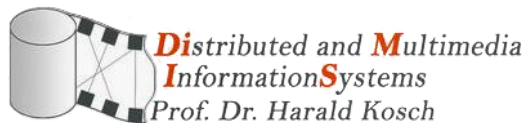


Consent based on the Layered Privacy Language (LPL)





HELLO! BONJOUR! SERVUS!

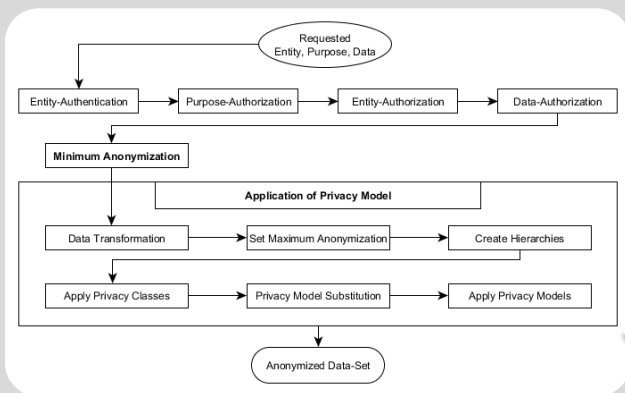
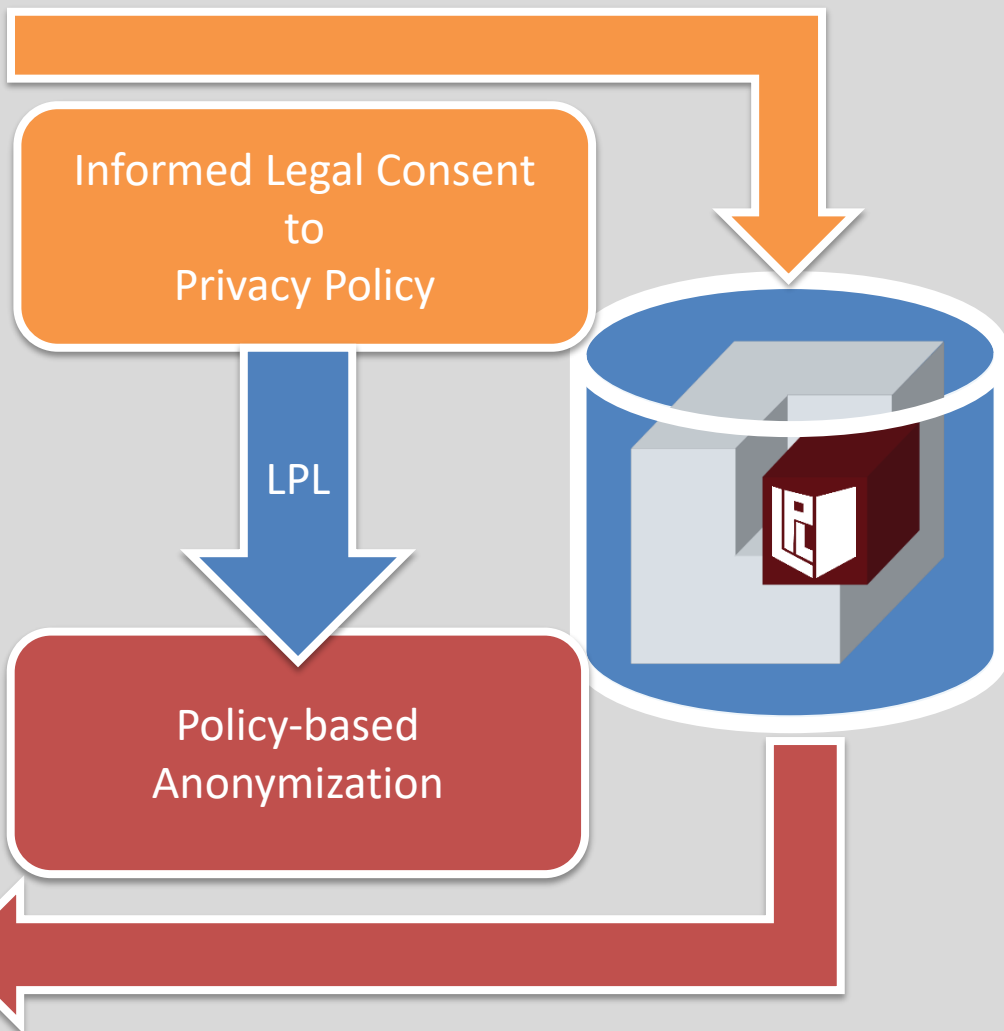
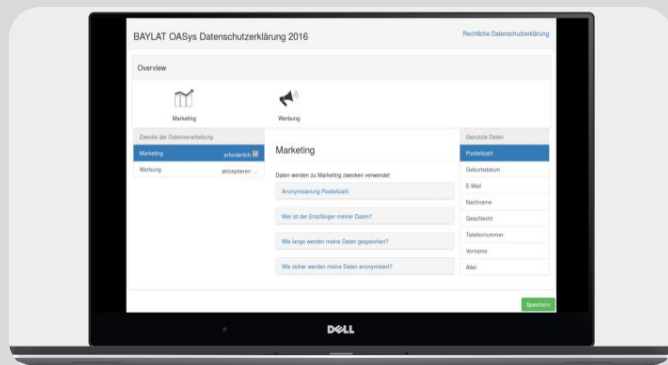
2nd Year Cotutelle PhD Student

