Layered Privacy Language (LPL)
An Overview

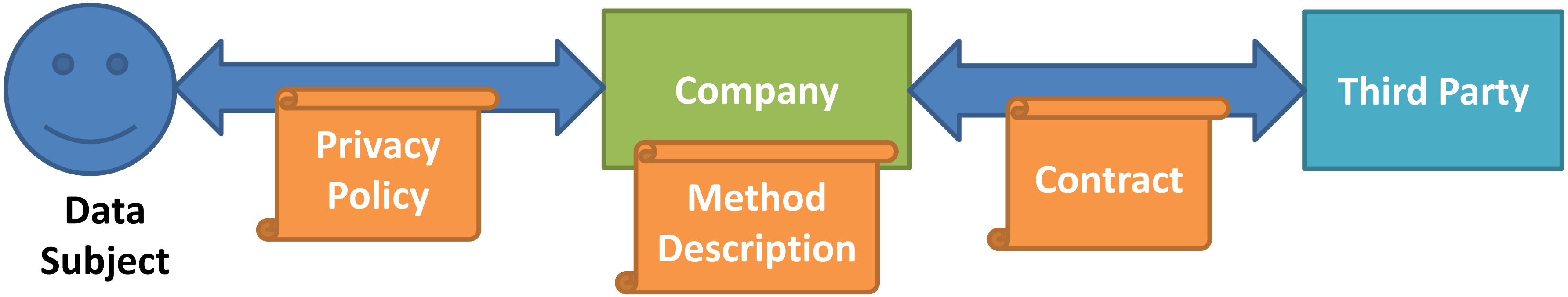
Motivation

General Data Protection Regulation (GDPR)

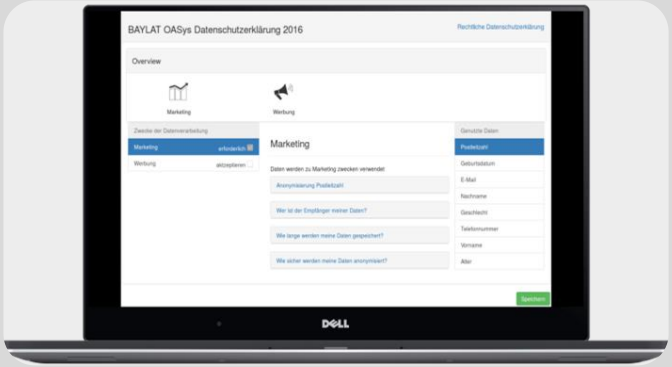
- Privacy by Design and Privacy by Default
- Consent and Data Subject Rights
- Severe Penalties (4% of turnover)
- And much more things to consider…

The Problem

- **Everything is paperwork!**
- Which Privacy Policy applies?
- Who has access?
- What can be accessed?



LPL – Systematic Integration



BAYLAT OASys Datenschutzerklärung 2016

Marketing

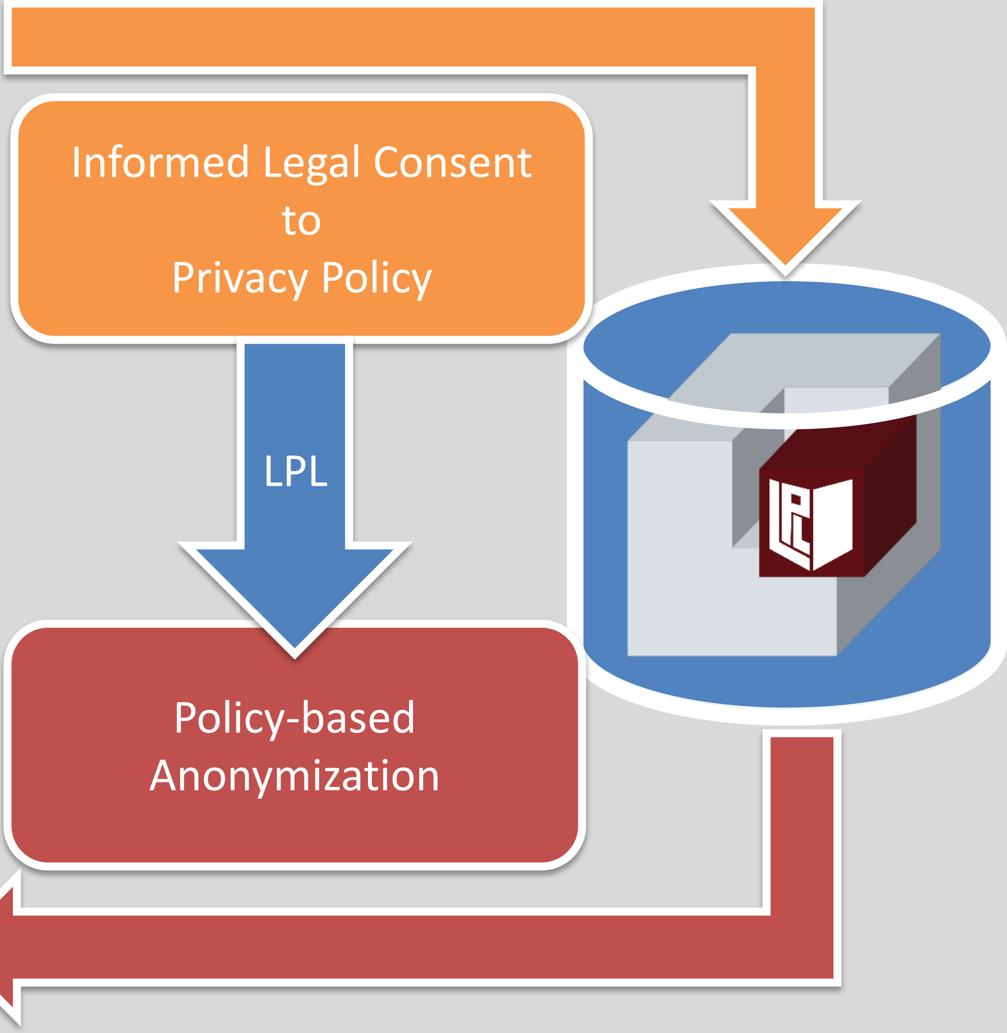
Daten werden zu Marketing zwecken verwendet

Anonymisierung Postleitzahl

Wer ist der Empfänger meiner Daten?

