Organization Questions

- **Is the Lecture applicable for „Security“ Domain and not only for „Information and Communication“?**
- **A: Unfortunately only for „Information and Communication“**

- **Can we re-schedule the lecture because of conflicts with other lectures?**
- **A: Unfortunately this is not possible. This lecture is not mandatory, so there is no basis for rescheduling lectures.**

- **Can I write a „Klausur auf Schein“ for this lecture?**
- **A: Yes, we allow to do the exam to receive a „Schein“. You have to communicate to us at least 2 weeks before the exam that you will do this (or whenever the deadlines for exam registration end).**

Chapter 2:
From GDPR to Privacy Languages

Privacy-Preservation Technologies in Information Systems

Dr. Armin Gerl

WS 2021/2022

Privacy is a Human Right

Article 8 Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority

Charter of Fundamental Rights of the European Union

Furthermore, Privacy as a Human Right can be found in the

- Universal Declaration of Human Rights (Art. 12) of December 1948 or the
- Treaty on the Functioning of the European Union (Art. 16).

Legal Framework for Privacy in Europe:
General Data Protection Regulation

History of GDPR

- **24 October 1995: Directive 95/46/EC** on the protection of individuals with regard to the processing of personal data and on the free movement of such data) is adopted
- 22 June 2011: Publication of EDPS Opinion on EC Communication 'A comprehensive approach on personal data protection in EU‘
- 25 January 2012: EC proposal to strengthen online privacy rights and digital economy
- 23 March 2012: The Article 29 Working Party (WP29) adopts an Opinion on the data protection reform proposal
- 12 March 2014: The **European Parliament demonstrates strong support for the GDPR** by voting in plenary with 621 votes in favour, 10 against and 22 abstentions
- 15 December 2015: The European Parliament, the Council and the Commission reach an agreement on the GDPR
- 2 February 2016: The Article 29 Working Party issues an action plan for the implementation of the GDPR

History of GDPR

- 27 April 2016: Publication of the **Regulation (EU) 2016/679 (General Data Protection Regulation)**
- 24 May 2016: **GDPR enters into force** (20 days after publication)
- 10 January 2017: The European Commission proposes two new regulations on **privacy and electronic communications (ePrivacy)** and on the **data protection rules applicable to EU institutions (currently Regulation 45/2001)** that align the existing rules to the GDPR
- 6 May 2018: Members States must have transposed the **Data Protection Directive for the police and justice sectors into national legislation**. It will be applicable from this day
- 25 May 2018: Corrigendum to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- **25 May 2018: The General Data Protection Regulation will apply from this day**
  - **Harmonized data privacy laws across Europe (all member states), e.g. in Germany the DSGVO**

Structure of GDPR

- GDPR consists of 11 Chapters with a total of 99 Articles
- 173 Recitals
  - Detailing furthermore the intentions of the articles (very interesting and important to interpret the articles)
- Comments
  - Specialized Texts for legal experts for the interpretation of the GDPR, i.e., comments are usually created for the national laws derived from GDPR for example in Germany there is:
    - ❖ Datenschutz-Grundverordnung (DSGVO)
      - ❖ Federal Law: Bundesdatenschutzgesetz (BDSG-neu)
        - ❖ State Law: Bayerische Landesdatenschutzgesetz
    - ❖ Area Specific Law: Telekommunikationsgesetz (TKG), Telemediengesetz (TMG)
    - ❖ Religion Specific Law: Gesetz über den Kirchlichen Datenschutz (KDG)

We cover only the basics of GDPR!

GDPR

Chapter 1 (Art. 1 – 4)
General provisions

Chapter 2 (Art. 5 – 11)
Principles

Chapter 3 (Art. 12 – 23)
Rights of the data subject

Chapter 4 (Art. 24 – 43)
Controller and processor

Chapter 5 (Art. 44 – 50)
Transfers of personal data to third countries or international organisations

Chapter 6 (Art. 51 – 59)
Independent supervisory authorities

Chapter 7 (Art. 60 – 76)
Cooperation and consistency

Chapter 8 (Art. 77 – 84)
Remedies, liability and penalties

Chapter 9 (Art. 85 – 91)
Provisions relating to specific processing situations

Chapter 10 (Art. 92 – 93)
Delegated acts and implementing acts

Chapter 11 (Art. 94 – 99)
Final provisions

Chapter 2.1:
Key Issues

Privacy-Preservation Technologies in Information Systems

Dr. Armin Gerl

WS 2021/2022

Core Principles of the GDPR

The type and amount of personal data a company/organisation may process depends on the reason for processing it (legal reason used) and the intended use. The company/organisation must respect several key rules, including:

- **Lawfulness, Fairness and Transparency:**
  - personal data must be processed in a lawful and transparent manner, ensuring fairness towards the individuals whose personal data is being processed (‘lawfulness, fairness and transparency’);
- **Purpose Limitation:**
  - there must be specific purposes for processing the data and the company/organisation must indicate those purposes to individuals when collecting their personal data. A company/organisation can’t simply collect personal data for undefined purposes (‘purpose limitation’);
  - the company /organisation can’t further use the personal data for other purposes that aren’t compatible with the original purpose;

Core Principles of the GDPR cont.

- **Data Minimisation:**
  - the company/organisation must collect and process only the personal data that is necessary to fulfil that purpose (‘data minimisation’);
- **Accuracy:**
  - the company/organisation must ensure the personal data is accurate and up-to-date, having regard to the purposes for which it is processed, and correct it if not (‘accuracy’);
- **Storage Limitation:**
  - the company/organisation must ensure that personal data is stored for no longer than necessary for the purposes for which it was collected (‘storage limitation’);
- **Integrity and Confidentiality:**
  - the company/organisation must install appropriate technical and organisational safeguards that ensure the security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technology (‘integrity and confidentiality’).

Privacy by Design / Privacy by Default

- “Privacy by Design” and “Privacy by Default” have been frequently-discussed topics related to data protection and first thoughts were expressed already in the 1970s.
- Privacy by Design (Art. 25 GDPR):
  - “data protection through technology design”
  - Privacy should be already integrated in the technology when it is created and not as an “Add-on”.
  - Uncertainty of “Privacy by Design” meaning and implementation:
    - **incomplete implementation** of the GDPR in EU States
    - include definitions of the means for processing TOMs (technical and organizational measures) **at the time that they are defined** in order to fulfil the basics and requirements of “Privacy by Design”.
    - Legislation leaves **completely open which exact protective measures are to be taken**, e.g. only mentioning of “pseudonymisation” but no more details given.
- Privacy by Default (Art. 25 GDPR):
  - Implement appropriate TOMs for ensuring that, by default, only personal data which are **necessary for each specific purpose** of the processing are processed
  - Also applies to **amount of personal data collected**, the **extent of their processing**, the **period of their storage** and their **accessibility** (especially forbid publication)

Controller

- **Controller = Legal Entity**
  - responsible for processing
  - E.g. Company or Public Institution

- Controller has to implement appropriate TOMs to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR
  - Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons
  - TOMs have to be reviewed and updated where necessary.
  - includes the implementation of appropriate data protection policies

- Joint Controllers
  - two or more controllers jointly determine the purposes and means of processing
  - Transparently communicate their respective responsibilities, i.e. in the privacy policy