Mail: Armin.Gerl@uni-passau.de

Thesis: **Modelling of a Privacy Language and Efficient Query-based Anonymization**

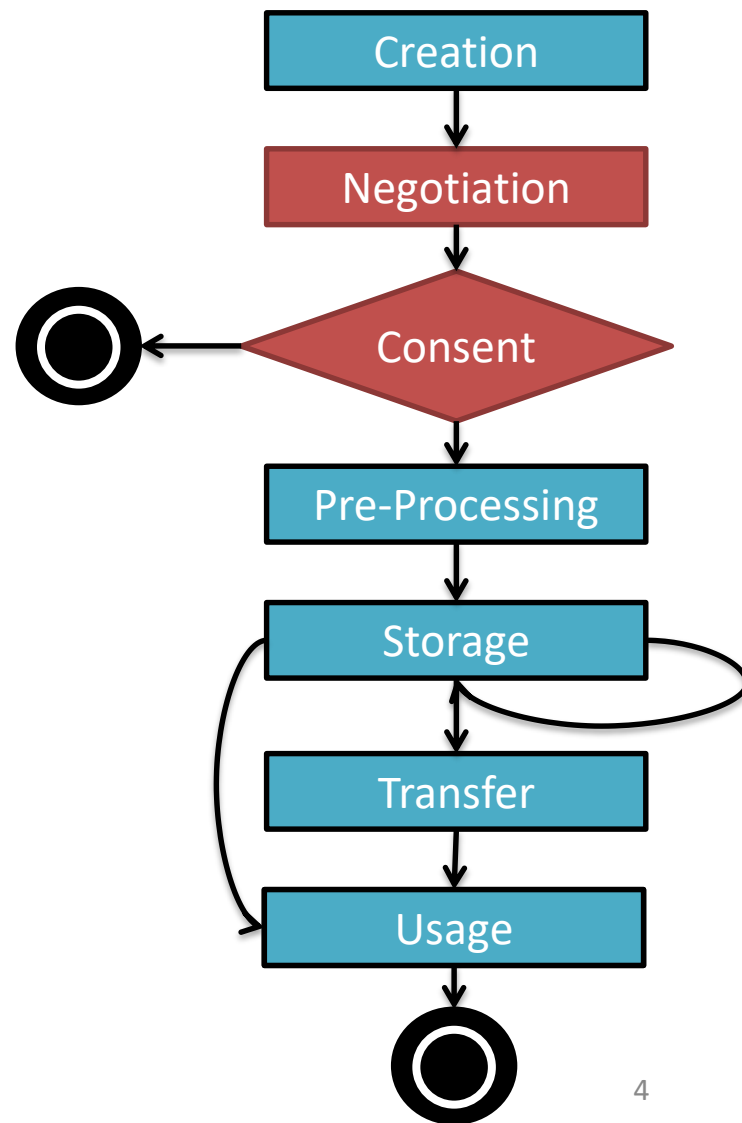
Supervisors: Prof. Harald Kosch, Prof. Lionel Brunie

Co-Supervisor: Dr. Nadia Bennani



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**



Art. 7 GDPR - Conditions for consent

‘...controller shall be able to **demonstrate that the data subject has consented...**’

‘...the request for consent shall be presented in a manner which is

- **clearly distinguishable from the other matters,**
- **in an intelligible and easily accessible form,**
- **using clear and plain language.’**

‘...right to withdraw his or her consent at any time.

- **Prior to giving consent,** the data subject **shall be informed** thereof.
- It shall be **as easy to withdraw as to give consent.’**

- Consent has to be given freely and not enforced

Recital 32 - Conditions for consent

Consent should be given by a **clear affirmative act** ... such as by a **written statement**, including by **electronic means**, or an oral statement.

Examples:

- ✓ ticking a box
- ✓ choosing technical settings
- ✓ another statement or conduct which clearly indicates ... the data subject's acceptance
- Silence, **pre-ticked boxes or inactivity should not** therefore **constitute consent**

If the data subject's consent is to be given following a **request by electronic means**, the **request must be clear, concise** and **not unnecessarily disruptive to the use of the service** for which it is provided.

Recital 32 - Conditions for Consent

Consent should cover **all processing activities** carried out for the **same purpose or purposes**. When the **processing has multiple purposes**, consent should be given for **all of them**.