Wie lange werden meine Daten gespeichert?

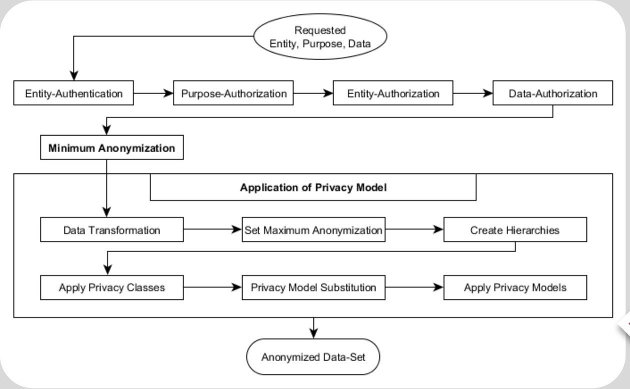
Wie sicher werden meine Daten anonymisiert?



Informed Legal Consent to Privacy Policy

LPL

Policy-based Anonymization



Layered Privacy Language (LPL)

On May 25 2018 the **General Data Protection Regulation (GDPR)** will be enforced

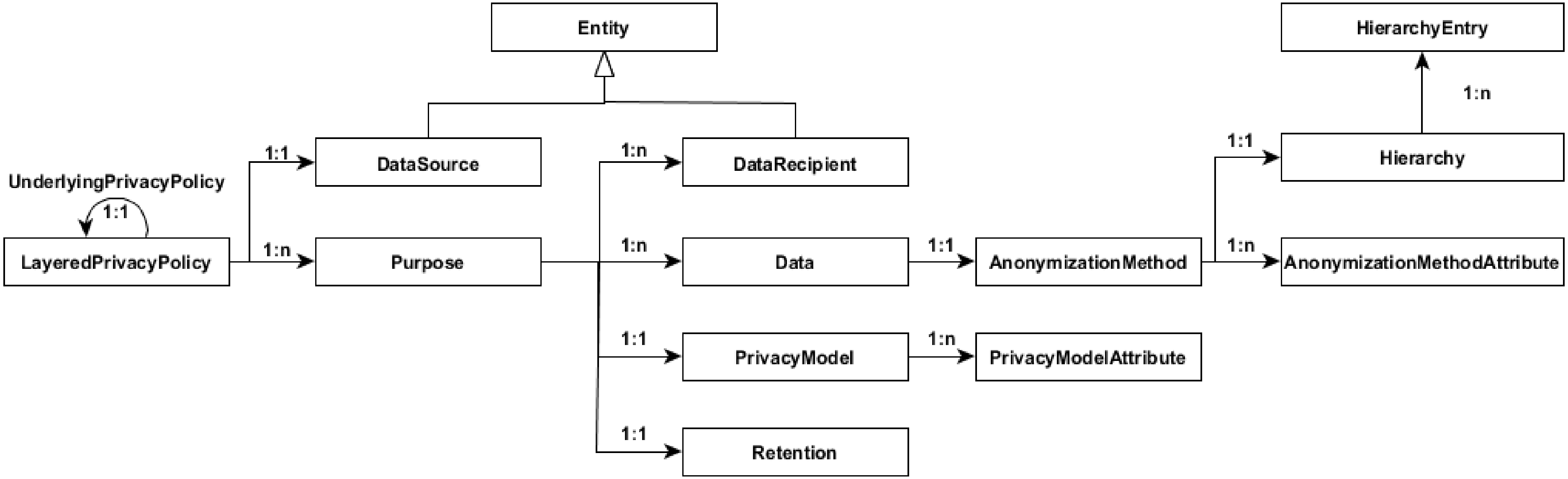
Legal View:

- Privacy Policy Structure
- Data Subject Rights
- Consent
- Human-Readability

Technical View:

- Access Control
- Anonymization Method
- Privacy Model
- Provenance

LPL is a language combining the Legal and Technical View on Privacy

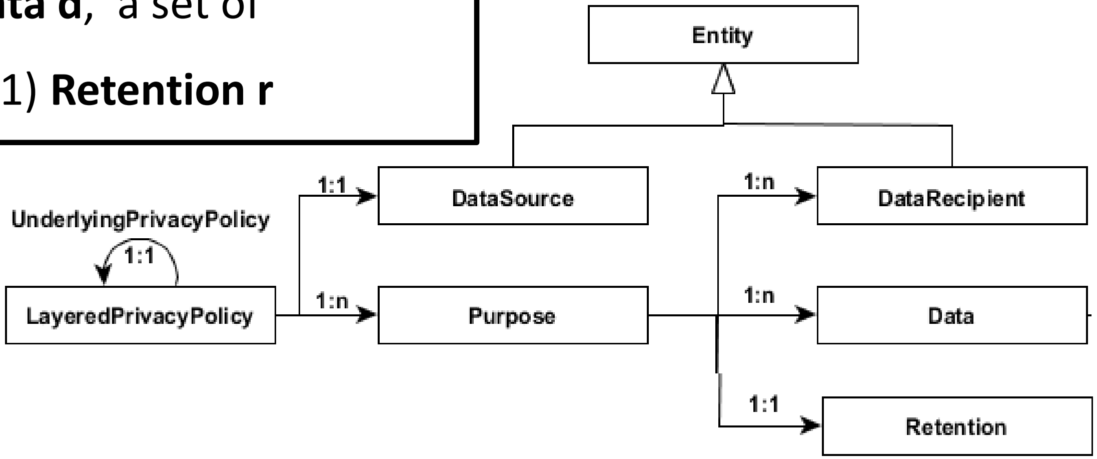


LPL – Privacy Policy Structure

The **LayeredPrivacyPolicy lpp** is the root-element of each LPL privacy policy

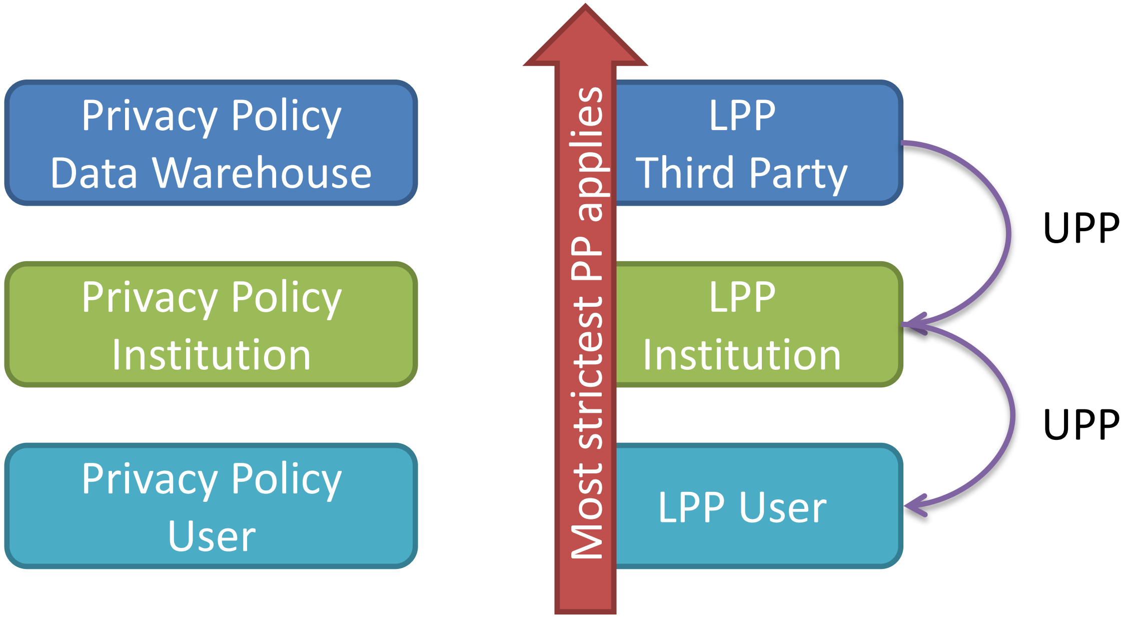
For each **LayeredPrivacyPolicy lpp** defines a set of **Purposes p** as well as a (1) **DataSource ds**

Each **Purpose p** defines a set of **Data d**, a set of **DataRecpients dr** as well as a (1) **Retention r**



LPL – Why Layers?

For each **Layered Privacy Policy (LPP)** another (1) LPP can be added as ‚Underlying Privacy Policy‘



