

Privacy & Usability

The perspective of a Data Protection Commissioner

Marit Hansen
Data Protection Commissioner
Schleswig-Holstein, Germany

Privacy & Us
Kiel, 1 July 2019



www.datenschutzzentrum.de

Overview



Source: stux via Pixabay

- Privacy & Usability going together
- Requirements from the GDPR
 - Principles
 - Information
 - Data Protection by Design and by Default
- Adverse effects
- Conclusion

General remarks

- Usability is a **requirement for all interaction** with human beings
- In the field of privacy and data protection:
 - Support^{*)} of **data subjects**
 - Support^{*)} of users on behalf of data **controllers** and data **processors**
 - ^{*)}: **Support** means:
 - **facilitate** data-protection friendly actions,
 - **prevent** undesired actions,
 - proper **defaults**
- **"Non-usability"** as a suitable measure for data protection?
 - *"Our system is so complex that an attacker could not understand it ..."*
 - Security... by obscurity ✗ **NO!**

Overview



 Source: stux via Pixabay

- Privacy & Usability going together
- **Requirements from the GDPR**
 - Principles
 - Information
 - Data Protection by Design and by Default
- Adverse effects
- Conclusion

Data protection principles

Whenever **personal data** are processed,

Art. 5 (1) GDPR:

- a) 'lawfulness, fairness and transparency'
- b) 'purpose limitation'
- c) 'data minimisation'
- d) 'accuracy'
- e) 'storage limitation'
- f) 'integrity and confidentiality'

Personal data:
any information relating
to an identified or
identifiable natural
person ('data subject')

Art. 5 (2) GDPR:

'accountability'

GDPR: leverage on business? High fines. Theory or reality?

Article 83

General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

GDPR: leverage on business? High fines. Theory or reality?

Article 83

General conditions for imposing administrative fines

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
- (b) the data subjects' rights pursuant to Articles 12 to 22;

Overview



Source: stux via Pixabay

- Privacy & Usability going together
- Requirements from the GDPR
 - Principles
 - **Information**
 - Data Protection by Design and by Default
- Adverse effects
- Conclusion

Consent

- “‘consent’ of the data subject means any **freely given, specific, informed and unambiguous indication** of the data subject's wishes by which he or she, **by a statement or by a clear affirmative action**, signifies agreement to the processing of personal data relating to him or her;” – Art. 4 No. 11 GDPR
Design of information and communication
- “If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is **clearly distinguishable from the other matters**, in an **intelligible and easily accessible form**, using **clear and plain language**.” – Art. 7 (2) s. 1 GDPR
- “It shall be **as easy to withdraw as to give consent**.” – Art. 7 (3) s. 4 GDPR
Design of functionality

Data subjects' rights: information

- “The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject **in a concise, transparent, intelligible and easily accessible form**, using **clear and plain language**, in particular for any information addressed specifically to a child.” – Art. 12 (1) s. 1 GDPR
- “The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided **in combination with standardised icons** in order to give in an **easily visible, intelligible and clearly legible** manner a **meaningful overview** of the intended processing. Where the icons are presented electronically they shall be machine-readable.” – Art. 12 (7) GDPR
Design of information and communication

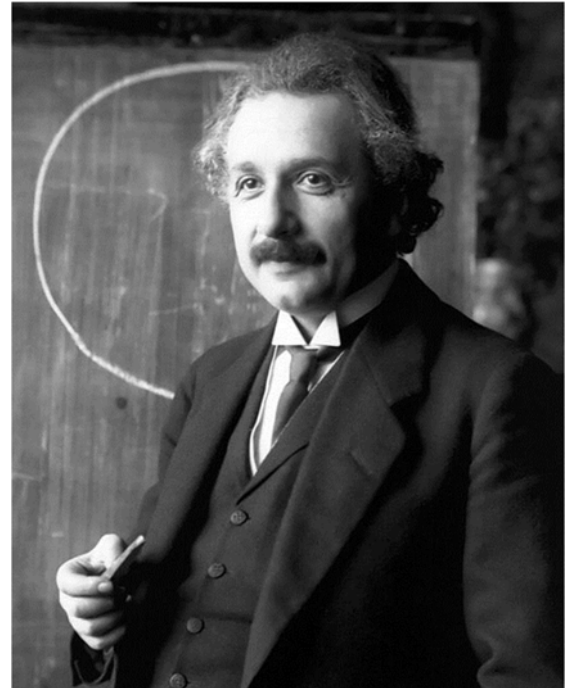
Simplify your information

Everything should be as simple as possible, but not simpler.