- Differentiation of purposes is required
- Consent has to be given for each purpose
- Consent covers all processes for the same purpose

Art. 12 GDPR

Transparent information, communication and modalities for the exercise of the rights of the data subject

Art. 13 GDPR

Information to be provided where personal data are collected from the data subject

Art. 14 GDPR

Information to be provided where personal data have not been obtained from the data subject

GDPR	
Article	Requirement
Art. 12(1) Sentence 1	Clear and Plain Language
Art. 12(1) Sentence 2	Written or Electronic Information
Art. 12(2)	Data Subject Rights Realization
Art. 12(3)	Response Time for Data Subject Rights
Art. 12(5)	Excessive Data Subject Rights Requests
Art. 12(7)	Standardized Icons
Art. 13(1)(a), Art. 14(1)(a)	Identity and Contact Details of Controller
Art. 13(1)(b), Art. 14(1)(b)	Contact Details of Data Protection Officer
Art. 13(1)(c), Art. 14(1)(c)	Purposes and Legal Basis for Processing
Art. 13(1)(d), Art. 14(2)(b)	Legitimate Interest
Art. 14(1)(d)	Categories of Personal Data
Art. 13(1)(e), Art. 14(1)(e)	Recipients of Personal Data
Art. 13(1)(f), Art. 14(1)(f)	Third Country Transfer and Safeguards
Art. 13(2)(a), Art. 14(2)(a)	Storage Period
Art. 13(2)(b), Art. 14(2)(c)	Information on Data Subject Rights
Art. 13(2)(c), Art. 14(2)(d)	Information to Withdraw Consent
Art. 13(2)(d), Art. 14(2)(e)	Information to Lodge a Complaint
Art. 13(2)(e)	Information on Required Data
Art. 14(2)(f)	Source of Personal Data
Art. 13(2)(f), Art. 14(2)(g)	Automated Decision-Making

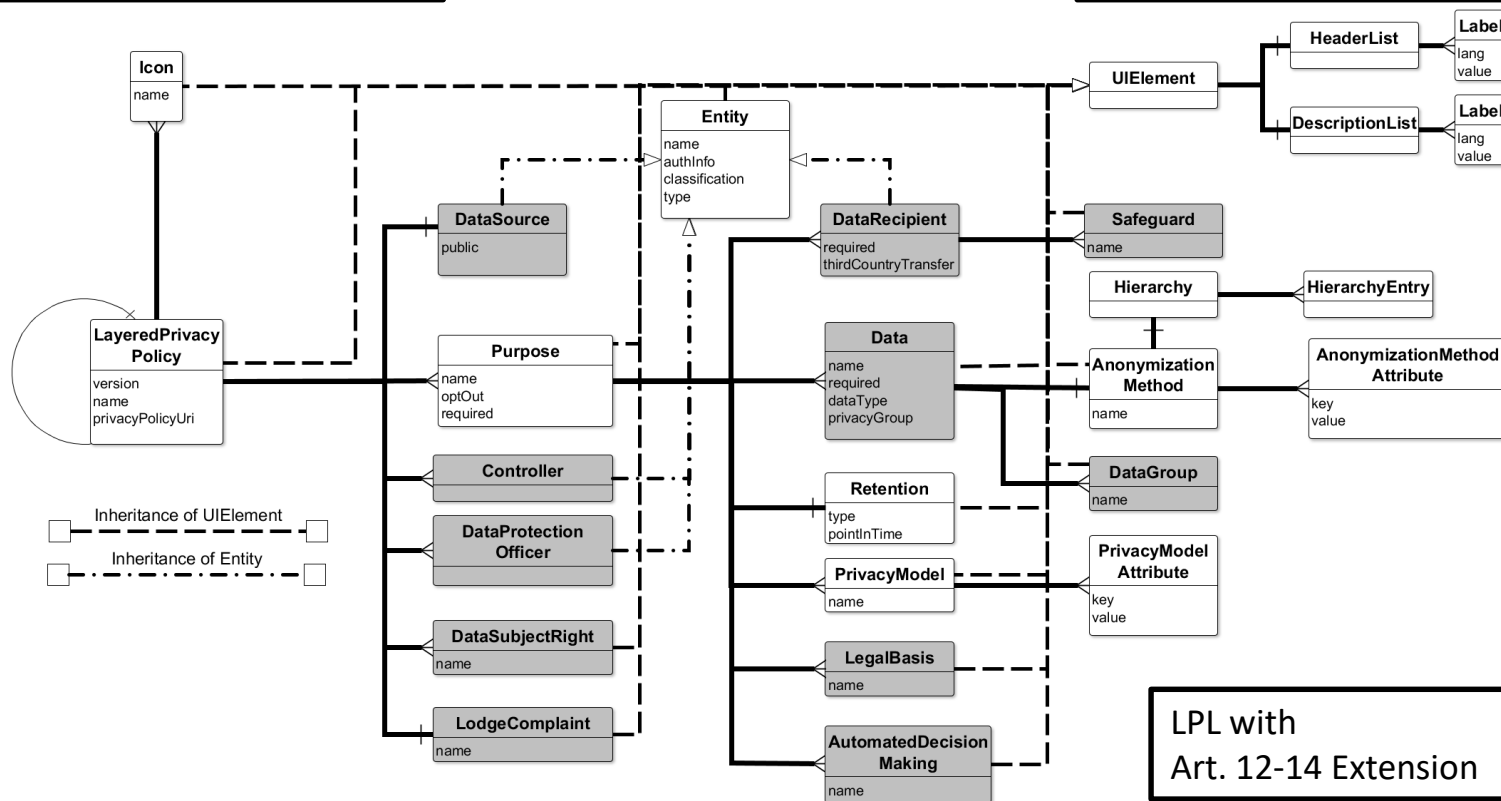
Information has to be provided in a clear and understandable way (Art. 7) otherwise consent might not be valid and no legal basis for the processing exists.