Privacy Policy Data Warehouse

Privacy Policy Institution

Privacy Policy User

Most strictest PP applies

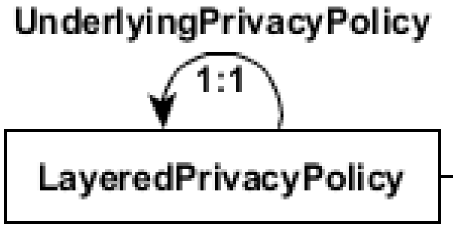
LPP Third Party

LPP Institution

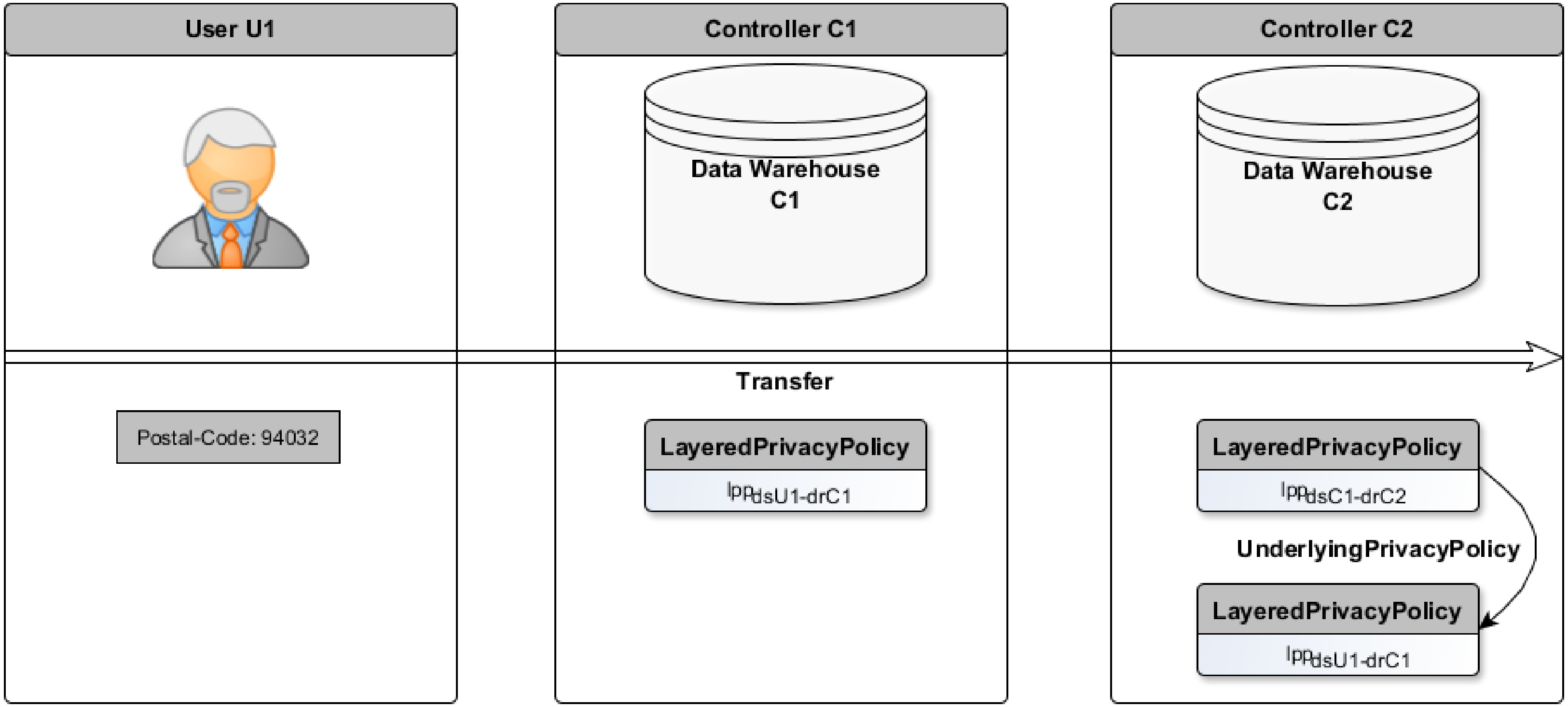
LPP User

UPP

UPP



LPL – Why Layers?



Elements and attributes of LPL have been omitted for better readability

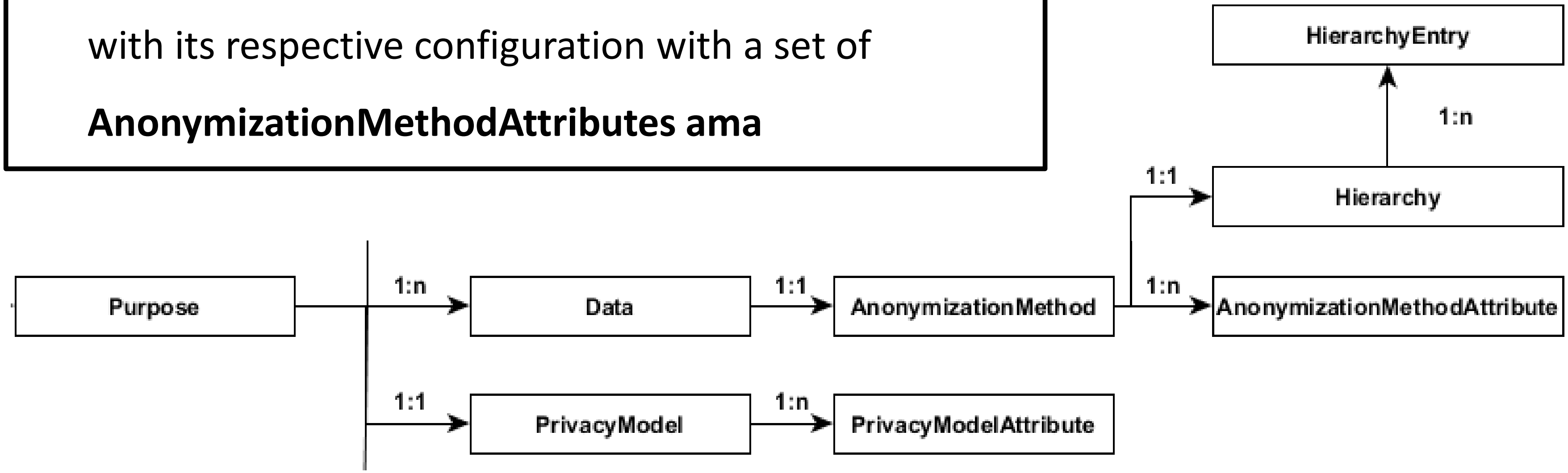
Personalized Privacy Policy in Car

National/Global Policies of Company

LPL – Anonymization

Each **Purpose p** defines a (1) **PrivacyModel pm** with its respective configuration with a set of **PrivacyModelAttributes pma**

Each **Data d** defines a (1) **AnonymizationMethod am** with its respective configuration with a set of **AnonymizationMethodAttributes ama**