- Albert Einstein



Source: Karolina Grabowska via Pixabay



Formulas for clear text: readability

<https://saskia-vola.com/simple-metrics-for-textmining>

- **Readability** according to Carl-Hugo Björnsson, 1971: higher for simple texts that consist of short sentences and short words
- $$\text{LIX}(\text{text}) = \text{TotalWords}/\text{Sentences} + (\text{LongWords} \times 100)/\text{TotalWords}$$
- Typical LIX values between 20 (newspaper) and 70 (research paper)

How often used by DP authorities per year?
How many fines?

Formulas for clear text: informativity

<https://saskia-vola.com/simple-metrics-for-textmining>

- **Informativity:** higher when there are a lot of pieces of information one could capture without knowing the context or the author
- Relative amount of content words to non-content words
- **Content words:** nouns, proper nouns, verbs, and adjectives
- The content function ratio (CFR):

$$\text{CFR}(\text{text}) = \frac{\text{AmountOfContentWordTags}}{\text{AmountOfFunctionWordTags}}$$

How often used by DP authorities per year?
How many fines?

Comprehensibility index of the University of Hohenheim

Formeln	Text-Parameter
<ul style="list-style-type: none"> • Amstad-Formel • Wiener Sachtext-Formel • SMOG-Index (Deutsch) • Lix Lesbarkeits-Index 	<ul style="list-style-type: none"> • Durchschnittliche Satzlänge in Wörtern • Durchschnittliche Satzteilänge in Wörtern • Durchschnittliche Wortlänge in Buchstaben • Anteil der Wörter mit mehr als 6 Buchstaben • Anteil der Satzteile mit mehr als 12 Wörtern • Anteil der Sätze mit mehr als 20 Wörtern

Abbildung 4: Hohenheimer Verständlichkeits-Index

<https://www.service-tested.de/wp-content/uploads/2016/04/Erklärung-Verfahren-TÜV-geprüfte-Verständlichkeit.pdf>

<https://klartext.uni-hohenheim.de/hix>

Scale 0-20, e.g.

- doctoral thesis
- political science: 0-4
- BILD 16-20



Hohenheimer Index by TÜV

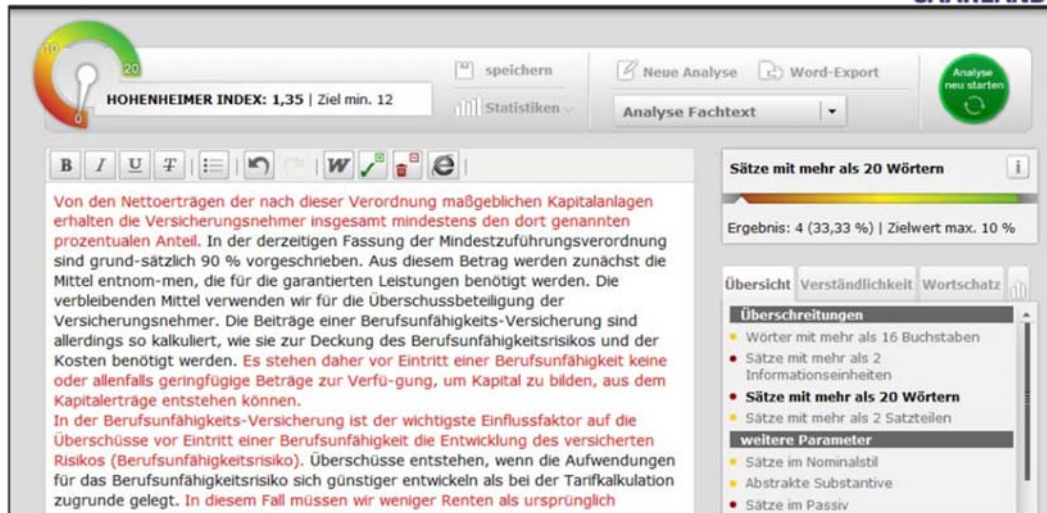


Abbildung 1: Maschinelle Textanalyse

<https://www.service-tested.de/wp-content/uploads/2016/04/Erklärung-Verfahren-TÜV-geprüfte-Verständlichkeit.pdf>

Multi-language?

Privacy & Usability - Data Protection Commissioner's Perspective

15

Example: "Datenschutz-Steckbrief"




- "data protection briefing"
- 2-page mini policy for giving information according to Art. 13 GDPR

Tätigkeitsbericht
2019 des ULD S-H,
Tz. 6.1.4:
<https://uldsh.de/tb37>


Privacy & Usability - Data Protection Commissioner's Perspective

16

Example: Transparency for "Bell Camera"




**Achtung
Klingelkamera**



Informationen zu Ihren Rechten erhalten Sie auf unserer Webseite:
www.datenschutzzentrum.de/datenschutzerklärung

Name und Kontaktdaten des Verantwortlichen:

ULD 

Unabhängiges Landeszentrum für Datenschutz
Holstenstraße 98
24103 Kiel
mail@datenschutzzentrum.de
0431/ 988 1200

