

DPVCG – status update

W3C[®]



COMMUNITY & BUSINESS GROUPS

[Home](#) / Data Privacy Vocabularies...

**DATA PRIVACY VOCABULARIES AND CONTROLS
COMMUNITY GROUP**

Timeline

- Launch 25/5/2018
- Presentation at MyData 2018 – 31-August-2018
- Last milestone: F2F in **3+4-DEC-2018** in Vienna
- 14 Telcos since, next one planned 12-FEB-2019
- The current goal is to agree on first public drafts of minimal sets of vocabularies to be finished by December 2018, with first stable working drafts being reached latest on **25 May 2019**.

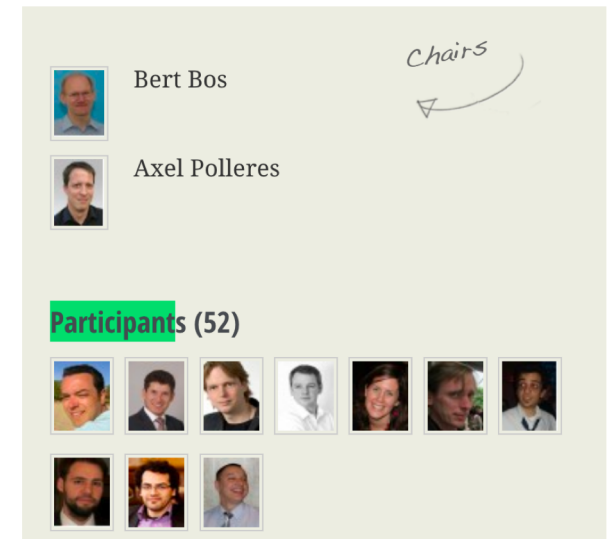
Suggestion: revisit
at next Plenary?

- → probably good to have another milestone (another F2F, March? April?)
- → SPECIAL deliverable **D6.5** Final report of the Community Group **[M30/M36]?**

Participation and Stakeholders:

52 participants

- Plan ahead: plan another F2F
 - Align with SPECIAL vocabs and Policy Language
- Align with active stakeholders:
 - Consent Receipt Specification (Kantara) - Mark Lizar
 - GDPRText (Trinity College Dublin) - Harshvardhan J. Pandit
 - DECODE project – Stefano Bozzoni
 - Project CitySPIN & Project Expedite (TU Vienna, WU) - Fajar Ekaputra, Elmar Kiesling, Javier)
 - Pret-a-LLOD.eu/MyData (INSIGHT) - Alexandros Nousias (**new**)
 - **ISSUE:** still (beyond our consortium) no significant industry involvement
 - E.g. what happened on the [“W3C Permissions and User Consent”](#) Workshop?
- Align with our internal use cases:
 - **DT, PROX** – agreed to have something complete by end of march, more general applications in the **telco sector**?
 - **TR** – more general applications in the **financial sector**?



Status DPVCG vocabularies:

Most actively discussed:

- [Personal Data Categories](#)
 - Needs structuring
- [Purposes](#)
- [Processing](#)
 - Needs structuring
 - Similar issue/question: Data Storage Location /Duration – Are these actually underneath processing?
 - storage (ISO/EU country codes), and security (ISO standards)

https://www.w3.org/community/dpvcg/wiki/Taxonomy#Hierarchical_Taxonomies

Hierarchical Taxonomies [\[edit\]](#)

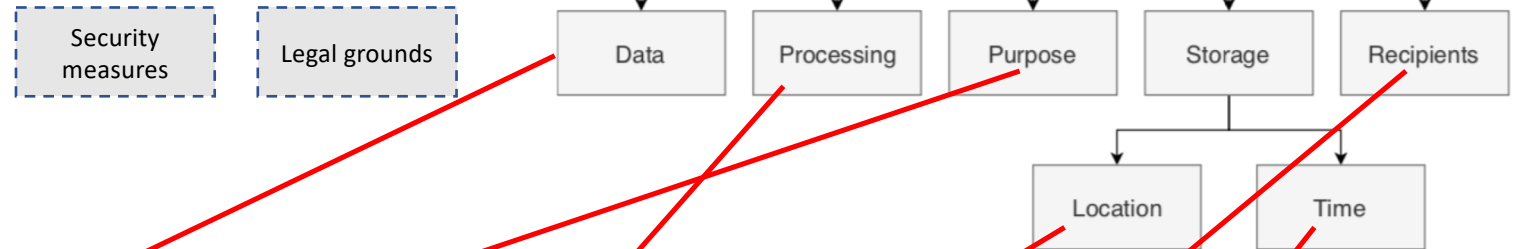
Approved (in-scope) [\[edit\]](#)