Data Subject and Personal Data

- **Data Subject = Natural Person**
  - Identifiable natural person is one who can be identified **directly or indirectly**
  - Identification via a reference to an identifier, e.g. name, id number, location data, online identifier, identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

- Personal Data:
  - **Any information** relating to an identified or identifiable natural person
  - Very broad and general definition, but also more specific definitions:
    - **Genetic Data**: personal data relating to the inherited or acquired genetic characteristics
    - **Biometric Data**: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics
    - **Data concerning Health**: personal data related to the physical or mental health

Processing

- Processing
  - **any operation** or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means
  - E.g. collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

- Lawfulness of Processing
- Processing shall be lawful only if and to the extent that at least one of the following applies:
  - the data subject has given **Consent** to the processing of his or her personal data for **one or more specific purposes**
  - processing is necessary for the **performance of a contract** to which the data subject is party
  - processing is necessary for **compliance with a legal obligation** to which the controller is subject
  - processing is necessary in order to **protect the vital interests** of the data subject or of another natural person
  - processing is necessary for the performance of a task carried out in the **public interest**
  - processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party

Consent

- When processing is based on consent, then the controller has to be able to show that the data subject has consented to processing personal data
- Consent decision has to be clearly distinguishable presented from other matters (prevention to hide the “consent checkbox” in fine print) using:
  - Intelligible and easily accessible form
  - Clear and plain language
- Consent must be freely given, specific, informed and unambiguous
  - **Freely given consent**: it must be voluntary and a real choice (no pressure, influence, etc.)
  - **Informed and specific**: the data subject must at least be notified about the **controller’s identity**, what **kind of data will be processed**, **how it will be used** and the **purpose** of the processing operations; Purpose has to be clearly defined
  - **Unambiguous**: requires either a statement or a clear affirmative act
- Right to withdraw consent at any time by data subject
  - It has to be as easy to withdraw as to give consent

Encryption

- Encryption refers to the procedure that converts clear text into a hashed code using a key, where the outgoing information only becomes readable again by using the correct key.
- Encryption is a safeguard to reduce the probability of a data breach
  - Risk-management has to be conducted by the company/controller
  - Similar to the Security Domain in which also no system is considered as fully secure
- GDPR does not define appropriate TOMs, but criteria:
  - the state of the art
  - implementation costs
  - the nature, scope, context and purposes of the processing
  - severity of the risks to the rights and freedoms of the data subject
  - Likelihood for manifestation of risks

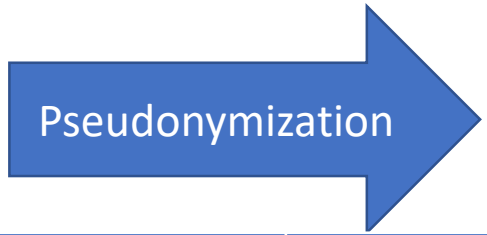
➢ The higher the risks involved in the data processing and the more likely these are to manifest, the stronger the taken security measures have to be and the more measures must be taken.

Pseudonymization

- Pseudonymisation
  - Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information
  - Additional information can be kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person
- Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.

Name	Age	Hobby
Max Mustermann	26	Football
Alice Wonderland	23	Photography

Identification via Name



Name	Pseudonym
Max Mustermann	A123
Alice Wonderland	B234

Additional Information, e.g., protected by encryption

Name	Age	Hobby
A123	26	Football
B234	23	Photography

Anonymization

- The principles of data protection should apply to any information concerning an identified or identifiable natural person.

➢ The principles of data protection (GDPR) does not apply to anonymous information

- Anonymous Data:
  - information which does not relate to an identified or identifiable natural person
  - personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable

- How to determine whether a natural person is identifiable?
  - Take into account **all reasonable means** likely to be used, e.g., such as singling out, either by the controller or by another person to identify the natural person **directly or indirectly**
  - "Reasonable Means" according to objective factors:
    - Costs and amount of time required for identification
    - Available technology at the time
    - Technological developments

Differentiation between State of Research and State of Technology!

Third Countries

- GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU
- GDPR applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to:
  - the offering of goods or services to such data subjects in the EU
  - the monitoring of their behavior as far as their behavior takes place within the EU

➢ GDPR is valid in the EU, but also outside the EU if data subjects of EU are addressed

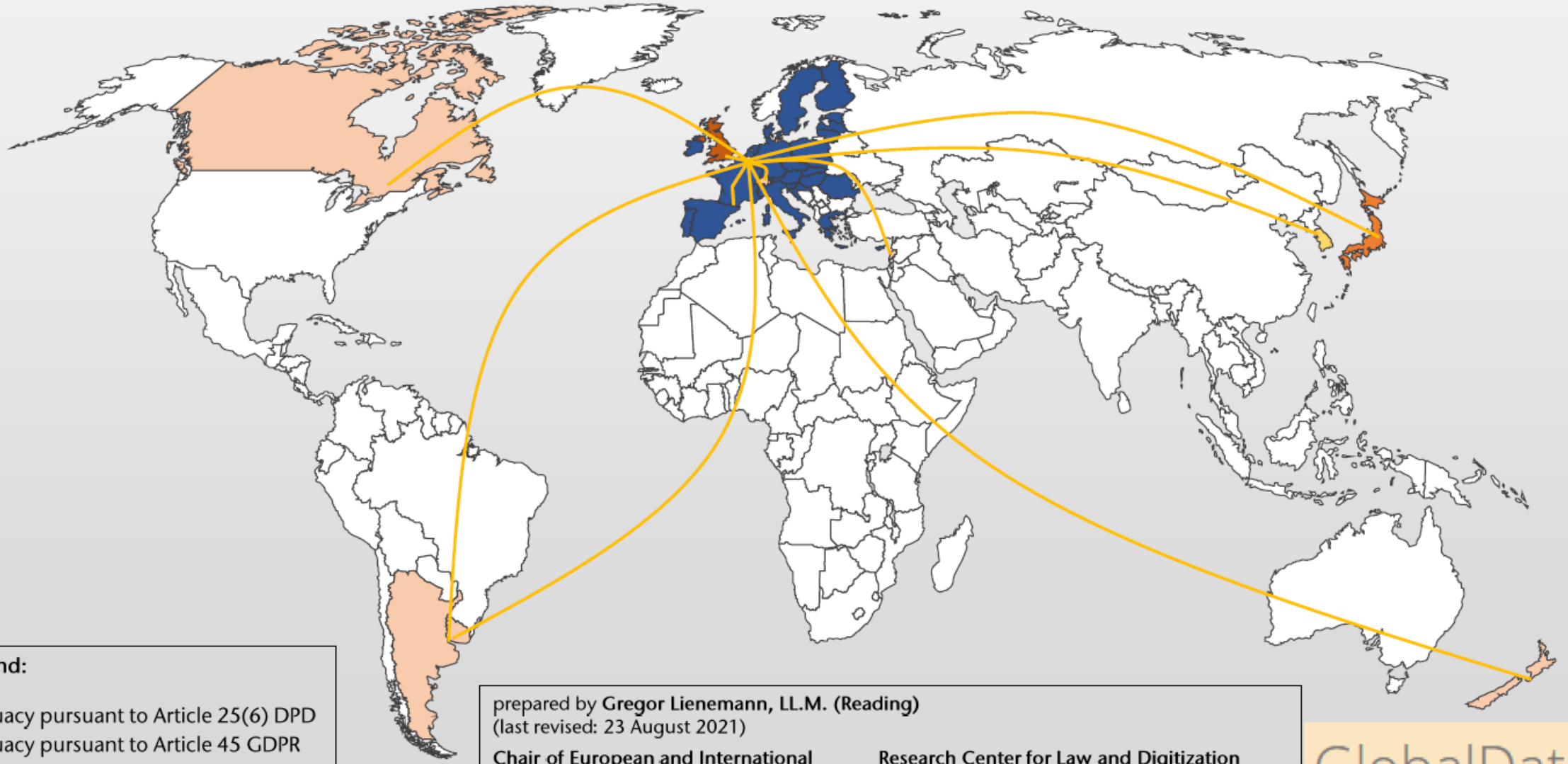
- Data Transfer to non-EU countries (Third Countries) requires additional safeguards or adequancy decision
  - Trusted Third Countries: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay
  - 2021: UK added and procedure with South Korea started