Kontakt Daten des Datenschutzbeauftragten:

bdsb@datenschutzzentrum.de
0431/ 988 1280

Zweck und Rechtsgrundlage der Datenverarbeitung:

Einlasskontrolle im Rahmen der Wahrnehmung des Hausrechts gemäß § 14 Abs. 1 Nr. 2 Landesdatenschutzgesetz (LD SG)

Funktionsweise der Kamera und Gegensprechfunktion:

Erst beim Klingeln werden die Kamera und die Gegensprechfunktion kurzzeitig angeschaltet. Der Erfassungsbereich der Kamera ist dann auf den unmittelbaren Eingangsbereich beschränkt. Eine Speicherung der Daten erfolgt nicht. Ansonsten sind die Kamera und die Gegensprechfunktion ausgeschaltet.

Example: Transparency of a more complex scenario



Information about
embedded "Yellow dots"
in colour copies

Tätigkeitsbericht
2019 des ULD S-H,
Tz. 10.4:
<https://uldsh.de/tb37>

ULD (2019): Report „Vorsicht: Yellow Dots!
Versteckte Informationen in Farbkopien“,
<https://www.datenschutzzentrum.de/artikel/1274-Yellow-Dots.html>

Transparency Guidelines

Art. 29 Working Party, WP 260 rev.01

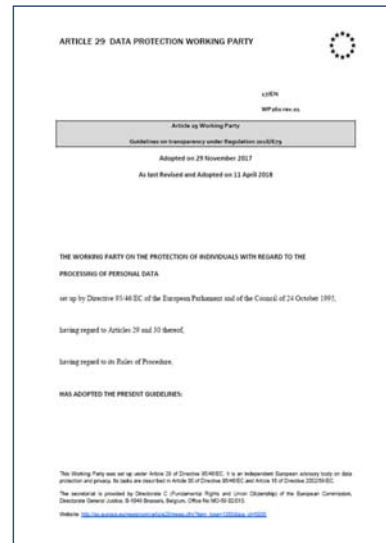
Poor Practice Examples

The following phrases are not sufficiently clear as to the purposes of processing:

- "We may use your personal data to develop new services" (as it is unclear what the "services" are or how the data will help develop them);
- "We may use your personal data for research purposes (as it is unclear what kind of "research" this refers to); and
- "We may use your personal data to offer personalised services" (as it is unclear what the "personalisation" entails).

Good Practice Examples¹⁴

- "We will retain your shopping history and use details of the products you have previously purchased to make suggestions to you for other products which we believe you will also be interested in" (it is clear that what types of data will be processed, that the data subject will be subject to targeted advertisements for products and that their data will be used to enable this);
- "We will retain and evaluate information on your recent visits to our website and how you move around different sections of our website for analytics purposes to understand how people use our website so that we can make it more intuitive" (it is clear what type of data will be processed and the type of analysis which the controller is going to undertake); and
- "We will keep a record of the articles on our website that you have clicked on and use that information to target advertising on this website to you that is relevant to your interests, which we have identified based on articles you have read" (it is clear what the personalisation entails and how the interests attributed to the data subject have been identified).



https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Overview



Source: stux via Pixabay

- Privacy & Usability going together
- Requirements from the GDPR
 - Principles
 - Information
 - Data Protection by Design and by Default
- Adverse effects
- Conclusion

Data Protection by Default

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.

"by default":
data protection-friendly
pre-settings as a
starting point for all
data processing!

Data Protection by Default vs. Usability

- Default setting always relevant – **depending on the purpose!**
- Changes are possible, but require intervention from user
- **Examples for (changeable) data protection defaults:**
 - Less storage of personal data (**necessity**)
 - Less storage outside the user's control
(e.g. no automatic phone number storage of an attempted call;
secure device instead of cloud – limited **accessibility**)
 - Less personalisation
(if no explicit purpose – limited **extent of processing**)
 - Earlier erasure of data (limited **storage period**)

Improved user
experience?

Support of people
with disabilities?

- **How strict?**

Temporary files?

Overview



Source: stux via Pixabay

- Privacy & Usability going together
- Requirements from the GDPR
 - Principles
 - Information
 - Data Protection by Design and by Default
- Adverse effects
- Conclusion

Presentation of information

from the perspective of the data controller

- Presentation of information is always ...
 - ... a challenge because of different target audiences
 - ... **incomplete**
 - ... **coloured**

- E.g. communication of a personal data breach to data subjects (Art. 34 GDPR):

"... shall describe **in clear and plain language** the nature of the personal data breach and contain at least the information and measures ..."

