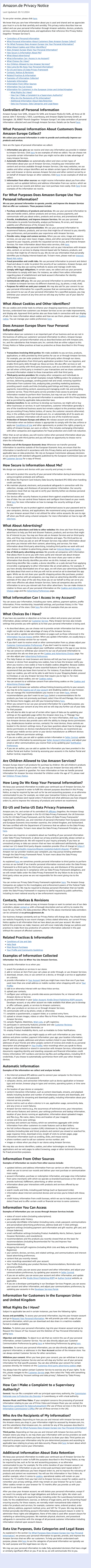
PriPoCoG[1]: Empowering End-Users' Data Protection Decisions

UNIVERSITÄT DUISBURG ESSEN

Open-Minded

Issue

lengthy textual privacy policies:



Amazon.de Privacy Notice

[1]

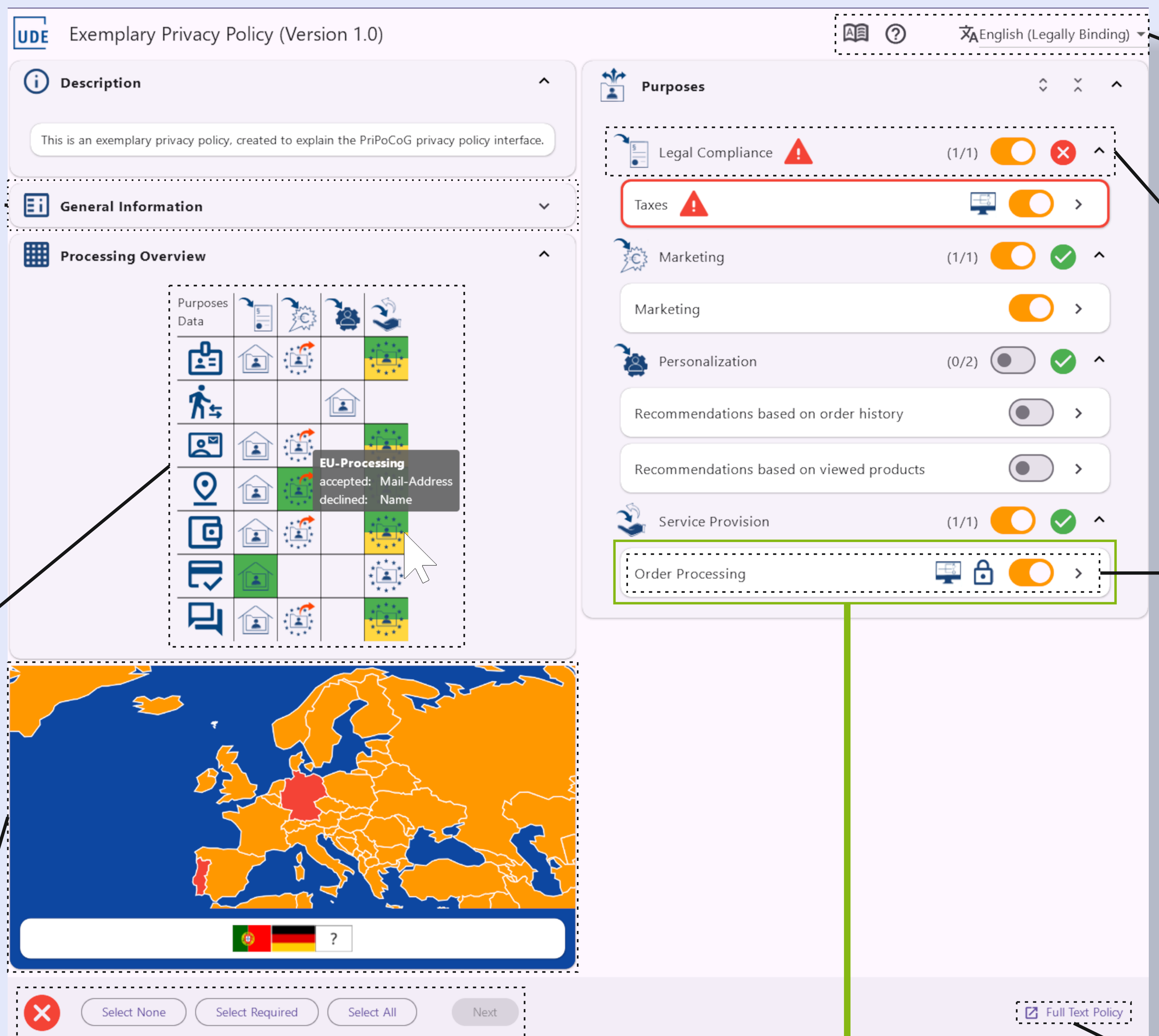
Customizable Privacy Policies in new Privacy Policy Interface