Legal View:

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

Technical View:

- Access Control
- Anonymization Method
- Privacy Model
- Provenance



LPL with
Art. 12-14 Extension

How does LPL fulfill the conditions for consent?

Required information is available

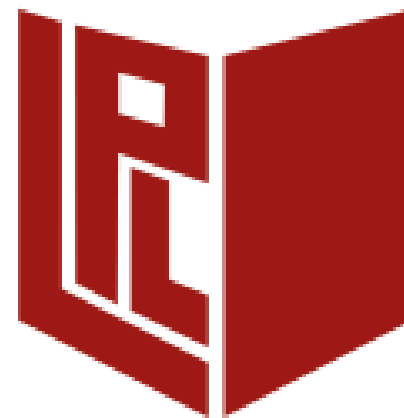
- Structured
- Human-readable (internationalization support)
- Support for Privacy Icons

Differentiation between purposes

- Required or optional
- Opt-in or opt-out
- Definition of data, data recipients, retention, ...

Presentation of LPL

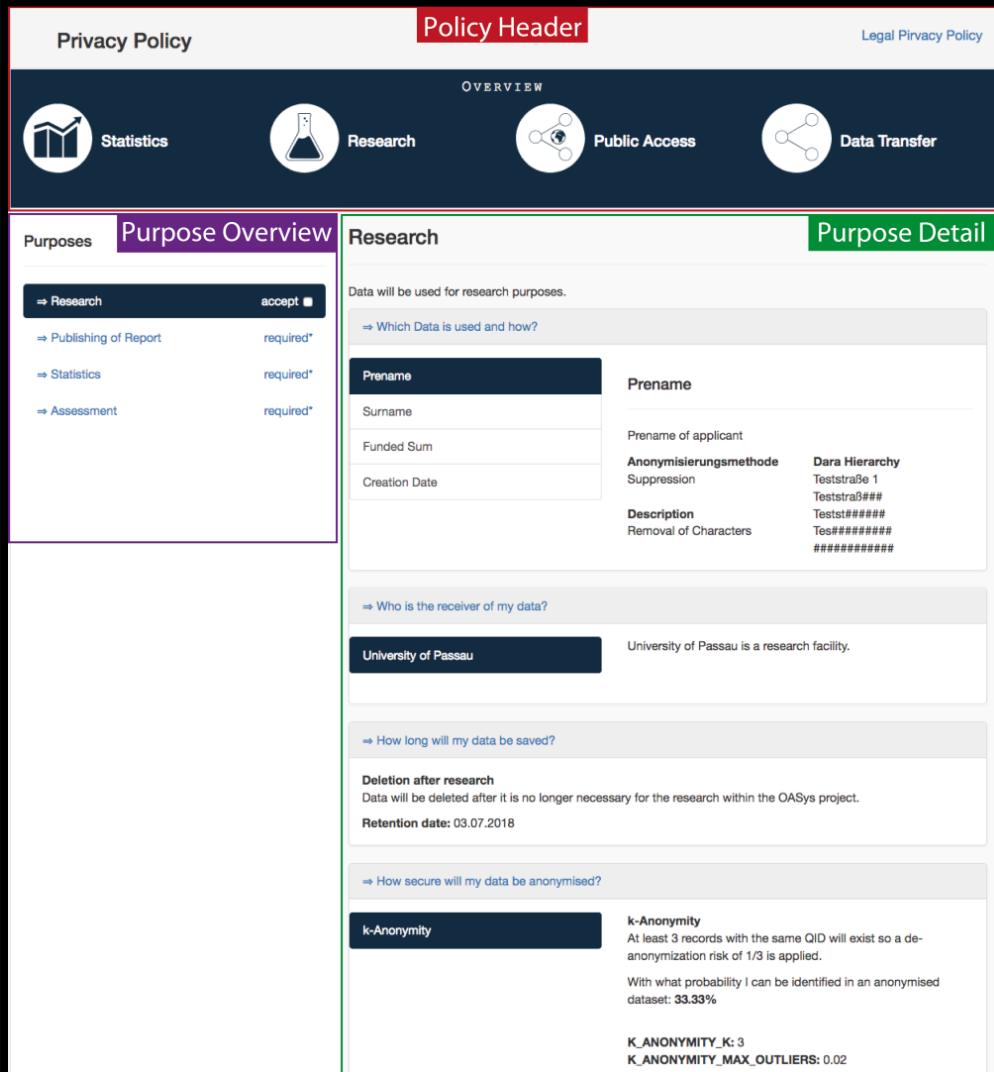
- LPL Personalized Privacy Policy UI



LPL does not verify if human-readable descriptions are in a **clear and plain language**

LPL Personalized Privacy Policy UI

- 1st Iteration
 - VISM Approach
 - Overview with Privacy Icons
 - Consent/Dissent to Purposes
 - Structured Information
- Proof-of-Concept for Web



The screenshot displays a web interface for a Privacy Policy. At the top, there is a 'Policy Header' with the title 'Privacy Policy' and a link to 'Legal Privacy Policy'. Below the header is a navigation bar with icons for 'Statistics', 'Research', 'Public Access', and 'Data Transfer'. The main content area is divided into two sections: 'Purpose Overview' and 'Research Purpose Detail'.