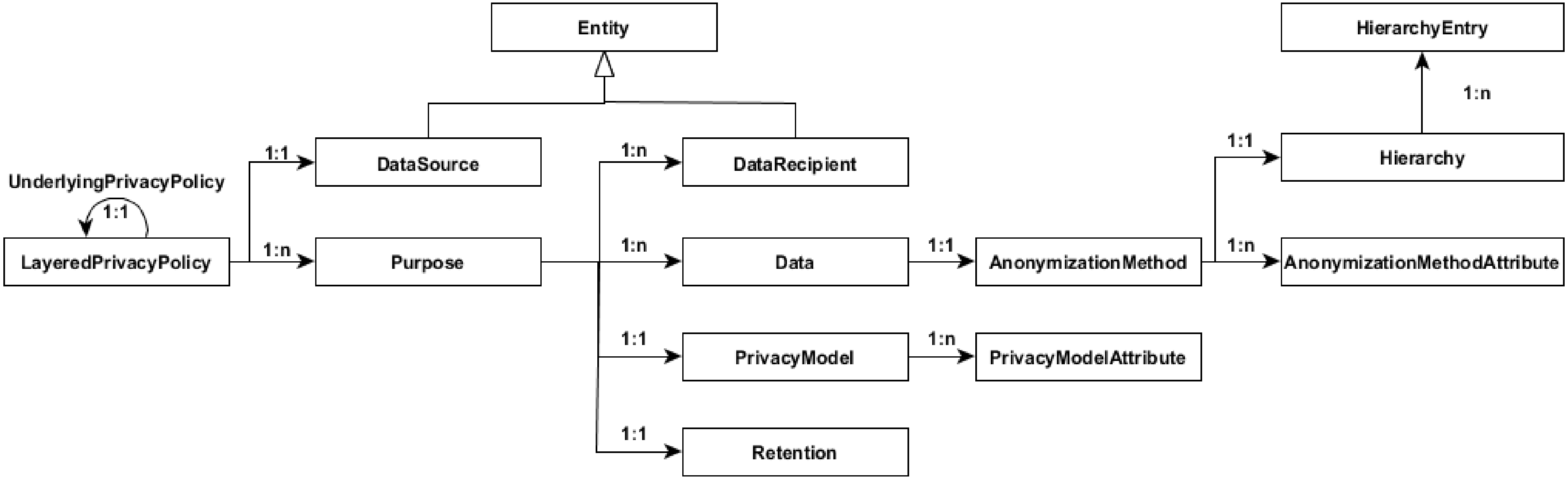
LPL- Personalization

Human-Readability

- Attributes describing content in clear text for elements
- LayeredPrivacyPolicy, Entity, Purpose, Data, Retention, Privacy Model, AnonymizationMethod

Personal Privacy

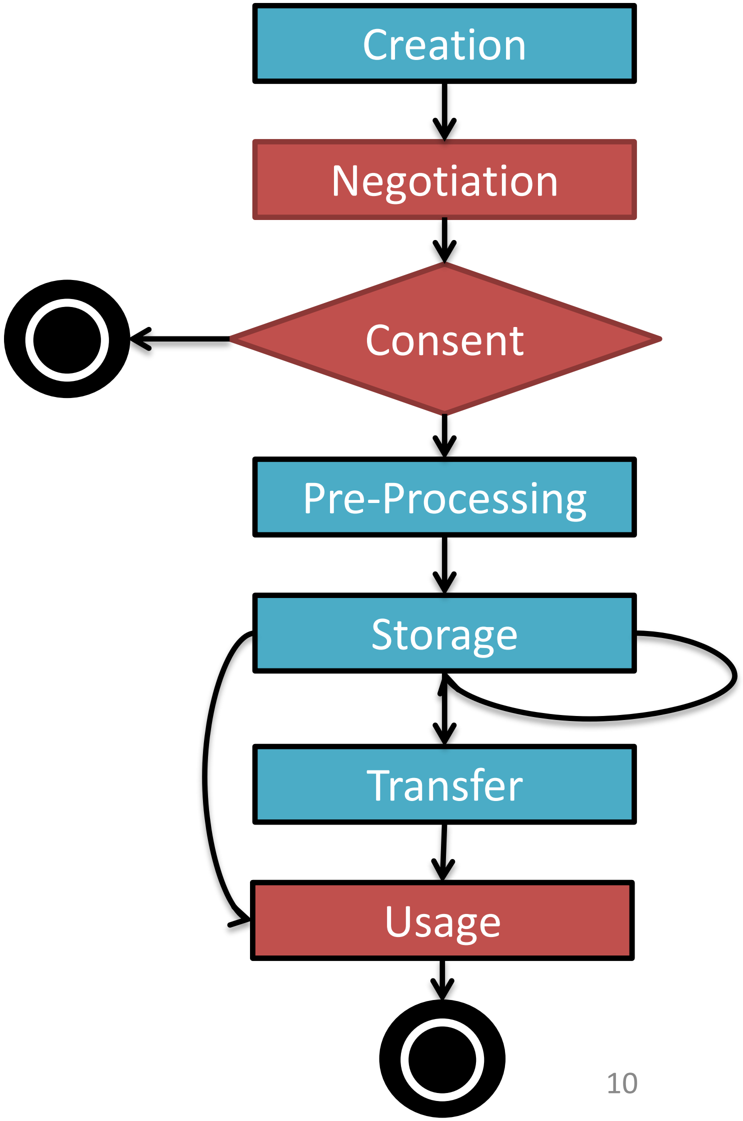
- Attributes describing if element can be dissented to
- Purpose, Data, DataRecipient



Privacy-Process

Usage of LPL for the Privacy Process

1. **Creation** of **LPL-Privacy Policy** based on **Legal Privacy Policy**
2. **Negotiation** of Privacy Policy to User
3. **Pre-Processing** of LPL-Policy if **Consent** is given
4. **Storage** of Data and LPL-Policy
5. **Transfer** of Data to Trusted Third Party (Optional)
6. **Usage** of Data