Example:
Problems of Metadata Transfer and Zoom (USA)

I01 | Adequacy Decisions by the European Commission

UNIVERSITY OF PASSAU
Faculty of Law

version 1.1



Map Legend:

- Adequacy pursuant to Article 25(6) DPD
- Adequacy pursuant to Article 45 GDPR
- Draft adequacy decision under the GDPR
- Adequacy under both GDPR & LED

prepared by **Gregor Lienemann, LL.M. (Reading)**
(last revised: 23 August 2021)

Chair of European and International Information and Data Law
Prof. Dr. Moritz Hennemann, MJur (Oxon.)

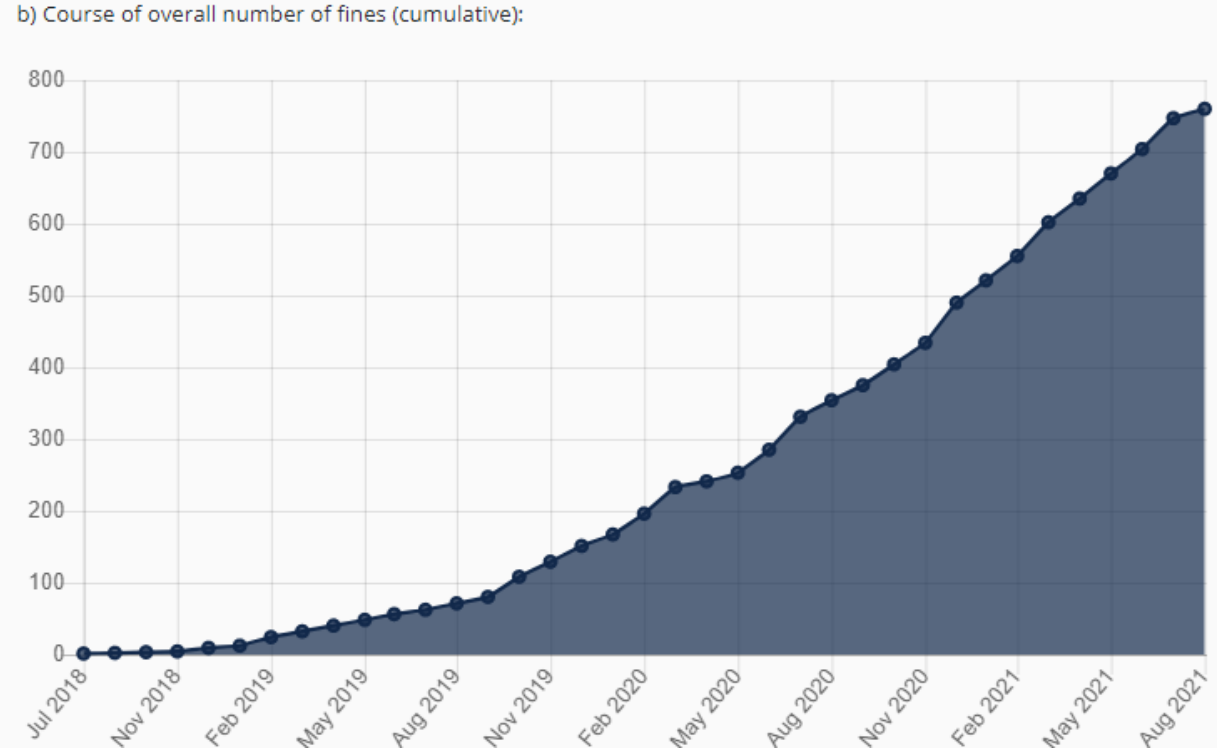
Research Center for Law and Digitization
https://www.jura.uni-passau.de/fakultaet/forschungseinrichtungen/fredi/global-data-law/

