Data Protection by Default – Requirements, Solutions, Questions

Marit Hansen
Data Protection Commissioner
Schleswig-Holstein, Germany

IPEN Workshop
Vienna, 9 June 2017

forum <privatheit> selbstbestimmtes_leben_in_der_digitalen_welt

ipen

ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Setting of ULD

- Data Protection Authority (DPA) for both the public and private sector
- Also responsible for freedom of information

Schleswig-Holstein
State of Germany

Flag

Coat of arms

Coordinates: 54°28'12"N 9°30'50"E

Country	Germany
Capital	Kiel
Government	
• Minister-President	Torsten Albig (SPD)
• Governing parties	SPD / Greens / SSW
• Bundesrat votes	4 (of 69)
Area	
• Total	15,763.18 km² (6,086.20 sq mi)
Population (2014-12-31)[1]	
• Total	2,830,864
• Density	180/km² (470/sq mi)

Source: en.wikipedia.org/wiki/Schleswig-Holstein

Source: www.maps-for-free.com

Overview

- Privacy by Default
- Data Protection by Design and by Default: not the same!
- How to?
- Potential undesired effects
- Conclusion

Privacy by Default à la Cavoukian

"Privacy by default":

- Part of "privacy by design"
- Privacy as the default setting:
  "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."

Photo: anncavoukian.com

→ *But what about an acting individual?*
→ *Is full system functionality achievable?*

Comment on early GDPR draft by the EDPS (2012)

EUROPEAN DATA PROTECTION SUPERVISOR
The European guardian of personal data protection

"The principle of data protection by default aims at protecting the data subject in situations in which there might be a lack of understanding or control on the processing of their data, especially in a technological context.

The idea behind the principle is that privacy intrusive features of a certain product or service are initially limited to what is necessary for the simple use of it.

The data subject should in principle be left the choice to allow use of his or her personal data in a broader way."

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf

Characteristics of defaults in design

- Default means:
  - Initial pre-setting (not only software UI)
  - Changes are possible …
  - … but usually not needed
  - Usually many users won't change it
  - In software design: "principle of least astonishment"


Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising

Leon et al. (2012): Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising

- Defaults can be powerful:

The **default effect** is the tendency for the vast majority of people to accept the default in an interaction. This occurs when avoiding the default is virtually effortless and increases with each step that is required to avoid the default. The default effect has significant implications for marketing, choice architecture, user experience, ethics and law.

http://simplicable.com/new/default-effect

E.g.: non-default actions for consent or buying goods

Data Protection by Design & by Default

- Art. 25 GDPR
- Targeted at controllers + data processors
- Producers of IT systems "should be encouraged" (Rec. 78)

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, […]

- 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

ULD www.datenschutzzentrum.de

Data Protection by Design & by Default

- Art. 25 GDPR
- Targeted at controllers + data processors
- Producers of IT systems "should be encouraged" (Rec. 78)

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. […]

- 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

Conditions "state of the art" and "the cost of implementation"?

Identical wording in Art. 25 + Art. 32 "Security of processing"

Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and processing as well as the risks of varying likelihood and severity for rights and processing, the controller shall, both at the time of the determination of the processing itself, implement appropriate technical and organisational measures designed to implement data-protection principles, such as data minimisation, necessary safeguards into the processing in order to meet the requirements data subjects.

2. The controller shall implement appropriate technical and organisation only personal data which are necessary for each specific purpose of the proce to the amount of personal data collected, the extent of their processing, the p In particular, such measures shall ensure that by default personal data are n intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may compliance with the requirements set out in paragraphs 1 and 2 of this Artic

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural controller and the processor shall implement appropriate technical and organisational measures to ensu security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure o personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification referred to in Article 42 may be used as an element by which to demonstrate compliance with the require in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the au

Several potentially limiting conditions (= upper + lower bound)

ULD www.datenschutzzentrum.de

Conditions "state of the art" and "the cost of implementation"?

On EU level nothing new, see Data Protection Directive 95/46/EC

Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and

Data Protection by Default

No potentially limiting conditions (SotA, costs, risks): more powerful?

Related to the "purpose limitation" principle (Art. 5)

Article 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.

In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Influences access rights, encryption, location of storage (country/processor), ...