Purpose Overview

Purposes	Consent Status
→ Research	accept
→ Publishing of Report	required*
→ Statistics	required*
→ Assessment	required*

Research Purpose Detail

Data will be used for research purposes.

⇒ Which Data is used and how?

Field	Description
Prenome	Prenome of applicant
Surname	
Funded Sum	
Creation Date	
Anonymisierungsmethode	Dara Hierarchy
Suppression	Teststraße 1
Description	Testst#####
Removal of Characters	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?

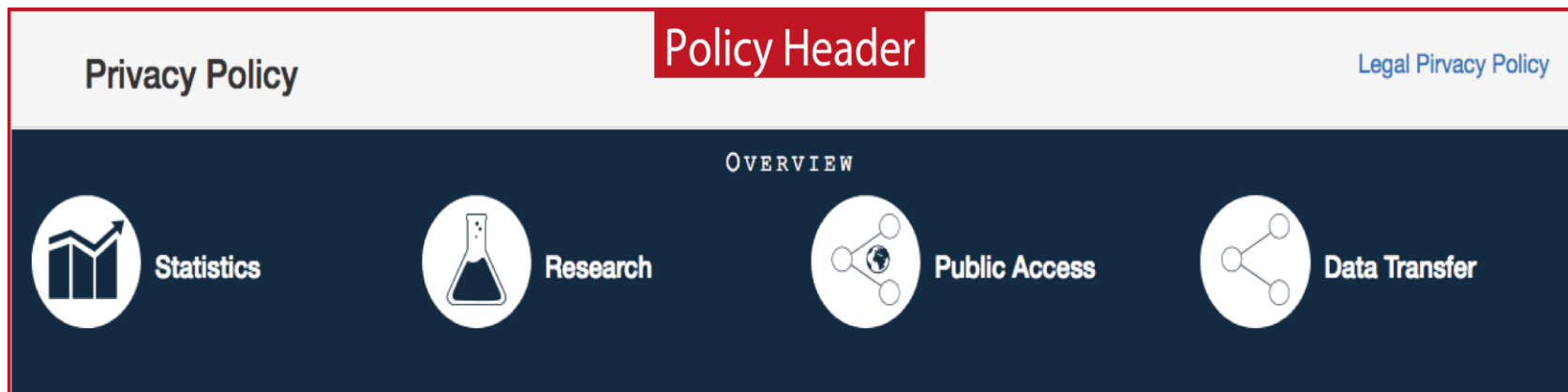
k-Anonymity
At least 3 records with the same QID will exist so a de-anonymization risk of 1/3 is applied.
With what probability I can be identified in an anonymised dataset: **33.33%**
K_ANONYMITY_K: 3
K_ANONYMITY_MAX_OUTLIERS: 0.02

Privacy Icons*

- Representation of Purposes
- „Overview at a glance“
- Standardised Privacy Icons are not yet defined (Idea: Privacy Icons in Context of Mobility?)

Layering (Legal Term)

- Regular Privacy Policy /Additional Details
- Provides Legal Certainty („State-of-the-Art“)



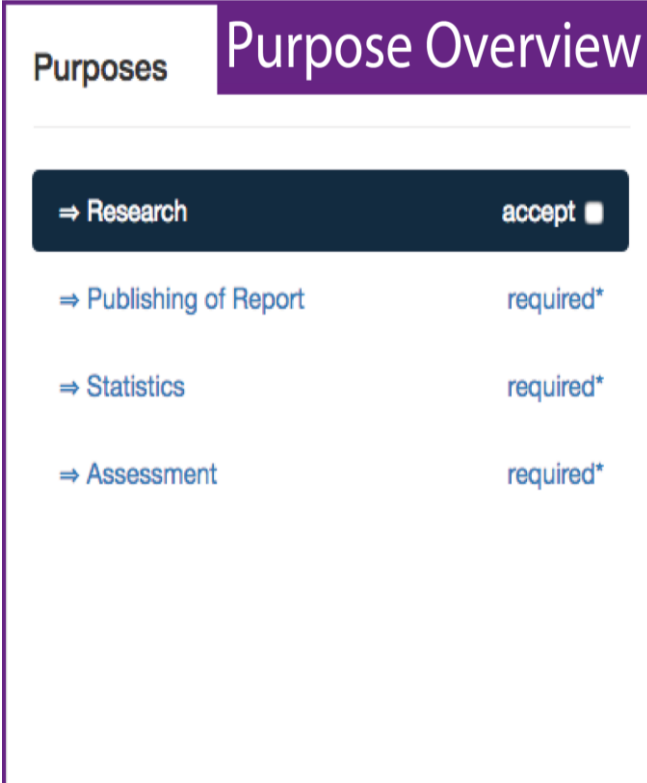
*Armin Gerl, Extending LPL to Support Privacy Icons for a Personal Privacy Policy User Interface, Proceedings of 32nd Human Computer Interaction Conference, BCS Learning and Development Ltd