Basic Information (required by GDPR):
- Data Controller
- Data Protection Officer
- Data Subject Rights:
  - Access
  - Rectification
  - Restriction
  - Objection
  - Human Intervention
  - Portability
  - Erasure
- Supervisory Authority

Compact Processing Overview:
- Which data for which purpose: e.g., Behavioral Data is processed for Personalization
- **columns** = purpose categories: e.g., Legal Compliance
- **rows** = data categories: e.g., Identifying
- **cells** = processing locations: e.g., Internally or Outside of EU
- **colors** = acceptance status: e.g., purpose completely accepted 🟩
- **mouse-over** = additional information

World Map:
- visualizes destinations of data transfers (cf. *Data Recipients* in *Purpose Details*)
- destinations highlighted in red
- other countries gray
- no specific country is provided:
  - map turns orange
  - question mark as flag
- flags of destinations listed below map
- zoomable & navigable

Main Controls:
- status of policy: ✓ compatible
  ✗ incompatible
- quick menu
- similar to cookie-banners



Exemplary Privacy Policy (Version 1.0)

English (Legally Binding)

Description

This is an exemplary privacy policy, created to explain the PriPoCoG privacy policy interface.

General Information

Processing Overview

Purposes

- Legal Compliance (1/1)
  - Taxes
- Marketing (1/1)
  - Marketing
- Personalization (0/2)
  - Recommendations based on order history
  - Recommendations based on viewed products
- Service Provision (1/1)
  - Order Processing