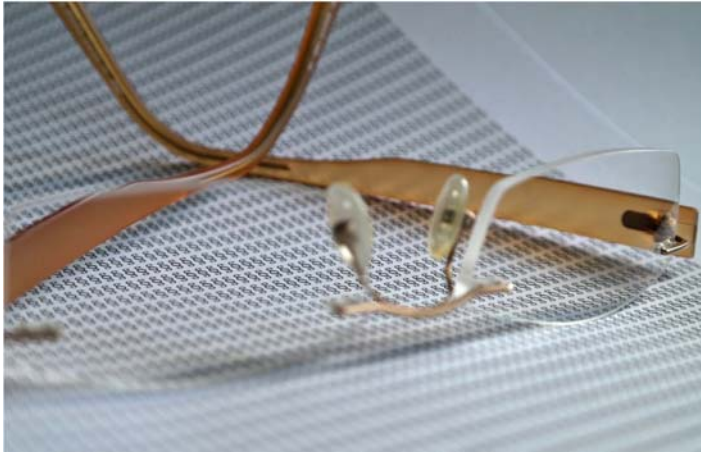


Source: Kerstin Riemer via Pixabay

How to inform about risks?

How to gain trust?

Better safe than sorry ... *from the perspective of the data controller*



Source: I_u_p_a via Pixabay

Data controllers want legal certainty, thereby relying on **legal standards** that for decades have been accepted before courts

Adverse design patterns

- **Greedy** apps and services
- Tricking users into disclosing more data (**various psychological tricks**):
 - "Profile completed" as status info
 - "We miss you" for contact reason
 - Loss Aversion
 - Illogical Reasoning
 - Perception of Scarcity, Fear of Missing Out ("you are missing ...")
 - ...

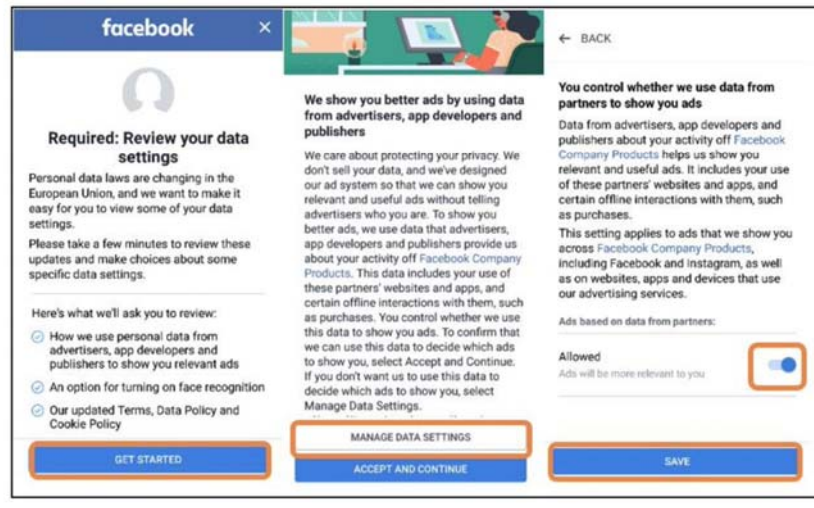
"Dark Patterns"!

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



Deceived by Design

As the screenshots below illustrate, the Facebook GDPR popup requires users to go into "Manage data settings" to turn off ads based on data from third parties. If the user simply clicks "Accept and continue", the setting is automatically turned on. This is not privacy by default.



<https://www.forbrukerradet.no/dark-patterns/> (2018)
- page 14

Privacy & Usability - Data Protection Commissioner's Perspective

27

Deceived by Design

	Facebook	Google	Windows	Chapter
No privacy intrusive default settings in popups	✗	✗	✓	4.1
Equal ease (number of clicks) for privacy friendly options in popups	✗	✗	✓	4.2
Design (colours and symbols) does not lead toward privacy intrusive option in popups	✗	✗	✗	4.2
Language does not lead toward privacy intrusive option in popups	✗	✗	✗	4.3
Privacy friendly options in popups come without "warnings"	✗	✗	✓	4.4
Users can clearly postpone the decision while accessing the service in the meantime	✗	✗	✗	4.5

<https://www.forbrukerradet.no/dark-patterns/> (2018)
- page 3

Privacy & Usability - Data Protection Commissioner's Perspective

28

Overview



Source: stux via Pixabay

- Privacy & Usability going together
- Requirements from the GDPR
 - Principles
 - Information
 - Data Protection by Design and by Default
- Adverse effects
- Conclusion

Conclusion



Source: congerdesign via Pixabay

- Usability is relevant; starting point "data protection by default"
- Data protection commissioners are not trained in usability issues → info needed
- Fines/sanctions for deficiencies caused by bad usability? → evidence needed
- Standing shoulder-to-shoulder with consumer protection
- GDPR as game changer?
 - Promise of a level playing field
 - We are not there, yet!