Personalization/Consent

- **Required Purposes:** Based on a legal basis
- **Optional Purposes:** Consent to Processing is possible (opt-in), Dissent is exactly as easy

Visual Information Seeking Mantra

- „Overview First, Details on Demand“
- Additional details for each purpose



The screenshot shows a 'Purpose Overview' interface. It features a dark blue header with the text 'Purpose Overview' in white. Below the header, there is a list of purposes. The first purpose, 'Research', is highlighted in a dark blue box and has an 'accept' button with a checked checkbox. The other three purposes, 'Publishing of Report', 'Statistics', and 'Assessment', are listed in blue text and are marked as 'required*'.

Purposes	Consent Status
⇒ Research	accept <input checked="" type="checkbox"/>
⇒ Publishing of Report	required*
⇒ Statistics	required*
⇒ Assessment	required*

Which data will be processed?

- Detailed Listing
- Data Grouping
- Definition of Anonymization

Who are the Data Recipients?

- Detailed Listing

How long is the data stored?

- Fixed Date, After Purposes Fullfillment,
No Deletion

How is the data set anonymized?

- Privacy Models (k-Anonymity, l-Diversity, etc.)

Research
Purpose Detail

Data will be used for research purposes.

⇒ Which Data is used and how?

Prenome	Prenome												
Surname	Prenome of applicant												
Funded Sum	<table style="width: 100%; border: none;"> <tr> <td style="padding: 2px;">Anonymisierungsmethode</td> <td style="padding: 2px;">Dara Hierarchy</td> </tr> <tr> <td style="padding: 2px;">Suppression</td> <td style="padding: 2px;">Teststraße 1</td> </tr> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">Teststraße###</td> </tr> <tr> <td style="padding: 2px;">Description</td> <td style="padding: 2px;">Testst#####</td> </tr> <tr> <td style="padding: 2px;">Removal of Characters</td> <td style="padding: 2px;">Tes#####</td> </tr> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">#####</td> </tr> </table>	Anonymisierungsmethode	Dara Hierarchy	Suppression	Teststraße 1		Teststraße###	Description	Testst#####	Removal of Characters	Tes#####		#####
Anonymisierungsmethode	Dara Hierarchy												
Suppression	Teststraße 1												
	Teststraße###												
Description	Testst#####												
Removal of Characters	Tes#####												
	#####												
Creation Date													

⇒ 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	<p>k-Anonymity At least 3 records with the same QID will exist so a de-anonymization risk of 1/3 is applied.</p> <p>With what probability I can be identified in an anonymised dataset: 33.33%</p> <p>K_ANONYMITY_K: 3 K_ANONYMITY_MAX_OUTLIERS: 0.02</p>
--------------------	---

User Interface 2nd Iteration

- Based on Art. 12 – 14 Extension
- In-depth personalization of policy
- Proof of concept scenario
- Qualitative Evaluation

