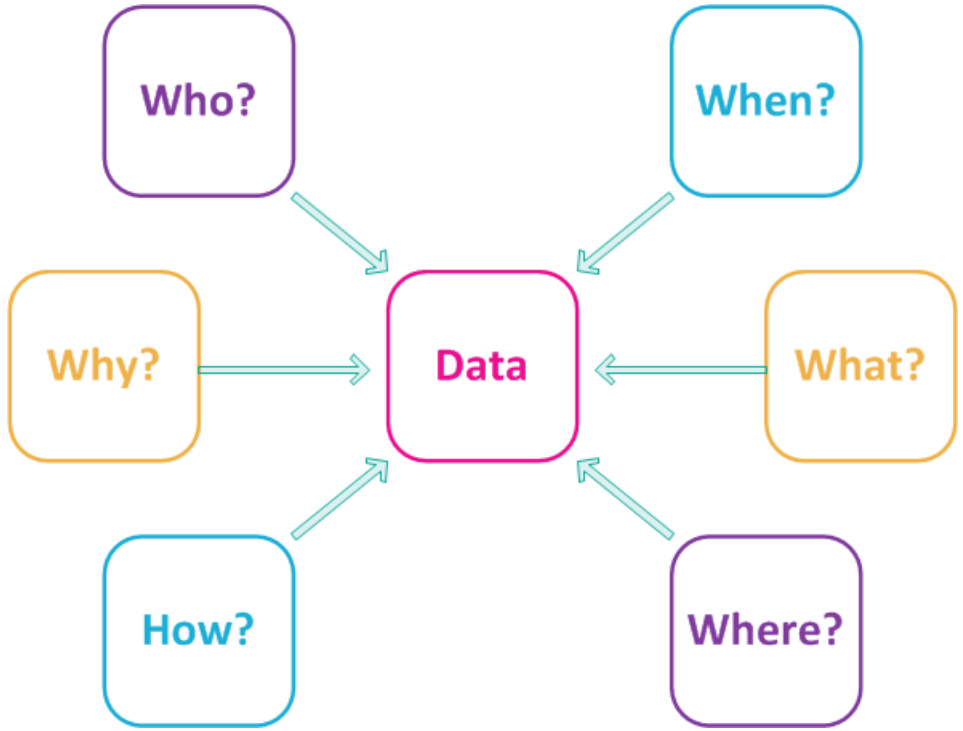
Data Privacy Vocabularies to fulfil GDPR Transparency & Compliance Checking requirements

SPECIAL

Author: Eva Schlehahn, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Germany