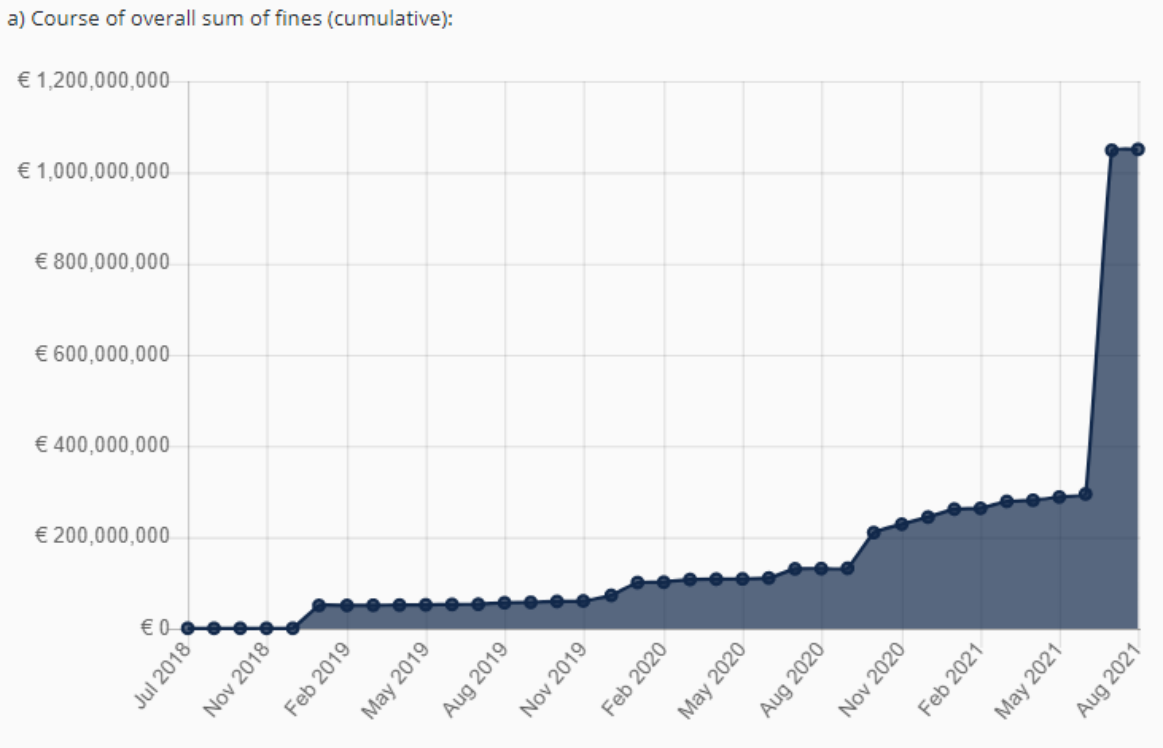
GlobalDataLaw

Fines and Penalties

- Less severe infringements: up to 10 million €, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher
- Reasons for this include:
  - Controller Responsibilities
  - Certification Body Responsibilities
  - Monitoring Body Responsibilities
- Serious infringements: up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher
- Reasons for this include:
  - Basic Principles for processing
  - Conditions for Consent
  - Data Subject Rights
  - International Data Transfer
- GDPR Fine is influence by: Gravity and nature, Intention, Mitigation, Precautionary measures, History, Cooperation, Data category, Notification, Certification and Aggravating/mitigating factors

Fines and Penalties





Statistics derived 01.09.2021, https://www.enforcementtracker.com/?insights

Fines and Penalties

Statistics: Highest individual fines (Top 10)

The following statistics shows the highest individual fines imposed to date per data controller (only top 10 fines).

	Controller	Sector	Country	Fine [€]	Type of Violation	Date
1	Amazon Europe Core S.à.r.l.	Industry and Commerce	LUXEMBOURG	746,000,000	Non-compliance with general data processing principles	16 Jul 2021
2	Google LLC	Media, Telecoms and Broadcasting	FRANCE	50,000,000	Insufficient legal basis for data processing	21 Jan 2019
3	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Employment	GERMANY	35,258,708	Insufficient legal basis for data processing	01 Oct 2020
4	TIM (telecommunications operator)	Media, Telecoms and Broadcasting	ITALY	27,800,000	Insufficient legal basis for data processing	15 Jan 2020
5	British Airways	Transportation and Energy	UNITED KINGDOM	22,046,000	Insufficient technical and organisational measures to ensure information security	16 Oct 2020
6	Marriott International, Inc	Accomodation and Hospitalty	UNITED KINGDOM	20,450,000	Insufficient technical and organisational measures to ensure information security	30 Oct 2020
7	Wind Tre S.p.A.	Media, Telecoms and Broadcasting	ITALY	16,700,000	Insufficient legal basis for data processing	13 Jul 2020
8	Vodafone Italia S.p.A.	Media, Telecoms and Broadcasting	ITALY	12,251,601	Non-compliance with general data processing principles	12 Nov 2020
9	notebooksbilliger.de	Employment	GERMANY	10,400,000	Insufficient legal basis for data processing	08 Jan 2021
10	Eni Gas e Luce	Transportation and Energy	ITALY	8,500,000	Insufficient legal basis for data processing	11 Dec 2019

Statistics derived 01.09.2021, https://www.enforcementtracker.com/?insights

2.2
Data Subject Rights

Privacy-Preservation Technologies in Information Systems

Dr. Armin Gerl

WS 2021/2022

Right of the Data Subject in the GDPR

- A data subject has certain rights related to their personal data:
  - Right to be informed about the collection and use of ones personal data
  - Right to access and receive ones data and related information
  - Right to correct and complete ones data
  - Right to delete ones data and right to be forgotten
  - Right to limit and oppose the processing of ones data
  - Right to not be subject to a decision based on automated processing of ones data
  - Right to complain to a supervisory authority

Right to be Informed

Art. 12 Transparent information, communication and modalities for the exercise of the rights of the data subject

- The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under [Data Subject Rights] relating to processing to the data subject in a **concise, transparent, intelligible and easily accessible form, using clear and plain language**, in particular for any information addressed specifically to a child.
- The information shall be provided in **writing**, or by other means, including, where appropriate, by **electronic means.**
- Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.
- Information provided and any communication and any actions taken under [Data Subject Rights] shall be provided **free of charge**.
- The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with **standardised icons** in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the **icons are presented electronically they shall be machine-readable**.

Right to be Informed

Art. 13 Information to be provided where personal data are collected from the data subject

- Art. 13 is the basis for Privacy Policies

Art. 14 Information to be provided where personal data have not been obtained from the data subject

- Art. 14 is applicable when personal data has been acquired beforehand and the data subject is addressed

Information that has to be provided for Art. 13 and 14 are basically the same (shortened):

- Contact Information on Controller and responsible DPO, Information on Data Subject Rights
- Purposes and Legal Basis for Processing
- Recipients of Personal data
- Transfers of Personal Data to a Third Country
- Data Retention Period
- Automated Decision-Making

The Privacy Paradox and Privacy Policies

Privacy Paradox

The Privacy Paradox is the observation that humans share personal information freely although they claim to worry about their privacy. Although people state in surveys that they worry on privacy they act mostly differently.

The Privacy Paradox is often used as reasoning to understand why people don't read the Privacy Policy or change their Privacy Settings

- Only a small percentage of "interested users" actually reads (parts) of the privacy policy
- Most users only activate the checkbox and go on with the registration process on the website

➢ Normal users don't have the time nor make the effort to read privacy policies, thus it may be argued that Explicit Consent and Transparency are not given

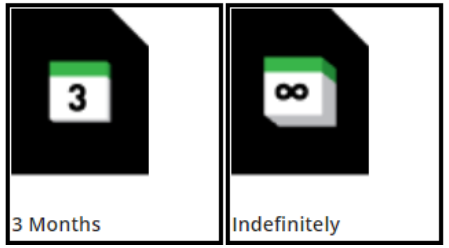
  ➢ Privacy Icons are one approach to create more Transparency

  ➢ For managing Explicit Consent and Transparency **Consent and Control User Interfaces** are proposed

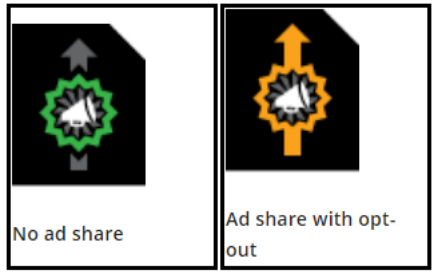
On Privacy Icons

Art. 12 “Standardised Icons”

- Privacy Policies are too long and too complex to read (TLDR), therefore there is a lack in transparency
- Privacy Icons should ease to help people to understand by providing easy and fast to understand information on what happens to your personal data
- Mozilla Privacy Icons (beta) have been one of the first well-known Privacy Icons Proposals (to the best of our knowledge)
- They covered the topics:
  - Retention Period

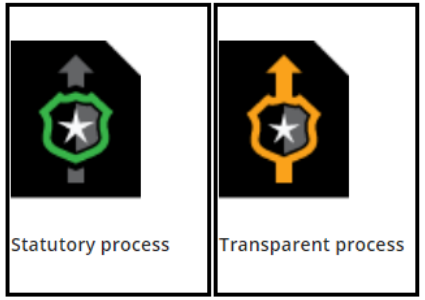


  - Ad networks



  - Third-party use

  - Law enforcement



Figures derived from https://wiki.mozilla.org/Privacy_Icons

On Privacy Icons

The idea is good but:

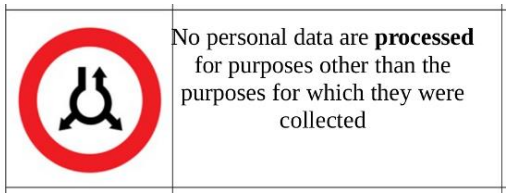
- No standardized Privacy Icon Set is in use till now

Open Questions:

- What information should be provided by the Icons? (Discussion on EU Proposal)
- How to design the Privacy Icons in a transparent way (no wrong interpretation possible)?
- Who defines and verifies that the shown Privacy Icons (and Privacy Policy) are correct?