- [Categories of Personal Data](#) (approved call [2018-09-18](#))
- [Purposes for handling Personal Data](#) (approved call [2018-09-18](#))
- [Categories of Data Processing](#) (approved call [2018-09-18](#))
- [Categories of Data Controllers, Data Processors, Recipients](#) (approved call [2018-09-18](#))
- [Data Storage Locations](#) (approved call [2018-09-18](#))
- [Security Measures](#) (approved in call [2018-09-18](#))
- [Data Storage Duration](#) (approved call [2018-09-18](#))

Proposed [\[edit\]](#)

- [Consent Actions](#) (to be agreed - proposed in call [2018-09-18](#))
- [Consent Collection Medium](#) (to be proposed)
- [Categories of Agents / Data Subjects / Entities](#) (to be proposed)
- [Rights](#) (to be discussed further, based on the overview by Eva: <https://lists.w3.org/Archives/>)
- [Principles](#) (to be proposed)
- [Obligations](#) (to be proposed)
- [Legal Basis](#) (to be proposed)
- [Compliance Related Terms](#) (to be proposed)
- [Consent States](#) (to be proposed)

How to connect the dots?



- Which metadata (properties do we need to connect them)?
- Legal Personal data handling:
 - A personal Data Category is undergoing specified processing by a specific **data controller** and/or transferred to some **recipient** for a particular purpose, based on a specific legal ground, with (optionally?) specified **security measures and restrictions** (e.g. **storage locations** and **storage durations**).

operating in a certain core business sector or sets of business activity/sector

Some questions here:

- **Restrictions** may be implicitly tied to the Legal ground?
- Consent is given to specified data handling (see above), by a specified **consent action**?
- Personal data Categories may be subdivided into **sensitive** data categories
- How to specify derivations of additional data categories? Does it (legally) need to be specified?

May be restricted to a certain business activity/sector, e.g. marketing/personalization of education services

Personal Data Categories

1. [Categories of Personal Information by Enterprivacy Consulting Group](#)
2. From use cases:
 - https://www.w3.org/community/dpvcg/wiki/Categories_of_Personal_Data
3. SPECIAL personal data categories:
 - https://www.specialprivacy.eu/images/documents/SPECIAL_D2.5_M21_V1.0.pdf
4. Special data categories according to GDPR (article 9, article 4)
 - PROPOSED: use 1. as an anchor and map the other three onto it, reach out to <https://enterprivacy.com> or the underlying academic paper.
 - Have started an OWL ontology for this:
 - <https://github.com/dpvcg/personal-data>
 - <https://webprotege.stanford.edu/#projects/4658d8e1-588e-4847-90c1-6118eabac007/edit/Classes>
 - Timeplan/Responsibles: Harsh, Fajar within a month.



Purposes

- Purposes outcomes of Dec 10 meeting (second half of the page)
- NAICS/NACE/ISIC codes? ([Harsh's notes](#))
- Combination of both: e.g. *Delivery* of Products in a specific business sector, mix of actions and sector.
- Question: isn't sector rather some restriction on the data controller/location/duration? (cf. slide "How to connect the dots?")
- Timeplan/Responsibles: Axel, Javier