Extending the LPL Privacy Framework

- Inference Detection/Prevention
- Logging for Accountability
- Pseudonymization

- 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

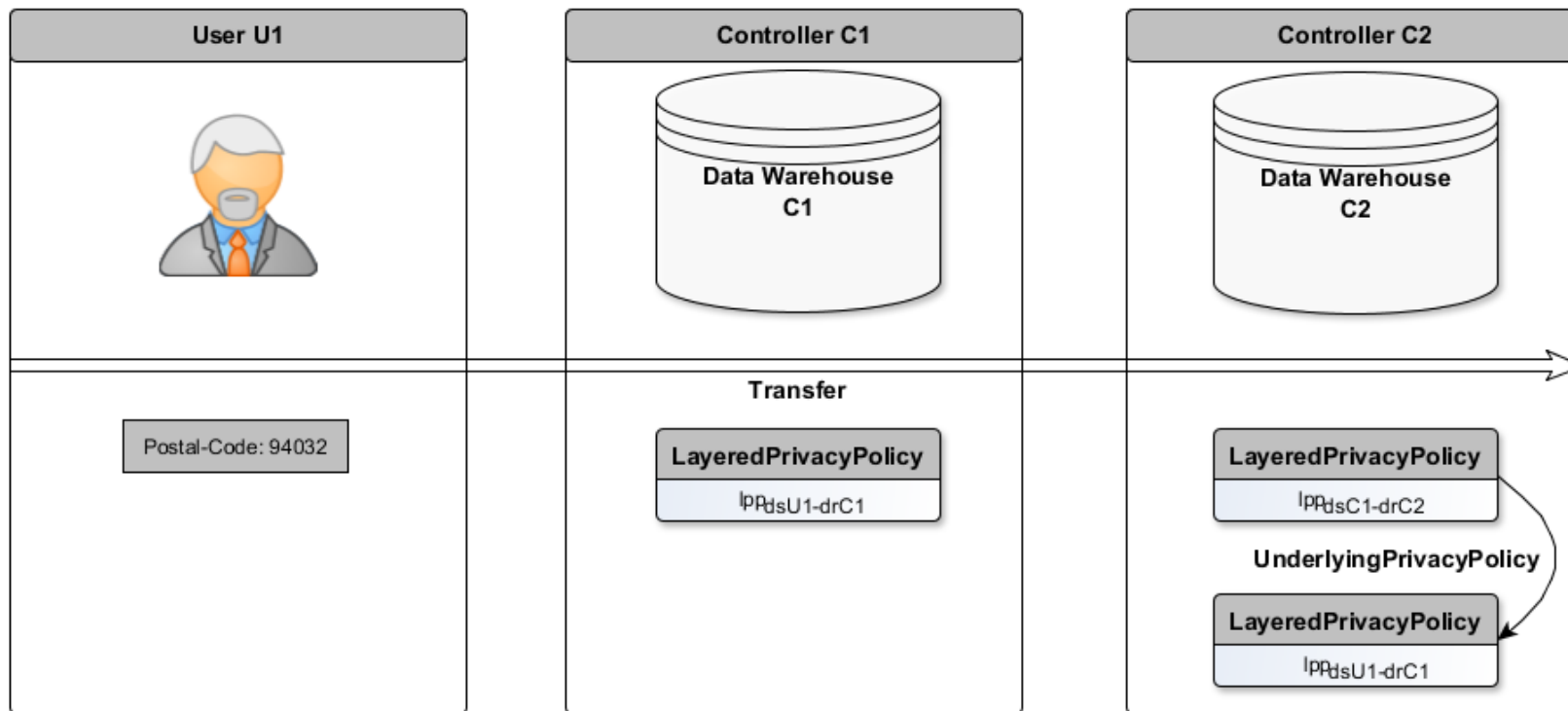
Thank you for your attention!

Any more questions?