- Additional Proposals and Examples:
  - The current version of the forthcoming EU Data Protection Regulation includes a set of privacy icons that should be used within European services and organizations
  - https://disconnect.me/icons
  - https://wiki.mozilla.org/Privacy_Icons
  - http://yale.edu/self/psindex.html
  - http://www.privacybird.org/
  - https://netzpolitik.org/2007/iconset-fuer-datenschutzerklaerungen/
  - http://knowprivacy.org/policies_methodology.html
  - The EU-funded PrimeLife project also proposed a set of privacy icons: Holtz, L. E., Zwingelberg, H., & Hansen, M. (2011). Privacy policy icons (http://link.springer.com/chapter/10.1007%2F978-3-642-20317-6_15) In Privacy and Identity Management for Life (pp. 279-285). Springer Berlin Heidelberg and Holtz, L. E., Nocun, K., & Hansen, M. (2011). Towards displaying privacy information with icons. In Privacy and Identity Management for Life (pp. 338-348). Springer Berlin Heidelberg.
  - The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services CREATe Working Paper 2014/15 (October 2014)

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



Discussion on EU Privacy Icon Proposal
https://hroy.eu/posts/encryptionEuDataIcons/

On Consent and Control UIs

Consent and Control Uis visualize the privacy policy in an interactive way:

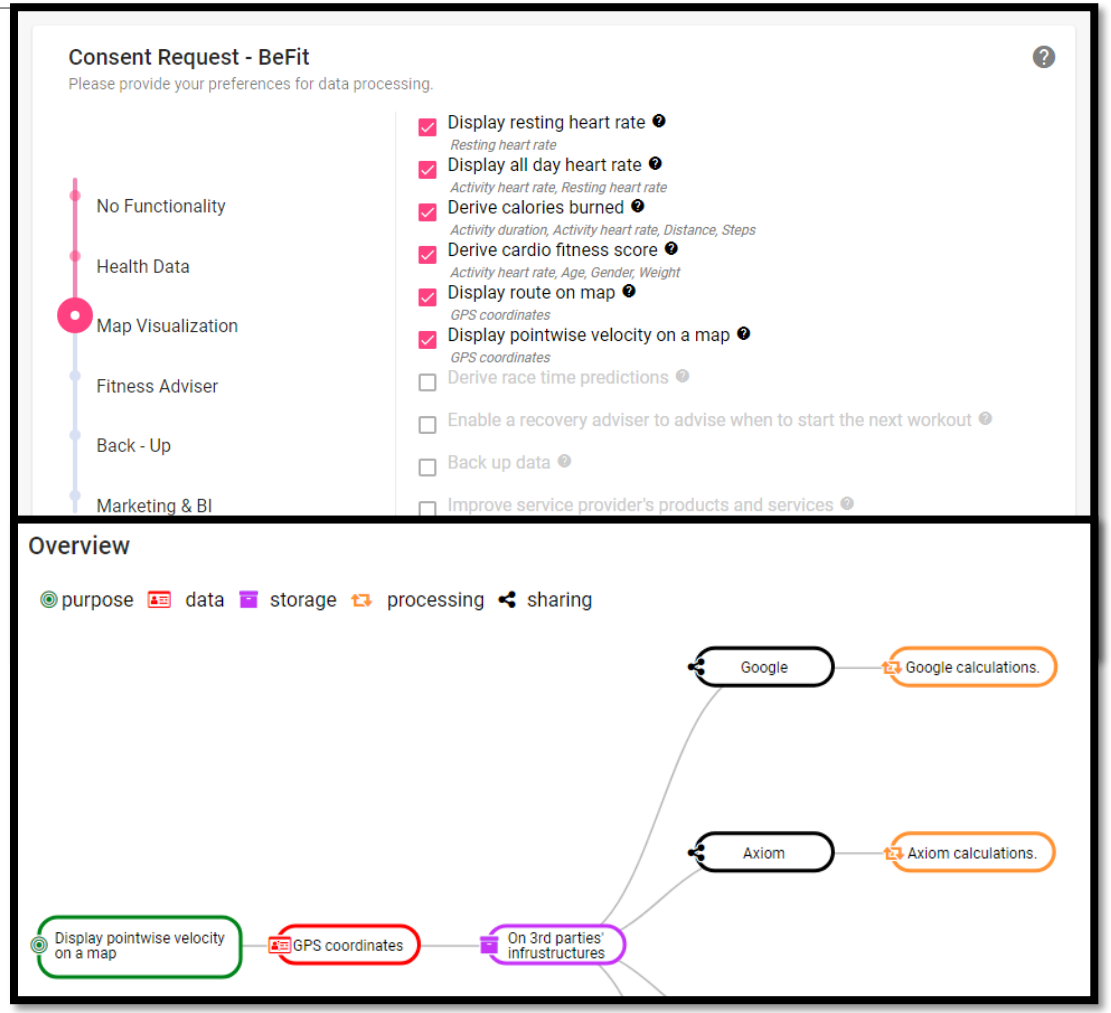
- Opt-In Choices /Checkboxes for Purposes
- Visualizations of Data Flows

Problems of this specific UI Prototype:

- Missing Information on Controller, DPO, and Data Subject Rights

In General: Complex UIs for Privacy Policies requires a machine-readable and human-readable format for Privacy Policies

➢ Privacy Languages (will be discussed later)



SPECIAL Project: Consent and Control UI Prototype 3 “CURE”, http://cr-slider.soft.cafe/en/

Right of Access

Art. 15 Right of Access by the Data Subject

- The data subject shall have the right to obtain from the controller **confirmation as to whether or not personal data concerning him or her are being processed**, and, where that is the case, **access to the personal data and the following information**:
  - the **purposes** of the processing;
  - the **categories of personal data** concerned;
  - the **recipients** or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
  - where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; [**Data Retention**]
  - [**Data Subject Rights**]
  - where the personal data are not collected from the data subject, **any available information to their source**;
  - the existence of automated decision-making, including profiling, and, at least in those cases, **meaningful information about the logic involved**, as well as the significance and the envisaged consequences of such processing for the data subject.
- The controller shall provide a **copy of the personal data undergoing processing**. Where the data subject makes the **request by electronic means** the information shall be provided in a **commonly used electronic form**.
- The right to obtain a copy shall **not adversely affect the rights and freedoms of others**.