Necessity of transparency from European data protection law perspective

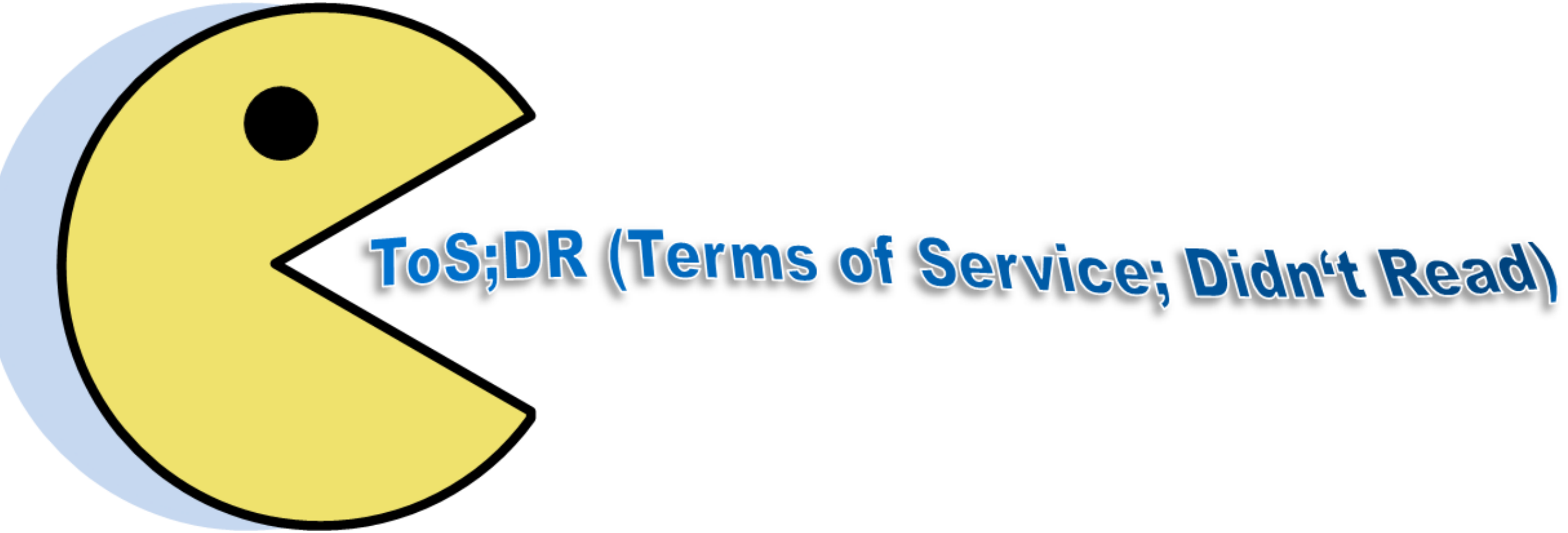


Necessary precondition to enable:

- Valid consent (Art 4 (11) GDPR),
- Data subject's rights (e. g. access, rectification…),
- Enforcement of data handling policies
- Demonstration of compliance

Scope: Data, systems, processes

Necessity of transparency from European data protection law perspective



Legal foundation of a technical approach for consent management and policy enforcement

GDPR:

- Art. 12 (1) GDPR:
  - The controller may **provide information by electronic means.**
- Art. 21 (5) GDPR:
  - When using information society services, the data subject may **exercise the right to object by automated means using technical specifications.'**
- Recital 32 GDPR:
  - Possibility of using **electronic means and technical settings** for information society services **for giving consent.**

Revelance of diverse case law, DPA decisions & upcoming ePrivacy Reg.

- Planet 49 CJEU judgment
  - Current cookie banners + tracking via opt-out NOT ok => consent needed
- Berlin DPA fine against Deutsche Wohnen (14,5m €, Oct 30th 2019)
  - GDPR infringement bc IT system did not foresee deletion concept & erasure function for data
- Current ePrivacy Regulation draft:
  - Requirements in flux, software settings for giving consent are now mentioned in Recital 20a -> might still change

Community building and standardisation effort:W3C Data Privacy Vocabularies and Controls Community Group (DPVCG)

https://www.w3.org/community/dpvcg/

Currently 58 participants:
Stakeholders from industry, research, government…

Goal: Development of a taxonomy of privacy terms, esp. with regard to GDPR. Examples are taxonomies of:

- personal data categories,
- different data processing purposes,
- events of disclosures,
- consent status/modalities
- types of processing operations.

Community building and standardisation effort:W3C Data Privacy Vocabularies and Controls Community Group (DPVCG)

https://www.w3.org/community/dpvcg/

W3C Community Group Draft Report

Data Privacy Vocabulary v0.1

Draft Community Group Report 26 July 2019

Latest editor's draft:

https://w3.org/ns/dpv

Editors:

Harshvardhan J. Pandit (Trinity College Dublin)

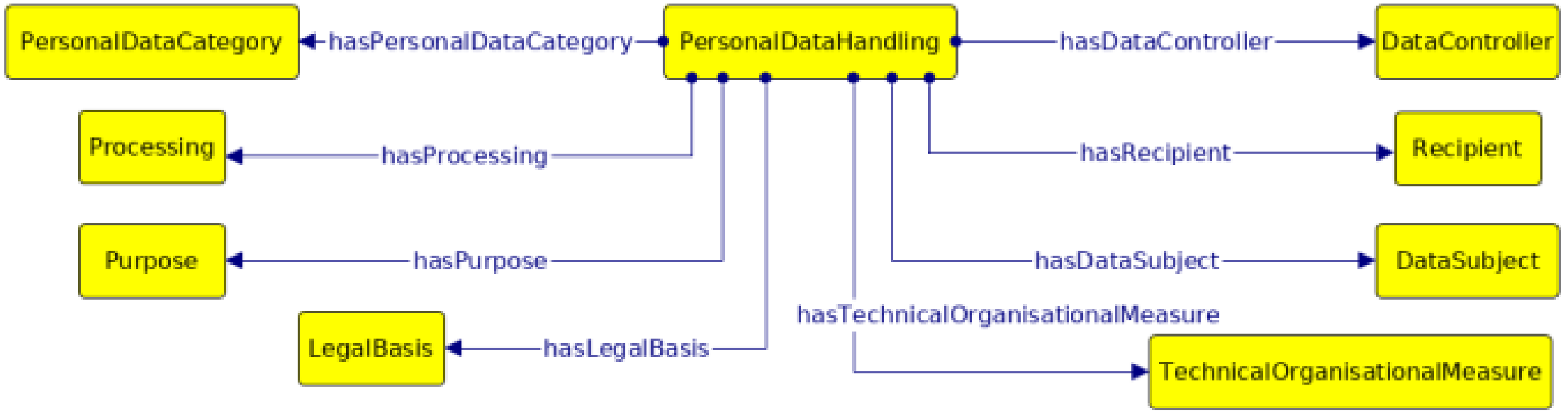
Axel Polleres (Vienna University of Economics and Business)