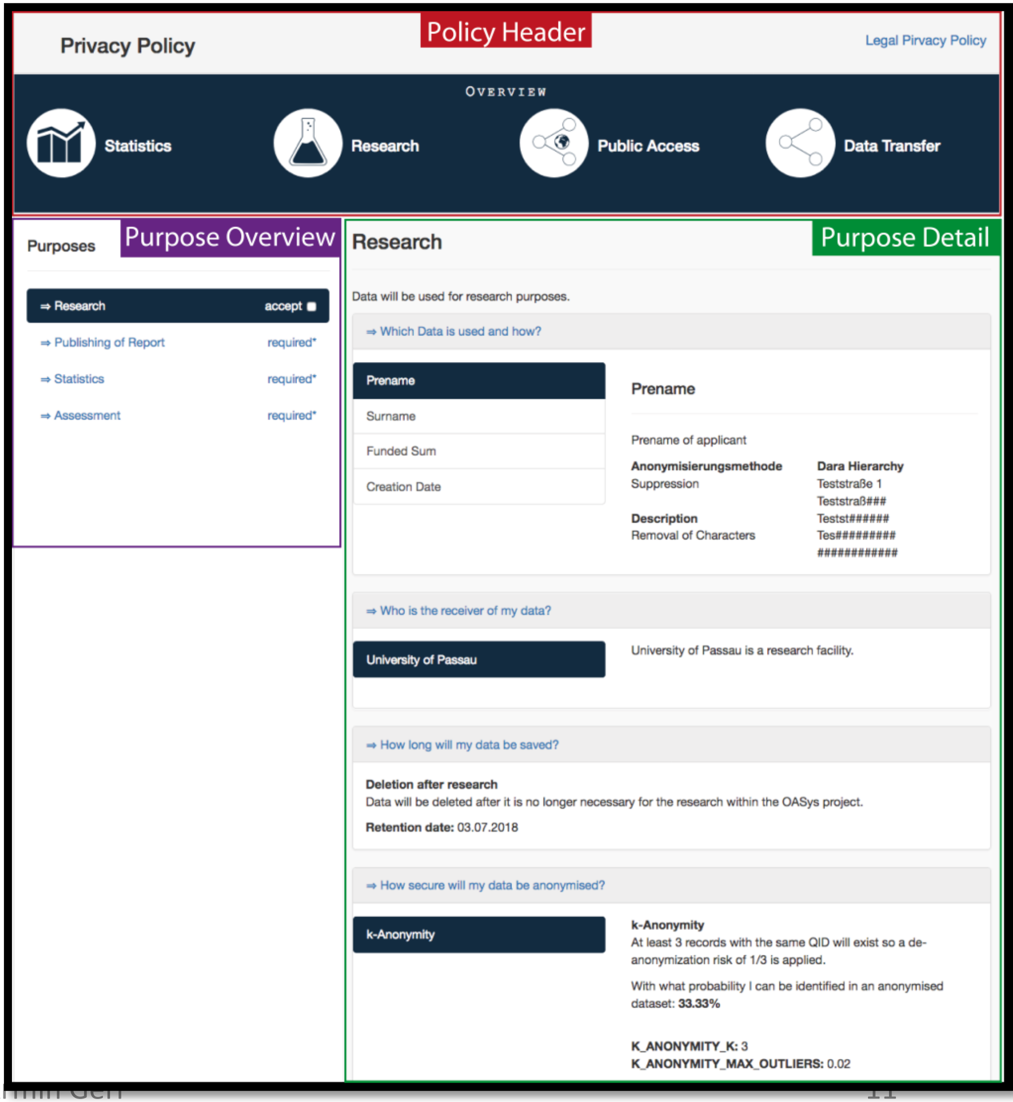
User Interface

LPL Personalized Privacy Policy UI

- VISM Approach
- Overview with Privacy Icons
- Consent/Dissent to Purposes
- ➢ Proof-of-Concept for Web-Applications

Future Work

- More Personalization (DataRecipient, Data, etc.)
- Domain-specific UI (automotive)



Research

Data will be used for research purposes.

⇒ Which Data is used and how?

Prename
Surname
Funded Sum
Creation Date

Prename

Prename of applicant

Anonymisierungsmethode
Suppression

Description
Removal of Characters

Dara Hierarchy
Teststraße 1
Teststraß###
Testst######
Tes#########
############

⇒ Who is the receiver of my data?

University of Passau

University of Passau is a research facility.

⇒ How long will my data be saved?

Deletion after research
Data will be deleted after it is no longer necessary for the research within the OASys project.

Retention date: 03.07.2018

⇒ How secure will my data be anonymised?