Basically like Art. 13 and 14

Processing „Right of Access“ Requests

- “Right of Access” Requests require the Controller to authenticate, collect personal data and information on the processing of the personal information
- This information should be all available due to various documentation requirements and in the best case automatically answered, e.g., facebook
- But: Reality for most companies is that “Right of Access” Requests are handled manually!
  - Only few (2-3) requests per year
  - No standardised solutions
  - High cost for proprietary solution
- Examples:
  - Telecommunication Provider Approach
  - COVID “Right of Access” Experiment

Request to access to personal data according to Art. 15 GDPR

To Whom It May Concern:

I am hereby requesting access according to Article 15 GDPR. Please confirm whether or not you are processing personal data (as defined by Article 4(1) and (2) GDPR) concerning me.

In case you are, please, in accordance with Art. 15(3) GDPR, provide me with a copy of all personal data concerning me that you are processing, including any potential pseudonymised data on me as per Article 4(5) GDPR. I am further requesting access to the following information pursuant to Article 15(1) GDPR:
1. the purposes of the processing;
2. the categories of personal data concerned;
3. the recipients or categories of recipient to whom the personal data have been or will be disclosed;
4. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
5. where the personal data are not collected from the data subject, any available information as to their source;
6. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for me.

In case you are processing anonymised data concerning me, please not only inform me about that but also explain the procedure used in an easily understandable way.

If you are transferring my personal data to a third country or an international organisation, I request to be informed about the appropriate safeguards according to Article 46 GDPR concerning the transfer.

https://www.datarequests.org/blog/sample-letter-gdpr-access-request/

Right to Rectification

Art. 16 Right to Rectification

- The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.
- Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

➢ Companies etc. have to correct personal data!

➢ Incomplete personal data has to be completed. This may be important for applying for a bank credit and updating your information there; keyword SCHUFA! (they have to consider your current live circumstances and income and not any old information that they may not have updated).

Right to Erasure (‚right to be forgotten‘)

Art. 17 Right to erasure (‘right to be forgotten’)

- The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her **without undue delay** and the controller shall have the **obligation to erase personal data without undue delay** where one of the following grounds applies:
  - the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
  - the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;
  - the data subject objects to the processing pursuant and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant;
  - the personal data have been unlawfully processed;
- Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, **taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers** which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
- Paragraphs 1 and 2 shall not apply to the extent that processing is necessary, e.g.:
  - for exercising the **right of freedom of expression and information**
  - for **reasons of public interest in the area of public health**
  - for archiving purposes in the **public interest**, **scientific** or **historical research** purposes or statistical purposes

Right to be Forgotten Vs. The Need to Backup

Does the „Right to be Forgotten“ also affect Backups?

- Personal Data is stored in the Information Systems and as Backup
- Right to be Forgotten includes
  - personal information in email systems, in marketing and sales CRM systems,, on employee desktops/laptops, corporate social media accounts…anywhere
  - including third party data processors (Controller has to inform them)
  - and backups!?
- Identifying and removing Personal Data on backup tapes is very time consuming and costly
  - Imagine finding and deleting all instances of specific Personal Data on 50 backup tapes
- Legal Experts opinion is both pro and con Backups
  - Approach 1: Transition to Backup Systems that enable a efficient and effective implementation the DSR
    - Does not exist yet -> A problem for many hospitals and Controllers processing medical data
  - Approach 2: Authorities should include “Backups” as an exemption for the DSR

Currently no clear solution on this issue!

Right to Restriction of Processing

Art. 18 Right to restriction of processing

- The data subject shall have the right to obtain from the controller **restriction of processing** where one of the following applies:
  - the **accuracy of the personal data is contested by the data subject**, for a period enabling the controller to verify the accuracy
  - the **processing is unlawful** and the data subject opposes the erasure of the personal data
  - the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the **establishment, exercise or defence of legal claims**
  - the data subject has objected to processing pursuant to Article 21(1)
- Where processing has been restricted, such personal data shall, with the exception of storage, **only be processed with the data subject's consent** or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.
- A data subject who has obtained restriction of processing **shall be informed by the controller before the restriction of processing is lifted**.

Right to Data Portability

Art. 20 Right to data portability

- The data subject shall have the **right to receive the personal data** concerning him or her, which he or she has provided to a controller, **in a structured, commonly used and machine-readable format** and have the **right to transmit those data to another controller** without hindrance from the controller to which the personal data have been provided, where:
  - the processing is **based on consent** pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a **contract** pursuant to point (b) of Article 6(1); and
  - the **processing is carried out by automated means**.
- In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the **right to have the personal data transmitted directly from one controller to another, where technically feasible**.
- The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Right to Data Portability

Art. 20 Right to data portability

- **„ right to have the personal data transmitted directly from one controller to another, where technically feasible”**
- Export to Data Subject in electronic format is “easy”
- Import from Data Subject to new Controller is manageable with manual work
- Automatic Exchange between Controller is hard
- (Personal) Data is stored in different ways
  - semantic (name <-> prename, surname)
  - syntactic (MySQL <-> PostgreSQL, XML <-> JSON)

➢ Common Data Portability Exchange Format is required!

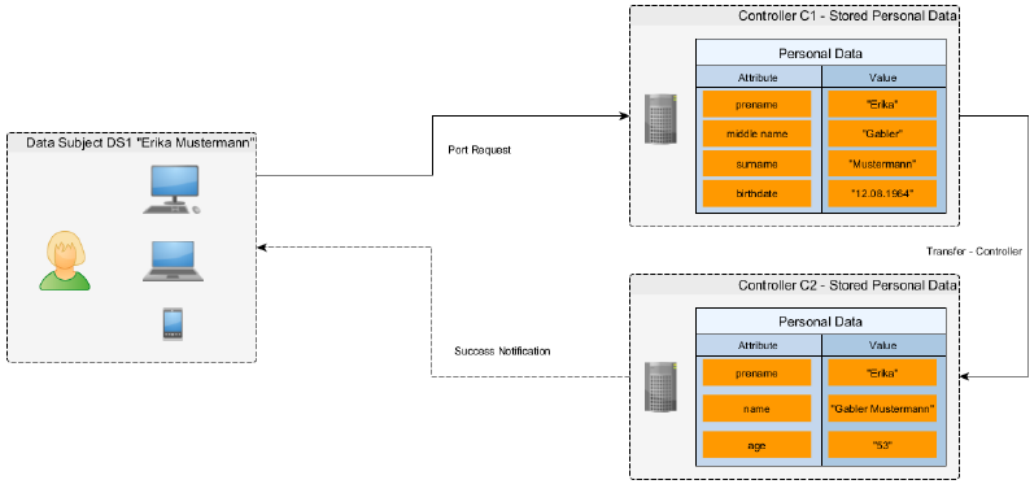
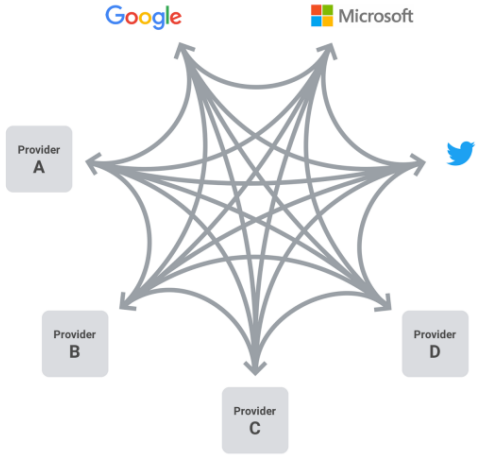


Figure 2: Controller Negotiation scenario showing the Data Subject DS1 initializing the Transfer of its personal data from Controller C1 to Controller C2 and receiving a success notification from Controller C2.