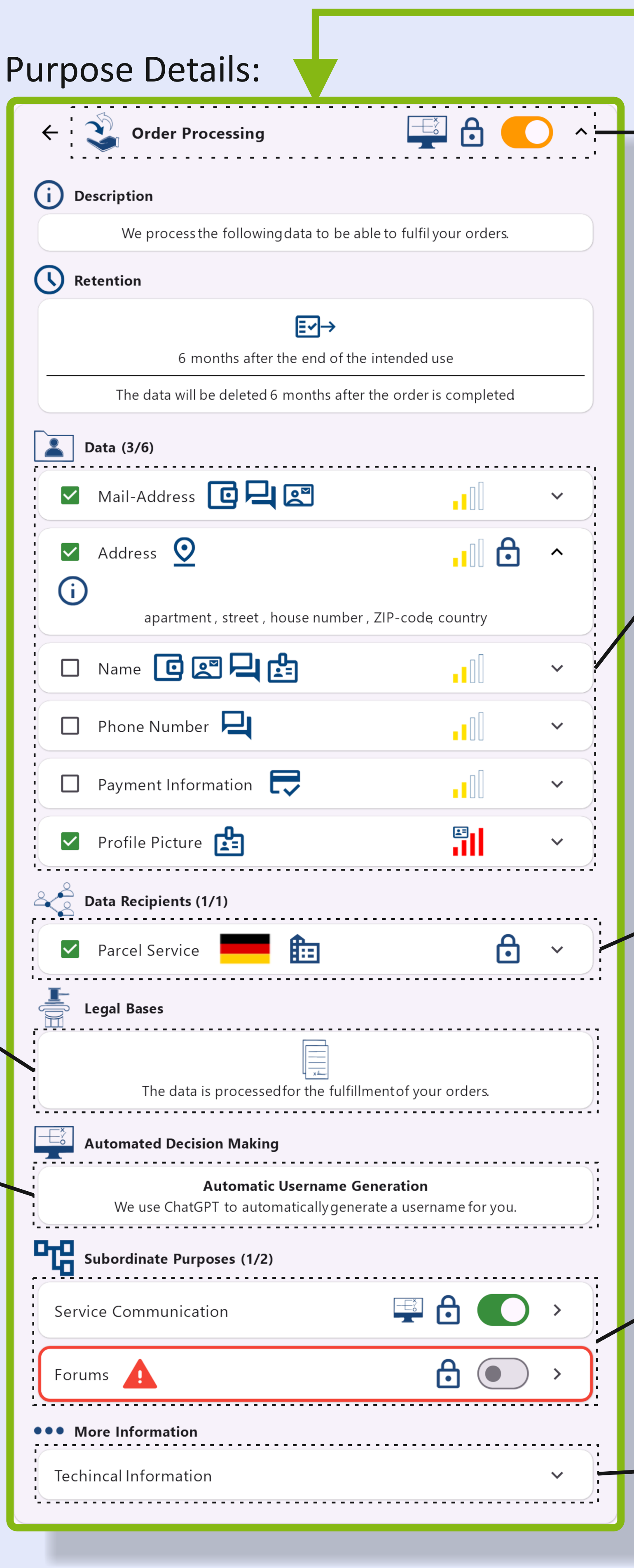
- glossary
- help
- language selection
  one policy file, many languages

Purpose Categories:
- icon
- name: *Legal Compliance*
- compatibility issue detected
- number of purposes
- switch (partially accepted)
- compatibility status of category: ✗ incompatible

Purpose *"Order Processing"*:
- automated decision-making
- required for policy compatibility
- switch (partially accepted)

link to textual privacy policy (required as long as EU has no standardized policy UI)

Purpose Details:



Order Processing

Description

We process the following data to be able to fulfil your orders.

Retention

6 months after the end of the intended use

The data will be deleted 6 months after the order is completed

Data (3/6)

- ☑ Mail-Address
- ☑ Address
  apartment , street , house number , ZIP-code, country
- □ Name
- □ Phone Number
- □ Payment Information
- ☑ Profile Picture

Data Recipients (1/1)

- ☑ Parcel Service

Legal Bases

The data is processed for the fulfillment of your orders.

Automated Decision Making

Automatic Username Generation
We use ChatGPT to automatically generate a username for you.

Subordinate Purposes (1/2)

- Service Communication
- Forums

More Information

- Techincal Information

List of Data:
- collected and processed for the current purpose *Order Processing*
- customizable via checkbox
- icons for data categories, e.g.:
  - Identifying
  - Communication
- severity indicator (How sensitive is this datum?)
- required for policy compatibility
- expandable for more information

List of Data Recipients:
- external data processors
- empty for internal-only purposes
- customizable via checkbox
- country flag of data recipient
- type of entity:
  - person
  - **legal entity**
  - public authority
- required for policy compatibility
- expandable for more information

Legal Bases of the Purpose:
- consent
- **contract**
- legal obligation
- legitimate interest
- public task
- vital interest

Explains how automated decision-making is used, when it is used.

Subordinate Purposes:
- purpose can be arranged hierarchically
- customizable using switches
- clicking opens *Purpose Details* of selected purpose

Additional Technical Information:
- what privacy models are applied to data (e.g., k-anonymity)
- how is data pseudonymized

TRY THE DEMO YOURSELF

(not optimized for mobile)

Methodology

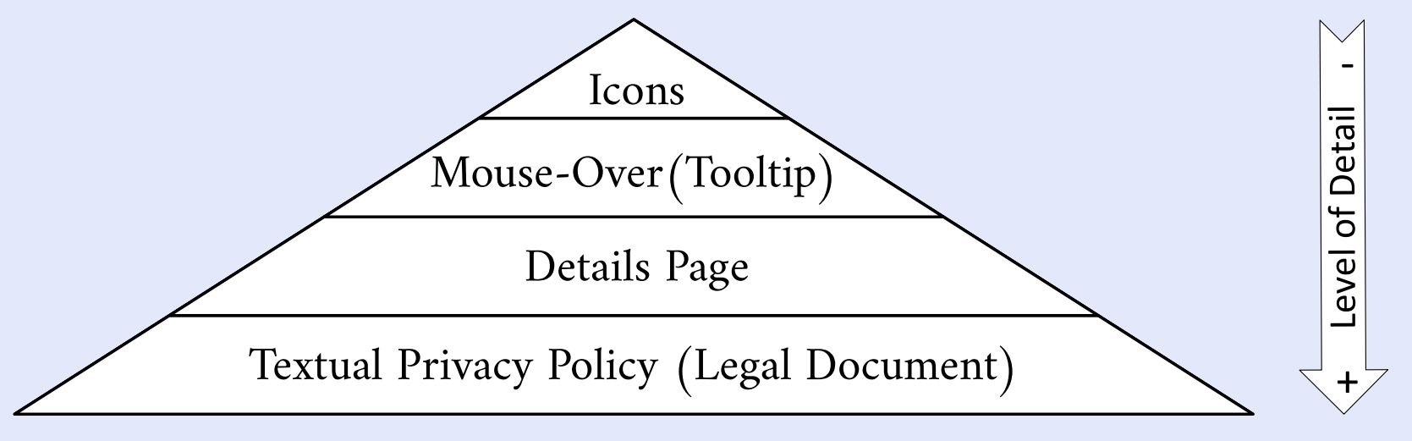
Literature Review:
- searched for:
  - policy interfaces
  - representations
  - customizable privacy policies
- 165 papers reviewed
- indentifying valuable concepts

Group Interview:
- 15 participants
- 30 minutes
- 6 guiding questions
- open discussion

⟹ 10 requirements + diverse concepts

Summary

Contribution:
- literature review
- group interview
- 4 levels of detail
- processing overview
- map for data transfers
- extension of DaPIS icon set [2]
- 15 concepts in total
- prototypical implementation



different levels of detail target different levels of interest in privacy protection:
- Pragmatists: quick decision using icons in *Processing Overview*
- Enthusiasts/Experts: scroll through details pages of purposes

Benefits:
- more details (e.g., mapping data to purposes)
- less legalese
- quick processing overview
- privacy enthusiast can go into detail
- varying levels of detail

Limitations:
- acceptance by policy authors
- lacking standardization by EU
- not *yet* thoroughly evaluated

Authors:

Jens Leicht - jens.leicht@uni-due.de
Julien Lukasewycz - julien.lukasewycz@uni-due.de
Maritta Heisel - maritta.heisel@uni-due.de

paluno - The Ruhr Institute for Software Technology
University of Duisburg-Essen, Duisburg, Germany

[1] **Pri**vacy **Po**licy **Co**mpliance **G**uidance framework (PriPoCoG)

References:

[1] Amazon Europe Core; *Amazon.de Privacy Policy*; Web Page; (Accessed: 2025-03-13); 2025. https://www.amazon.de/gp/help/customer/display.html?nodeId=201909010&language=en_GB

[2] Arianna Rossi, Monica Palmirani, and Chiara Cavazzuti; *Data Protection Icon Set (DaPIS) v.3.0*; Web Page; (Accessed: 2025-03-04); 2021; DOI: doi.org/10.5281/zenodo.7182819; https://zenodo.org/records/7182819

Artifacts:

prototypical implementation: https://github.com/jensLeicht/PrivacyPolicyInterface
extended DaPIS icon set: https://github.com/jensLeicht/DaPIS

UDE

PALUNO The Ruhr Institute for Software Technology