Backup Slides

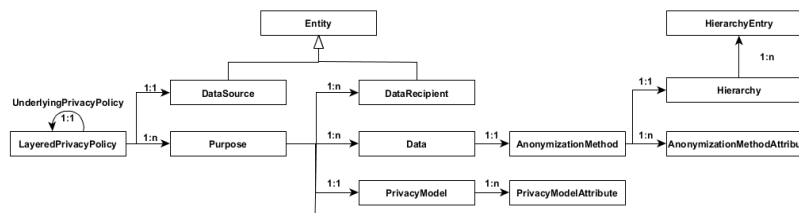


Elements and attributes of LPL have been omitted for better readability

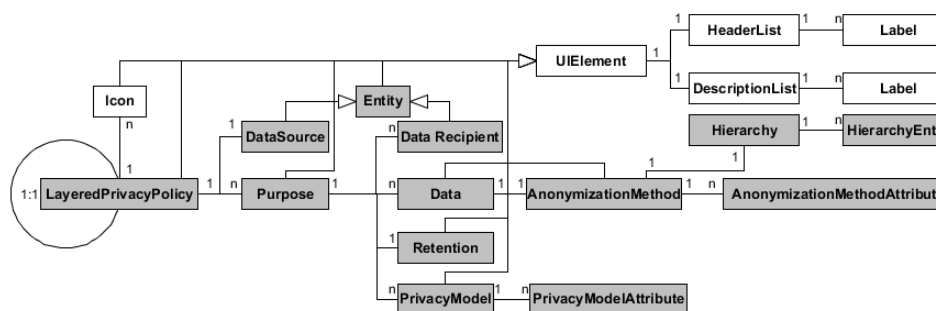
Personalized
Privacy Policy
in Car

National/Global
Policies of
Company

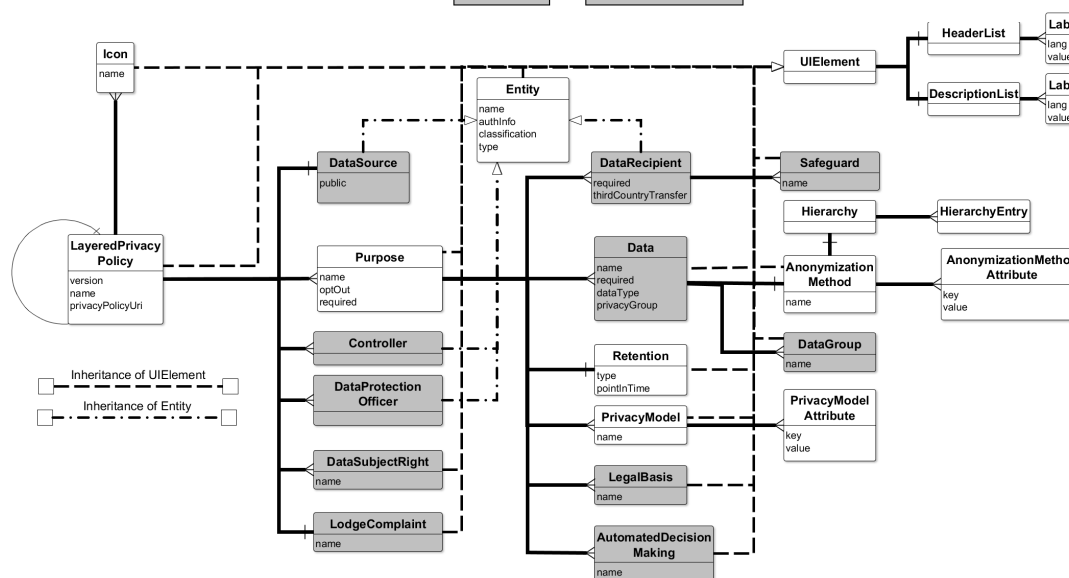
Layered Privacy Language:

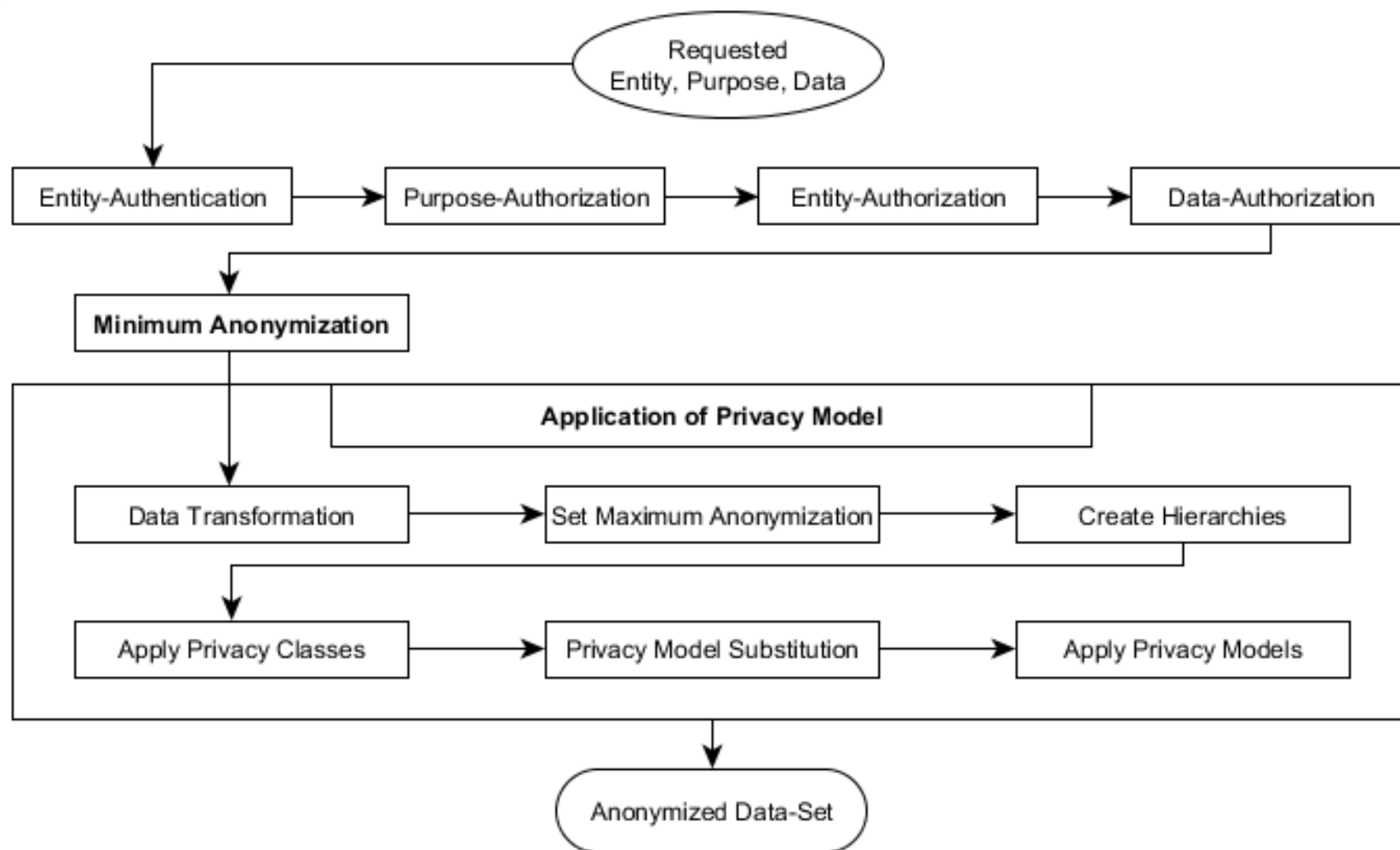


LPL UI Extension:



LPL Art. 12-14 Extension:





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				
	CPEExchange	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					