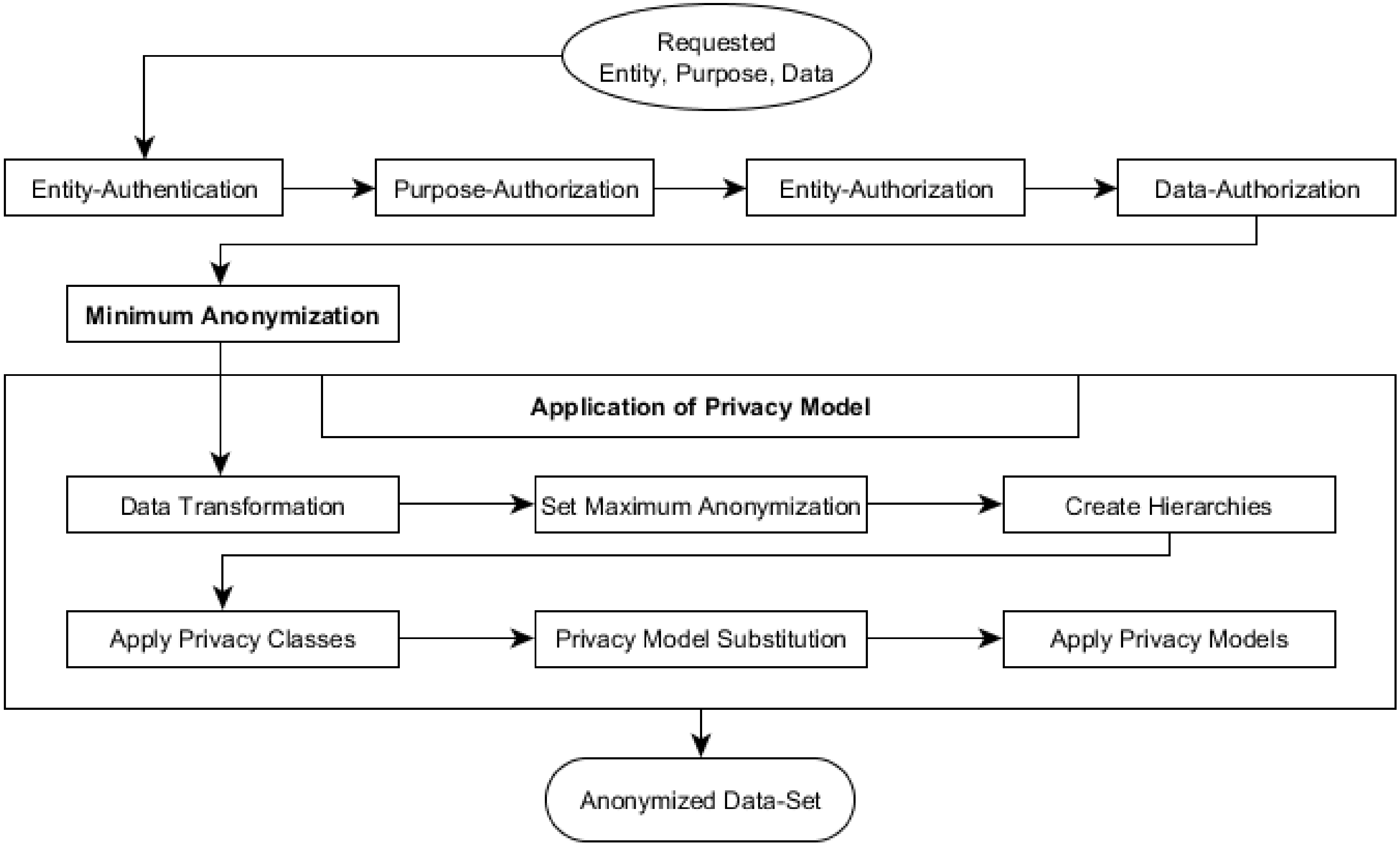
k-Anonymity

k-Anonymity
At least 3 records with the same QID will exist so a de-anonymization risk of 1/3 is applied.

With what probability I can be identified in an anonymised dataset: **33.33%**

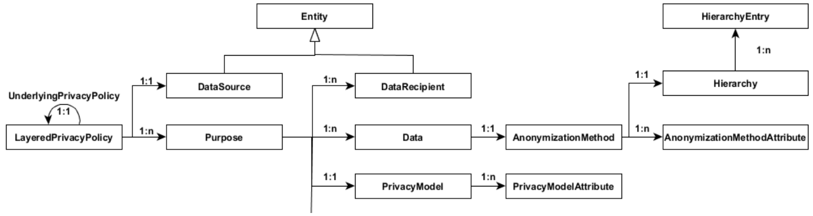
K_ANONYMITY_K: 3
K_ANONYMITY_MAX_OUTLIERS: 0.02

Privacy-Process: Usage

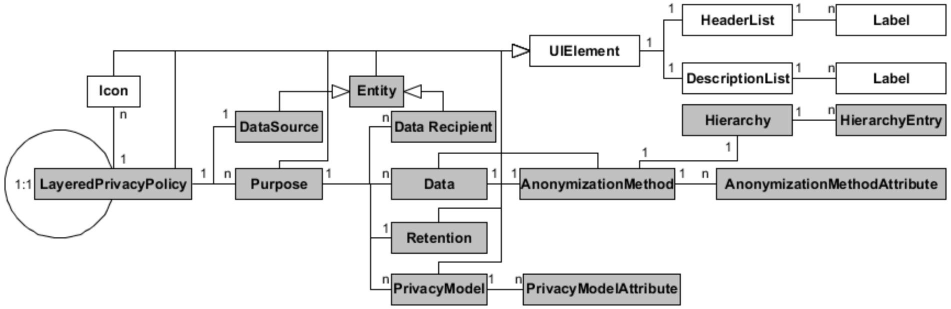


LPL Evolution

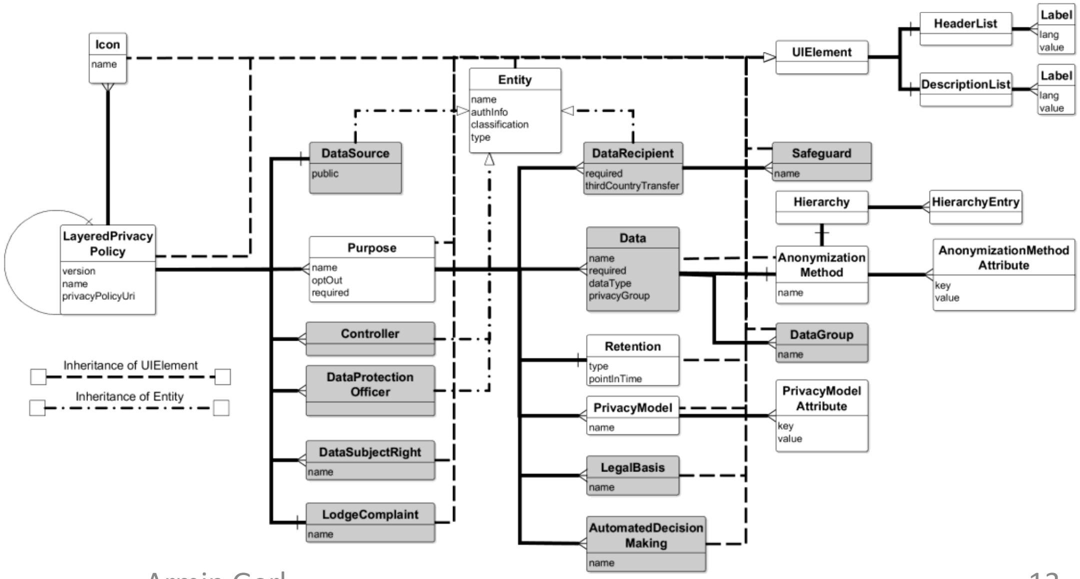
Layered Privacy Language:



