GDPR transparency requirements

Harald Zwingelberg, Eva Schlehahn, ULD

W3C Workshop on Privacy and Linked Data

'Data Privacy Controls and Vocabularies'

18/04/2018

SPECIAL

European Commission

Horizon 2020
European Union funding
for Research & Innovation

GDPR: Various sources that require transparency

Article	Title
5 para. 1 a)	Principles relating to processing of personal data
12	Transparent information, communication and modalities for the exercise of the rights of the data subject
13	Information to be provided where personal data are collected from the data subject
14	Information to be provided where personal data have not been obtained from the data subject
15	Right of access by the data subject
19	Notification obligation regarding rectification or erasure of personal data or restriction of processing
25	Data protection by design and by default
30	Records of processing activities
32	Security of processing
33	Notification of a personal data breach to the supervisory authority
34	Communication of a personal data breach to the data subject
40	Codes of conduct
42	Certification

Necessity of transparency from a data protection perspective

- Involved stakeholders need to have all relevant and sufficient information to understand the relevant steps of data processing, the decisions based on the results of the processing, as well as the related risks
  - Which data and to which extend?
  - In which way, using which means?
  - For which purposes and processed by whom?
  - Transfer to other parties and foreign countries?

- Necessary precondition to enable data subject's rights (e.g. access, rectification…)

- Crucial element of fair and lawful data processing

➢Scope: Data, systems, processes -> over the whole lifecycle of processing (collection to deletion)

High level examples how transparency can be supported

- Verification of data sources, keeping track of data
- Documentation of IT processes
- Logging of accesses & changes of the data stock
- Versioning of different prototypes/systems
- Documentation of testing
- Documentation of (related) contracts
- Documentation of consent (if applicable: given/refused/withdrawn)
- Consent management possible from a mobile
- Support of data subject‘s rights via technology, e.g. easy access, deletion, rectification

Data protection focus for technical specifications I

➢Categories of personal data

- Typical classes of data, e.g. master record data, location and movement data, call records, communication metadata, logfile data.
- E.g. special categories of personal according to Art. 9 GDPR
  - racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation

➢Support documentation of

- processing purpose(s) + legal ground
- consent exact wording (versioning) and current status, e.g.
  - given – if yes, specific whether explicit or implicit
  - pending / withheld
  - withdrawn
  - referring to the personal data of a minor
  - referring to the personal data of a disabled person in need of specific accessibility provisions to manage consent

Data protection focus for technical specifications II

- Support documentation of
  - Involved controller(s)
  - Involved processor(s)
  - Cross-border data transfers and involved countries
    - Data transfer within the European Union
    - Data transfer to a third country and basis for compliance with Art. 44 et seq. GDPR (adequacy decision, appropriate safeguards, binding corporate rules) and where possible a link documenting the latter, e.g. to the Commission's adequacy decision or the BCR.
    - Other third country

- Enforce rules how to handle the data, e.g.
  - User/access activity allowed, like read-only, write, rectify, disclose, deletion
  - Anonymize / pseudonymize / encrypt
  - Time for deletion [delete by…], [delete x month after <event>], etc.
  - Notify [define notification rules e.g. towards data subject, eventually with predefined action time]

- Availability of the data to inform of data subjects

For consent management: layered approach instead of text walls

First, top-layer should

- *'always contain information on the processing which has the most **impact on the data subject** and processing which could **surprise** the data subject.'**

Recommendation: Communicate at least

- processing purpose,
- data recipients and
- where/how more in-depth information can be found

Specification must support multi-layered aproach, e.g. foresee data fields for several layers of detail

*(Art. 29 WP260 p. 17; supported already by Art. 29 Working Party WP100, 2004)

Thank you / contact details

Authors of this presentation:

Harald Zwingelberg

Eva Schlehahn

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

(Independent Centre for Privacy Protection Schleswig-Holstein)

Holstenstr. 98

24103 Kiel

Germany

special@datenschutzzentrum.de

Technical/Scientific contact

Sabrina Kirrane

Vienna University of Economics and Business

sabrina.kirrane@wu.ac.at

Administrative contact

Jessica Michel

ERCIM W3C

jessica.michel@ercim.eu

Project partners and credits

Horizon 2020
European Union funding
for Research & Innovation

The project SPECIAL (Scalable Policy-awarE linked data arChitecture for prIvacy, trAnsparency and compLiance) has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731601 as part of the ICT-18-2016 topic Big data PPP: privacy-preserving big data technologies.