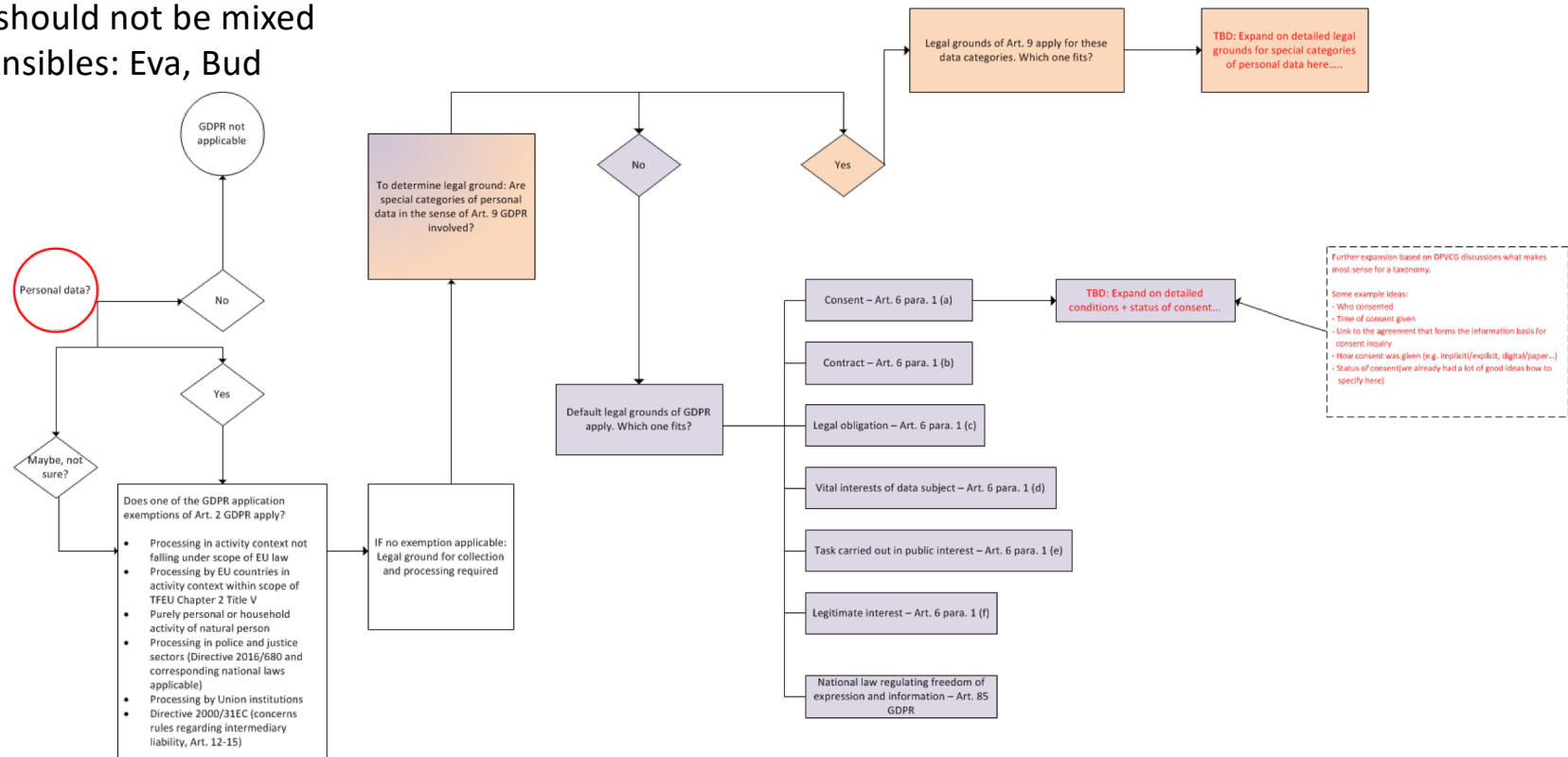
Legal Grounds:

Legal Grounds

ISSUE-7: Are the legal grounds except consent and legitimate interest actually purposes?

Rather no, should not be mixed

Timeplan/Responsibles: Eva, Bud



Processing

- Open - [https://www.w3.org/community/dpvcg/wiki/Categories of Data Processing](https://www.w3.org/community/dpvcg/wiki/Categories_of_Data_Processing)
- Needs volunteers to work!

Data Controllers / Recipients



- Main business activitie(s)/sector
- Country of operation / country of legislation?

- SPECIAL: thinking of different policies (policy **restrictions**) to 3rd party **recipients**

- Needs volunteers to work!

Storage location/duration



- regions, country codes,
 - EU,
 - EU-like, EU-jurisdiction countries
 - → there is a fixed reference list with **time**,
- Duration:
 - Start, end, interval, explicit expiry date, event-based (2months after account closed), “as long as needed” (might be connected to legal grounds, e.g. keeping exam records)
- Other restrictions:
 - Regularity of processing/collection
- SPECIAL: has some starting points, no “event-based” yet.

Security measures/restrictions



- E.g. Linking to ISO standards followed and certifications.
- Do we have a list?
 - https://www.w3.org/community/dpvcg/wiki/Security_Measures
 - <https://coolharsh55.github.io/dpvcg-info/Security.html>

Discussion and Input welcome 😊

Notes from the discussion:

- Outcome of W3C user consent and permissions not yet clear (device/web app permissions?)
- Industry involvement hopefully when we have something to show from the group
- February 27 meetup with ne projects in Brussels – Rigo might go, we should advertise the group to them
- We should prioritise for now to get something stabilized, rather than expand the group
- Javier and me should work with Piero
- Piero thinks we should not conflate **legal ground** and **purpose**
- **Personal Data categories:**
- ***E.g. demographic, location at a certain granularity*** – shall we just distinguish for every category whether it is collected in a anonymous or personally identifiable manner, e.g. location at a certain granularity.