Authors:

cases related to making personal data processing interoperable by respective standards in order to ease proof of compliance with the GDPR and related privacy

group have signed the W3C Community Co Agreement.

Data protection focus for technical specifications I: Policies entailing the necessary information



Data protection focus for technical specifications II

- **Categories of personal data**
  - E. g. master record data, location and movement data, call records, communication metadata, log file 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 (evtl. incl. 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
    - etc…

Data protection focus for technical specifications III

- **Support documentation** of
  - Involved controller(s)
  - Involved processor(s)
  - Storage location and cross-border data transfers, involved countries
    - Location of data centre where processing & storage occurs
    - Location of controller establishment
    - Relevant could be:
      - Data transfer within the European Union
      - Data transfer to a third country with basis for compliance acc. to Art. 44 et seq. GDPR (treating them as 'EULike', i. e. adequacy decision, appropriate safeguards, binding corporate rules), where possible with link documenting the latter, e. g. to the Commission's adequacy decision or the BCR
      - Other third country
- Suggestion: Use country codes (e.g. TLD, ISO 3166) - allows for later adaption in case of legal changes
- Suggestion: Incorporate also rules that exclude data transfers to some jurisdictions ('notUS', 'notUK')

Data protection focus for technical specifications IV

- **Enforce rules how to handle the data**, e. g.
  - User/access activity allowed, like read-only, write, rectify, disclose, deletion
  - Anonymize / pseudonymize / encrypt
  - Notify [define notification rules e. g. towards data subject, eventually with predefined action time]
  - Time for deletion – ideas could be:
    - delete-by_ or delete-x-date_month_after <event>
    - no-retention (no storage beyond using once)
    - stated purpose (until purpose has been fulfilled)
    - legal-requirement (storage period defined by a law requiring it)
    - business practices (requires a deletion concept of controller)
    - Indefinitely (e. g. for really anonymized data, public archives…)

More info and funding notice

Project website: **https://www.specialprivacy.eu/**

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.

Thank you / contact details

SPECIAL project website: **https://www.specialprivacy.eu/**

Author of this presentation: Eva Schlehahn

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD, Independent Centre for Privacy Protection Schleswig-Holstein)

Email: uld67@datenschutzzentrum.de

Twitter: @eschlehahn

SPECIAL project technical/scientific contact: Sabrina Kirrane

Vienna University of Economics and Business

Email: sabrina.kirrane@wu.ac.at

SPECIAL project administrative contact: Jessica Michel

ERCIM / W3C

Email: jessica.michel@ercim.eu

RECAP & WRAP UP

Data Privacy Vocabularies to fulfil GDPR Transparency & Compliance Checking requirements

Issues discussed

- For showing GDPR compliance, what's the most important IT system feature needed?
- Who would benefit the most from a data privacy vocabulary/ontology/taxonomy?
- What should such a data privacy vocabulary, i.e taxonomy cover?

- **How SPECIAL addressed these issues + how YOU can use these results:**
  - Deliverables, prototypes, ontologies & vocabularies, code repository, platform demonstrators, UI demos ALL Open Access: **https://www.specialprivacy.eu/**
  - Everyone can engage in the W3C DPCG: **https://www.w3.org/community/dpvcg/**