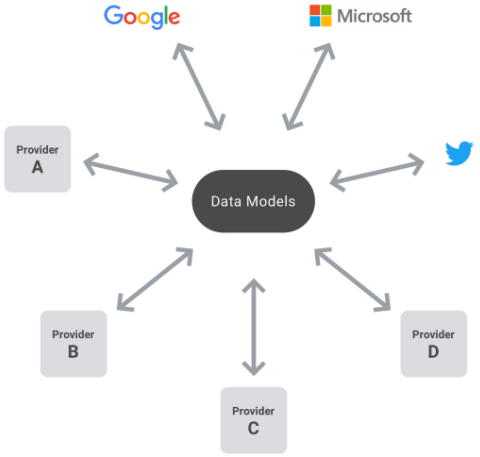
A. Gerl, D. Pohl., The Right to data portability between legal possibilities and technical boundaries, *Practical Implementation of the Right to Data Portability- Legal, Technical and Consumer-Related Implications, 2017, 208-224.*

Data Transfer Project

- Allows data transfer between any two providers using the provider's existing authorization mechanism, and allow each provider to maintain control over the security of their service
- Key Components:
  - **Data Models** are the canonical formats that establish a common understanding of how to transfer data.
  - **Adapters** provide a method for converting each provider's proprietary data and authentication formats into a form that is usable by the system.
  - **Task Management Library** provides the plumbing to power the system
- Established 2018
- Contributors:



Without the DTP
Each provider has to build and maintain Adapters for every other provider's proprietary APIs and, potentially, data formats



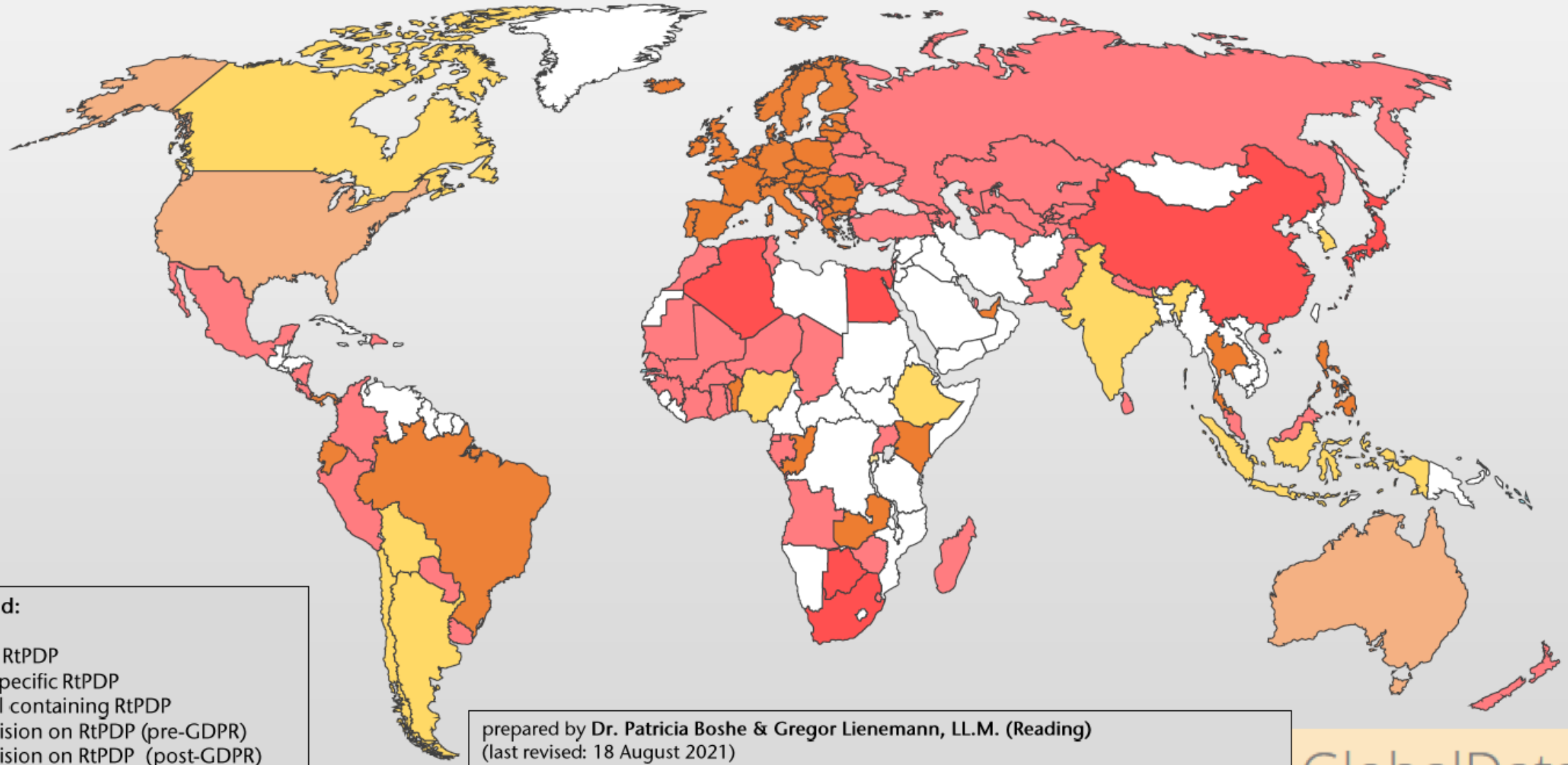
With the DTP
Each provider only has to build and maintain an API that supports the DTP Data Models, which are based on standard formats where available

https://datatransferproject.dev/dtp-overview.pdf

R01 | Right to Personal Data Portability

UNIVERSITY OF PASSAU
Faculty of Law

version 1.1



Map Legend:

- General RtPDP
- Sector-specific RtPDP
- Draft bill containing RtPDP
- No provision on RtPDP (pre-GDPR)
- No provision on RtPDP (post-GDPR)
- No stand-alone data protection law

prepared by **Dr. Patricia Boshe & Gregor Lienemann, LL.M. (Reading)**
(last revised: 18 August 2021)

Chair of European and International Information and Data Law
Prof. Dr. Moritz Hennemann, MJur (Oxon.)

