen Newslettersystem **gespeichert**, in dem sich die Interessierten **selbstständig eintragen** und auch wieder **austragen** können. Auf diese Möglichkeit wird im Abspann jedes Newsletters hingewiesen.

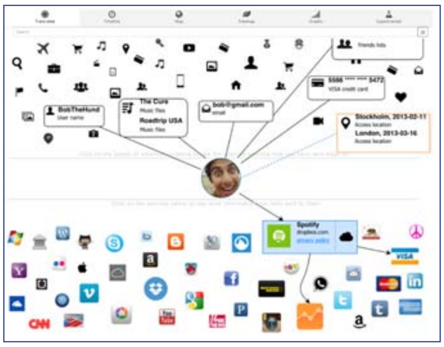
Im Newslettersystem werden keine versendeten Newsletter **gespeichert**, d. h. es findet keine Archivierung der Nachrichteninhalte statt.

Die **rechtliche Grundlage**:
- Einwilligung (§ 2 Abs. 1 Nr. 1 Datenschutzordnung)
- Die Einwilligung wird in Form eines **Double-Opt-In**-Verfahrens abgegeben.

Beispiel: Double-Opt-In

BEISPIEL

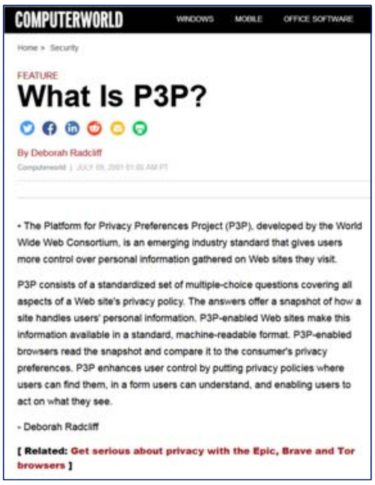
https://www.datenschutzzentrum.de/dokumentation/ (2019)



Source: Angulo et al. (2015): Usable Transparency with the Data Track: A Tool for Visualizing Data Disclosures, CHI EA '15 http://dx.doi.org/10.1145/2702613.2732701

Multi-level policies:
see also WP100 (2004):
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp100_en.pdf

Call for machine-reability – finally!?



COMPUTERWORLD WINDOWS MOBILE OFFICE SOFTWARE

Home > Security

FEATURE

What Is P3P?

By Deborah Radcliff

Computerworld | JULY 09, 2001 01:00 AM PT

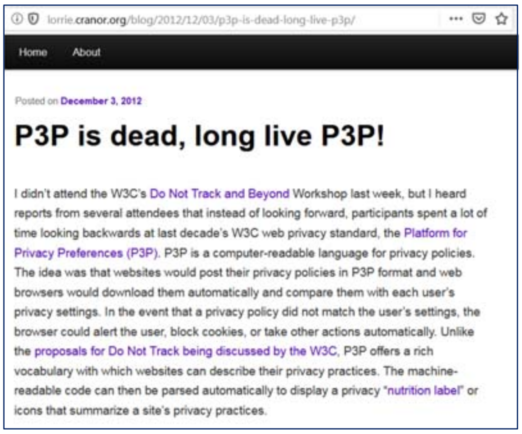
- The Platform for Privacy Preferences Project (P3P), developed by the World Wide Web Consortium, is an emerging industry standard that gives users more control over personal information gathered on Web sites they visit.

P3P consists of a standardized set of multiple-choice questions covering all aspects of a Web site's privacy policy. The answers offer a snapshot of how a site handles users' personal information. P3P-enabled Web sites make this information available in a standard, machine-readable format. P3P-enabled browsers read the snapshot and compare it to the consumer's privacy preferences. P3P enhances user control by putting privacy policies where users can find them, in a form users can understand, and enabling users to act on what they see.

- Deborah Radcliff

[Related: Get serious about privacy with the Epic, Brave and Tor browsers]

```
https://www.computerworld.com/article/
2582859/what-is-p3p-.html
```



lorrie.cranor.org/blog/2012/12/03/p3p-is-dead-long-live-p3p/

Home About

Posted on **December 3, 2012**

P3P is dead, long live P3P!

I didn't attend the W3C's Do Not Track and Beyond Workshop last week, but I heard reports from several attendees that instead of looking forward, participants spent a lot of time looking backwards at last decade's W3C web privacy standard, the Platform for Privacy Preferences (P3P). P3P is a computer-readable language for privacy policies. The idea was that websites would post their privacy policies in P3P format and web browsers would download them automatically and compare them with each user's privacy settings. In the event that a privacy policy did not match the user's settings, the browser could alert the user, block cookies, or take other actions automatically. Unlike the proposals for Do Not Track being discussed by the W3C, P3P offers a rich vocabulary with which websites can describe their privacy practices. The machine-readable code can then be parsed automatically to display a privacy "nutrition label" or icons that summarize a site's privacy practices.

```
http://lorrie.cranor.org/blog/2012/12/03/
p3p-is-dead-long-live-p3p/
```

Image: jeferrb via Pixabay

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

E.g. for consent management

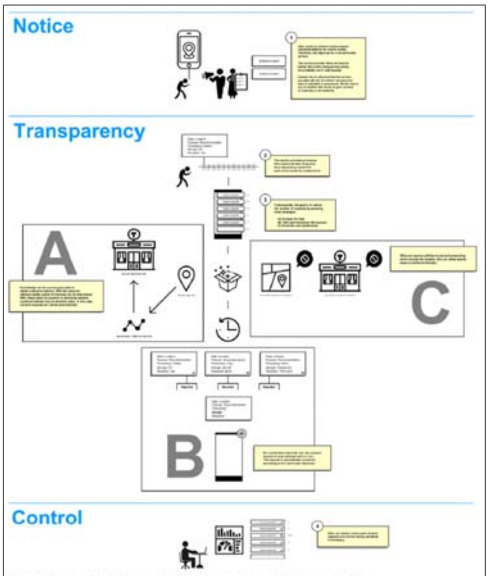


Figure 5: Storyboard for the concept of dynamic consent regarding the user interface

SPECIAL

EU Project
SPECIAL – Scalable Policy-awarE linked data arChitecture for prIvacy, trAnsparency and compLiance

```
https://www.specialprivacy.eu/
```

Beware!

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

DECEIVED BY DESIGN

How tech companies use dark patterns to discourage us from exercising our rights to privacy

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