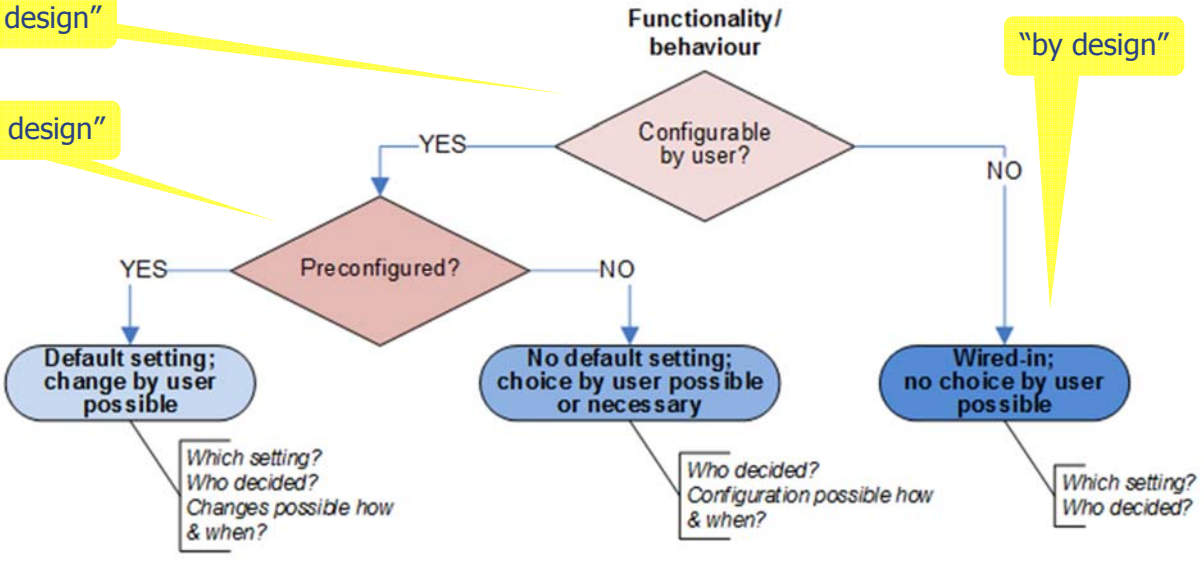
Social network clause

Three cases for "(pre-)configurability"

"by design"

"by design"

"by design"



Ex.: anonymous use, no tracking

Ex.: choice of payment system

Ex.: encrypted communication

Two different types of configuration

1. Configuration of a process necessary for the purpose within the application

   Not so easy answer on the best default
   – depending on the purpose / functionality

2. Configuration of an additional process that is not strictly needed for the original purpose (≠ "simple use" / "basic functionality")

   Easy answer: Default = "NO"
   if additional purpose / party / personal data processing

Checks for defaults w.r.t. necessary processes

Check:

- What do users expect? Rights & freedoms/interests?
  - In general?
  - On a more individual base?

  Granularity?
  Usability?
  User guidance?

- Where is user interaction necessary?
  - To decide on important parameters
    - Where to process data? Which jurisdiction?
    - Which additional parties?
    - Costs?
  - E.g.: choice of payment system
  - E.g.: choice of cloud storage location

  "One size fits all" doesn't work here

Scenarios for undermining the idea of DP by Default

By obstructing functionality or usability:

- Providing defaults that won't work conveniently
- Demanding user decisions too frequently

In all these cases:
Blaming DP law + authorities

By ignoring "simple use" options:

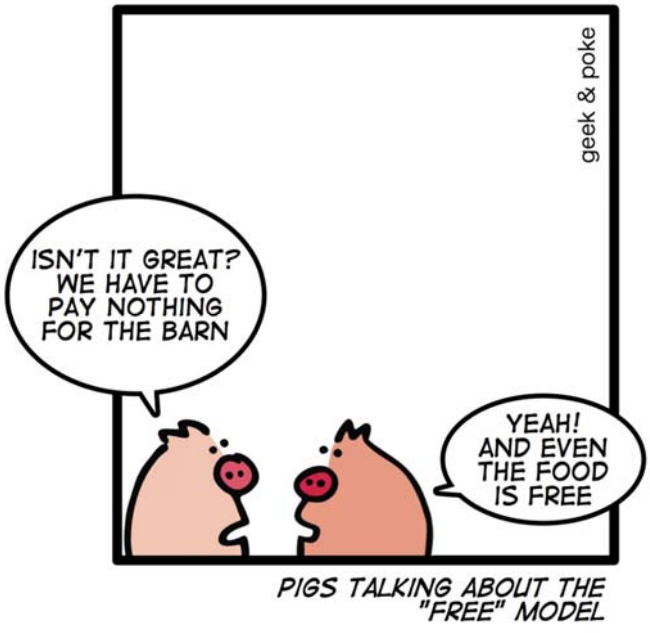
- Offering only services for purposes which need the data (e.g. personalised information)
- Relying on greedy technologies / infrastructures

By collecting more data:

- Data for finding out the best default for the user
- Good default, but any change will cause massive data collection (consent)

Potential side effects of DP by Default

- No default "payment by data": effect on business models, increasing prices
- Smart meter example (in standard implementation): transmission of only 1 value/year instead of smaller intervals not helpful for energy transition
- Disguising other default decisions (lock-in mechanisms)



http://geek-and-poke.com/geekandpoke/2010/12/21/the-free-model.html

Conclusion

- "Data Protection by Default"
  - … is a rather absolute requirement
  - … can be a game changer
  - … and "… by Design" are unlike twins

Photo: Leon Riskin

- Practical guidance is necessary:
  - How to figure out (the) best default(s)?
  - Best for which user groups?

- Many open questions in practice:
  - How to achieve by controllers?
  - How to supervise by DPAs?

Side remark

BTW: All translations are equivalent, aren't they?

- [FR] Article 25: Protection des données dès la conception et protection des données par défaut
- [ES] Artículo 25: Protección de datos desde el diseño y por defecto
- [NL] Artikel 25: Gegevensbescherming door ontwerp en door standaardinstellingen
- [DA] Artikel 25: Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger
- [SV] Artikel 25: Inbyggt dataskydd och dataskydd som standard
- [DE] Artikel 25: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Side remark

Check your language on Art. 25 (2)!

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. […]

(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. […]

MISTAKE:
extra word in the German version: "grundsätzlich" ("as a rule")

Thanks for your attention!

Marit Hansen

ULD, Holstenstr. 98, 24103 Kiel, Germany
marit.hansen@datenschutzzentrum.de

forum <privatheit> selbstbestimmtes_leben_in_der_digitalen_welt

iper

ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein