Exercise 04:
Privacy Policies, Privacy Languages

Privacy-Preservation Technologies in Information Systems

Dr. Wiem Fekih Hassen / Dr. Armin Gerl / Felix Bölz

WS 21/22

Task 1:
Privacy Policies

Privacy-Preservation Technologies in Information Systems

Dr. Wiem Fekih Hassen / Dr. Armin Gerl / Felix Bölz

WS 21/22

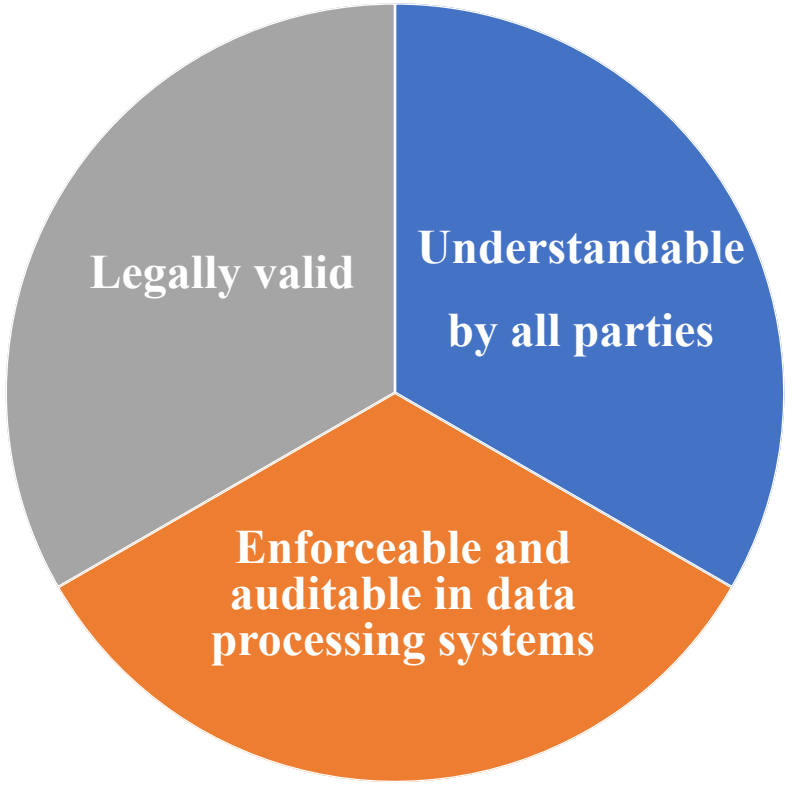
Privacy Policies

A **Privacy Policy is a legal document** between the User (Data Subject) and Service Provider (Controller) on how to :

- Collect the personal data
- Use the personal data
- Disclose the personal data

Privacy Policies Requirements

- GDPR requirements (Art. 13)
- Compliance to national legal frameworks



- GDPR Transparency requirements (Art. 12)
- Natural Language <-> Legal Expert Language
- Visual Aids (Privacy Icons)
- Consent and Control UIs
- Inclusion (Elderly, Children, etc. …)

- (Automatically) Enforce rules/consent of Privacy Policy
- (Automatically) Detect violation of Privacy Policy

→ Machine-readable Privacy Policies -> Privacy Languages

Source: Victor Morel, Raúl Pardo. SoK: Three Facets of Privacy Policies. *Workshop on Privacy in the Electronic Society*, Nov 2020, Virtual, France. ⟨hal-02267641v4⟩

Sets of Privacy Policies

Problem

- Controllers (organisation) offering services (or products) to users (data subject) have various policies regarding privacy.
- These typically exist within one document catering to legal evaluation, and thus one which is quite long and complex.
- Users are often encouraged to read such a policy, though as users are exposed to many of these, they mostly do not.
- As a countermeasure to this, controllers **partition their policies**, provide simplified versions, or bring relevant aspects to user attention when needed.

→ The use of privacy **icons**.

→ A privacy icon is worth a thousand-word policy.

Privacy Icons Problems

Problem

Privacy icons are easily **misunderstood**, as they are **oversimplified** concepts using **imagery** shared with numerous other concepts.

Solution

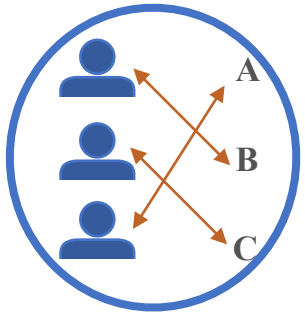
- A **consistent** set of icons, carefully grouped and not excessive, and the meaning should be explained.
- **Explanations** should be short and concise, and these paired with the icons should be put through user tests.
- Users (data subject) should be **able to understand** the icons when shown them in context.

Requirements when selecting appropriate icons

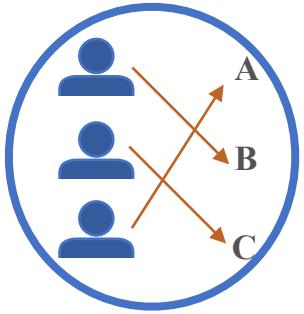
- Prevent misunderstanding.
- Use icons users are familiar with.
- Do not reassign meaning to familiar icons.
- Keep icon style and design consistent.

Pseudonymization and Anonymization Icons

Pseudonymization Icon



Anonymization Icon



Main Difference

Reversibility (Re-identification)

Source: https://cdn.netzpolitik.org/wp-upload/data-privacy-icons-v01.pdf

Task 2:
Privacy Statement of the University of Passau

Privacy-Preservation Technologies in Information Systems

Dr. Wiem Fekih Hassen / Dr. Armin Gerl / Felix Bölz

WS 21/22

Privacy Statement (s)

Many Privacy Statements

- Website of the University of Passau
- Multiple statements for StudIP
- HisQuis
- For new students
- etc.

→ Privacy statements are necessary for each **Managed Service**.

Student Personal Data

- Name
- Date of birth
- Adresse
- Email Adresse
- Phone number
- Student ID
- Nationality
- Previous institutes
- Degrees
- Grades
- Exams

Exams Review & GDPR

The student has the right to access to all of his/her personal data.

→ Exams are personal data.

Task 3:
Privacy Languages

Privacy-Preservation Technologies in Information Systems

Dr. Wiem Fekih Hassen / Dr. Armin Gerl / Felix Bölz

WS 21/22

Privacy Policy, Access Control, Privacy Preferences

Differences

- Privacy Policy languages are applicable for any domain.
- Access Control languages and Privacy Preferences languages are domain specific languages.
  - Access Control languages define Access Control rules on data and on documents.
  - Privacy Preferences languages define more less high requirements.

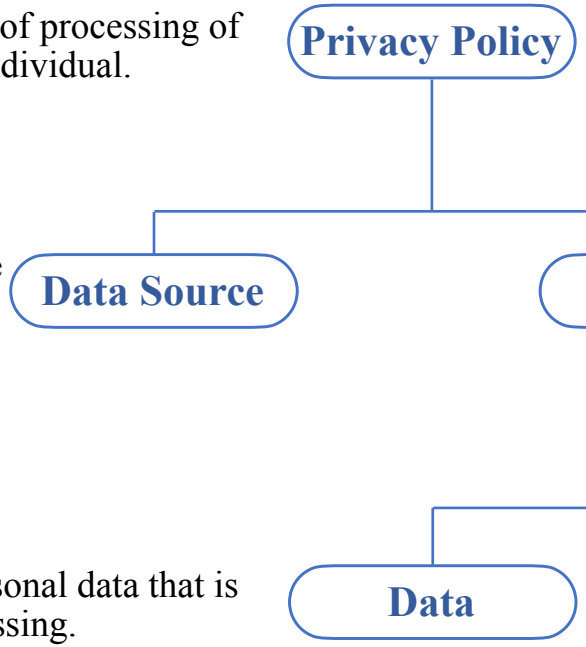
Privacy Policy, Access Control, Privacy Preferences

Similarities

- Access Control Language and Privacy Preferences Language are part of Privacy Policy Language

Privacy Policy Structure

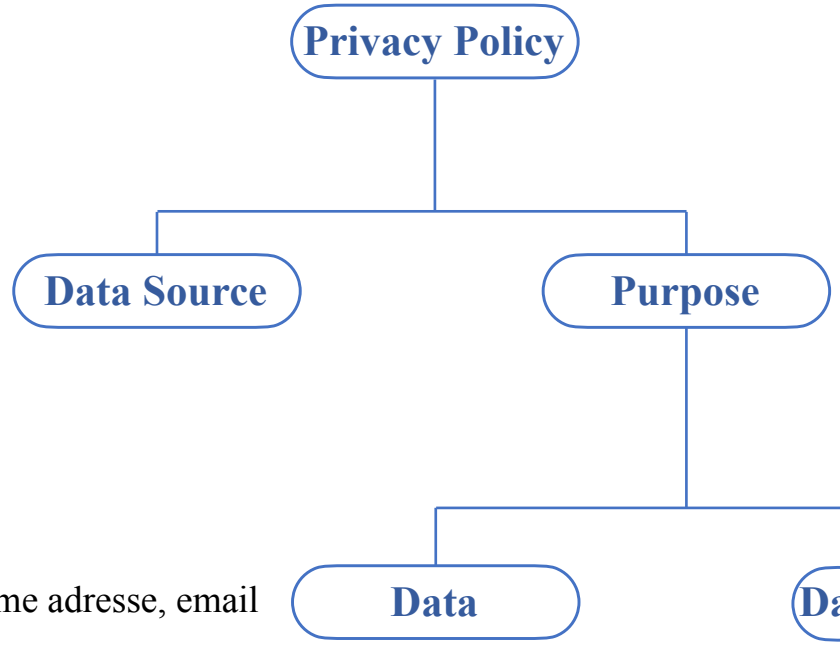
- Denotes all purposes of processing of personal data of an individual.



- The individual from which the personal data originates.
- Denotes the reason and extent of the processing of personal data.
- Denotes the personal data that is subject to processing.
- The entity which processes the personal data.

Example of Privacy Policy Language

Privacy Policy for E-commerce Store



- Personal information, e.g, name adresse, email adresse, phone number, etc.
- Credit and Financial Information, e.g, credit card, banking information.
- Network and device information, e.g, user device, WiFi usage.

- Administer the user account.
- Provide the user with access to particular tools and services.
- Obtain the user feedback on our sites and offerings.

- Third party services, e.g. Payment process

Limitations of Privacy Policy Language

- Data transfer between Companies
- Different meaning of, e.g., Purposes, Data etc.
  - Purpose: “Recommendation Service” in Online Shop does not equal the same on Dating Services
  - Data: “Name” in System A does not equal “Name” in System
- Semantics of privacy/privacy policies have to be defined!
- Privacy Language has to reference same semantic vocabulary!

See you next week ☺