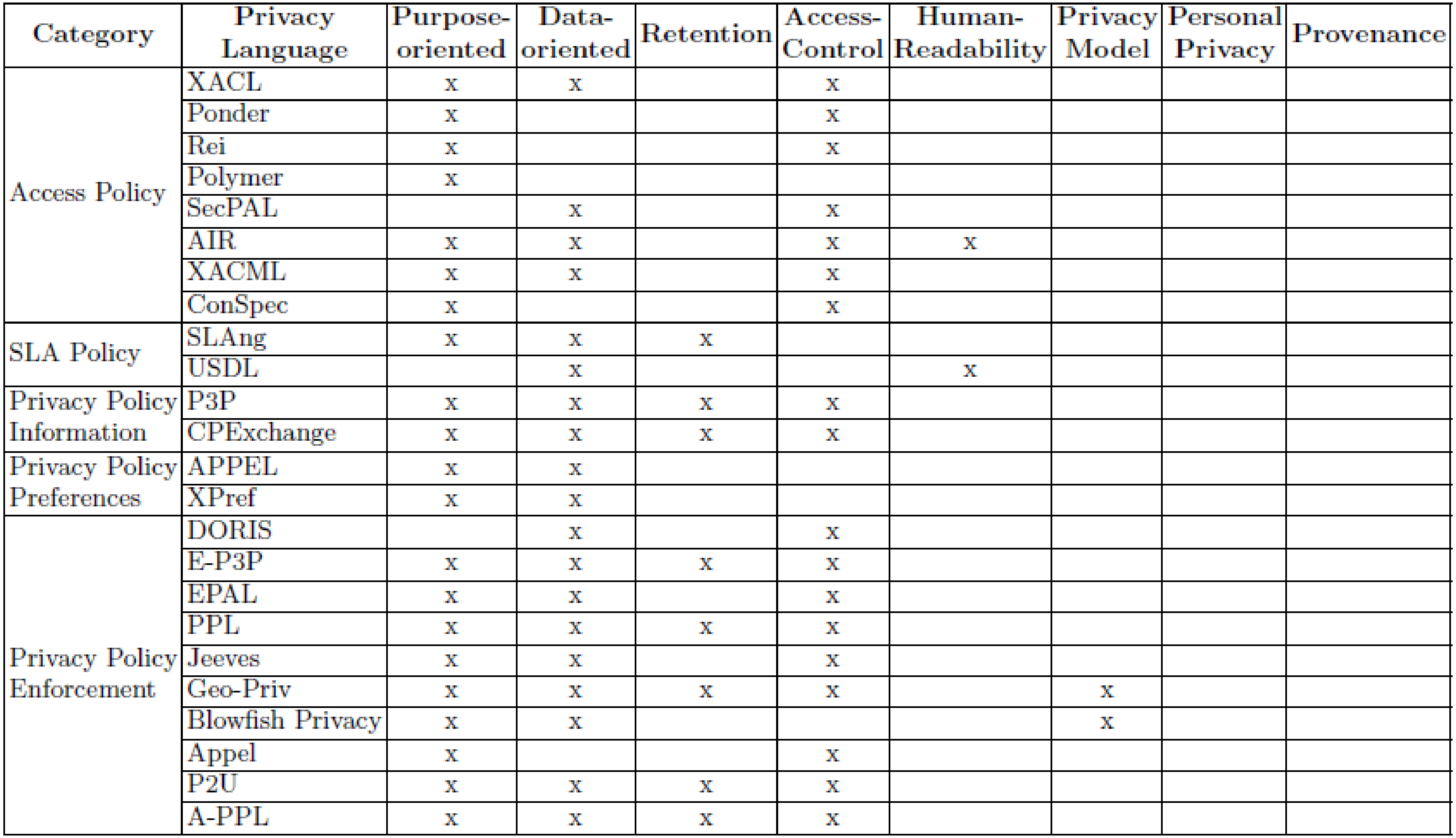
LPL UI Extension:



LPL Art. 12-14 Extension:



State-of-the-Art Analysis



Category	Privacy Language	Purpose-oriented	Data-oriented	Retention	Access-Control	Human-Readability	Privacy Model	Personal Privacy	Provenance
Access Policy	XACL	x	x		x				
	Ponder	x			x				
	Rei	x			x				
	Polymer	x							
	SecPAL		x		x				
	AIR	x	x		x	x			
	XACML	x	x		x				
	ConSpec	x			x				
SLA Policy	SLAng	x	x	x					
	USDL		x			x			
Privacy Policy Information	P3P	x	x	x	x				
	CPExchange	x	x	x	x				
Privacy Policy Preferences	APPEL	x	x						
	XPref	x	x						
Privacy Policy Enforcement	DORIS		x		x				
	E-P3P	x	x	x	x				
	EPAL	x	x		x				
	PPL	x	x	x	x				
	Jeeves	x	x		x				
	Geo-Priv	x	x	x	x		x		
	Blowfish Privacy	x	x				x		
	Appel	x			x				
	P2U	x	x	x	x				
	A-PPL	x	x	x	x				

Future Work

Privacy Framework

- Access Control and Support Structures
- Regulated Purposes (Data Subject Rights) Integration
- Extension for Pseudonymization

➢ Evaluation of all processes according to use cases

Publications

Published:

- Armin Gerl and Dirk Pohl, The Right to data portability between legal possibilities and technical boundaries, Stiftung Datenschutz, Practical Implementation of the Right to Data Portability, 2017
- Gerl A., Bennani N., Kosch H., Brunie L., (2018) LPL, Towards a GDPR-Compliant Privacy Language: Formal Definition and Usage. LNCS Transactions on Large-Scale Data- and Knowledge-Centered Systems, XXXVII, The final authenticated publication will be available online on SpringerLink, https://link.springer.com/
- Armin Gerl, Extending LPL to Support Privacy Icons for a Personal Privacy Policy User Interface, Proceedings of 32nd Human Computer Interaction Conference, BCS Learning and Development Ltd
- ARES Workshop iPAT: Armin Gerl and Dirk Pohl, Critical Analysis of LPL according to Articles 12 - 14 of the GDPR
- Mensch und Computer 2018: Armin Gerl and Florian Prey, LPL Personal Privacy Policy User Interface

Thank you for your attention!

Any more questions?

Contact

HELLO! BONJOUR! SERVUS!

2nd Year Cotutelle PhD Student
Mail: Armin.Gerl@uni-passau.de
Thesis: **Modelling of a Privacy Language and Efficient Query-based Anonymization**

Supervisors: Prof. Harald Kosch, Prof. Lionel Brunie
Co-Supervisor: Dr. Nadia Bennani