Research Center for Law and Digitization
https://www.jura.uni-passau.de/fakultaet/forschungseinrichtungen/fredi/global-data-law/

GlobalDataLaw

Right to Object

Art. 21 Right to object

- The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on **public interest** or **legitimate interest of the controller**, including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
- Where personal data are processed for **direct marketing purposes**, the data subject shall have the **right to object at any time** to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
- Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
- At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 **shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information**.
- In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her **right to object by automated means** using technical specifications.
- Where personal data are processed for **scientific or historical research purposes or statistical purposes** pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the **right to object to processing of personal data** concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Section in Privacy Policy

Automated individual decision-making, including profiling

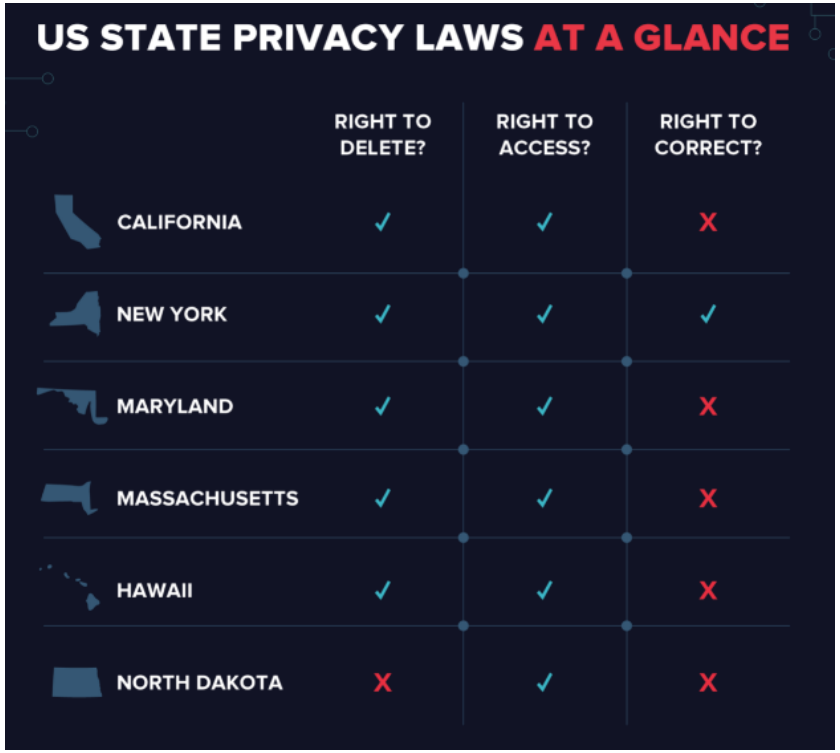
Art. 22 Automated individual decision-making, including profiling

- The data subject shall have the **right not to be subject to a decision based solely on automated processing**, **including profiling**, which produces legal effects concerning him or her or similarly significantly affects him or her.
- Paragraph 1 shall not apply if the decision:
  - is necessary for entering into, or performance of, a **contract** between the data subject and a data controller;
  - is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
  - is based on the **data subject's explicit consent**.
- In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the **right to obtain human intervention on the part of the controller**, to express his or her point of view and to contest the decision.

Privacy in USA, China, Brazil

- 1996 USA: **Health Insurance Portability and Accountability Act (HIPAA)**
- 2000 USA: **Children's Online Privacy Protection Act (COPPA)**
- 2020 USA/California: **California Consumer Privacy Act (CCPA)**
  - The right to know about the personal information a business collects about them and how it is used and shared;
  - The right to delete personal information collected from them (with some exceptions);
  - The **right to opt-out** of the sale of their personal information; and
  - The right to non-discrimination for exercising their CCPA rights.

➢ Clear influence from the GDPR

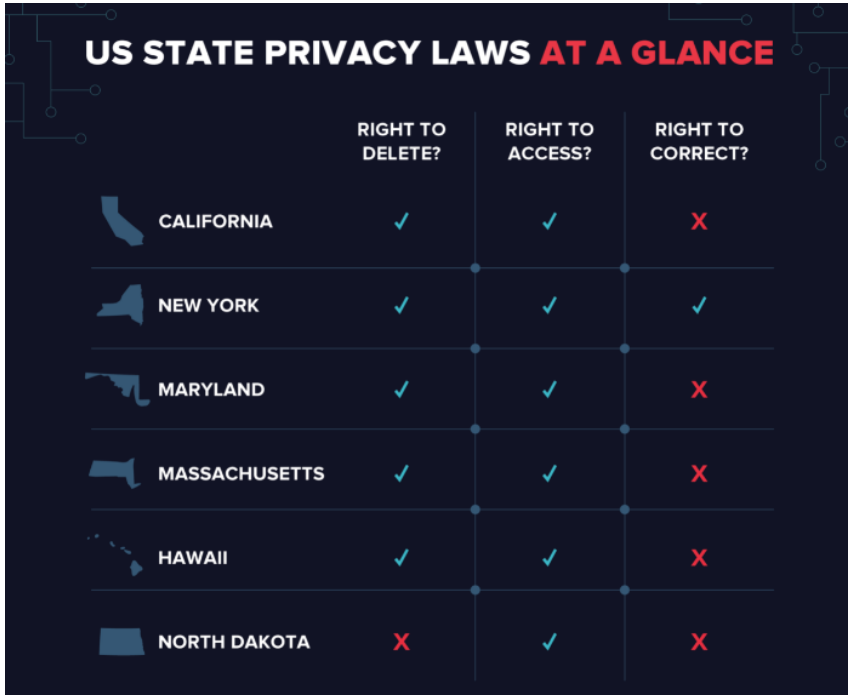


https://www.varonis.com/blog/us-privacy-laws/

Privacy in USA, China, Brazil

- 1996 USA: **Health Insurance Portability and Accountability Act (HIPAA)**
- 2000 USA: **Children's Online Privacy Protection Act (COPPA)**
- 2020 USA/California: **California Consumer Privacy Act (CCPA)**
  - The right to know about the personal information a business collects about them and how it is used and shared;
  - The right to delete personal information collected from them (with some exceptions);
  - The **right to opt-out** of the sale of their personal information; and
  - The right to non-discrimination for exercising their CCPA rights.

➢ Clear influence from the GDPR



https://www.varonis.com/blog/us-privacy-laws/

Privacy in China

- Nov. 1, 2021, China: Personal Information Protection Law (PIPL)
  - Goals:
    - protect the rights and interests of individuals
    - regulate personal information processing activities
    - facilitate reasonable use of personal information
  - Strong resemblance to the GDPR
    - PIPL has certain substantive obligations that differ from the GDPR
    - GDPR has obligations that are not included in the PIPL
  - Additional Legal Basis for Processing:
    - Necessary to enter into or perform a contract to which the individual is a party, or where necessary to conduct **human resources management** according to lawfully formulated **internal labor policies and lawfully concluded collective labor contracts**.
    - Necessary to perform legal responsibilities or obligations.
    - Necessary to respond to a public health emergency, or in an emergency to protect the safety of individuals' health and property.
    - To a reasonable extent, for **purposes of carrying out news reporting and media monitoring** for public interests.
    - Processing of personal information that is **already disclosed by individuals or otherwise lawfully disclosed**, within a reasonable scope in accordance with the PIPL.
    - Other circumstances as required by laws.

Rights under the GDPR	Rights under the PIPL
Right to information	✓
Right to access	✓
Right to correction/rectification	✓
Right to erasure	✓
Right to object to and restrict the processing of an individual's data	✓
Right to data portability	✓ (but needs to satisfy conditions stipulated by the Cyberspace Administration of China)
Right not to be subject to automated decision-making	✓
Right to withdraw consent	✓
Right to lodge a complaint with the regulator	✓

https://www.insideprivacy.com/data-privacy/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/

2.3
Privacy Policies and Privacy Languages

Privacy-Preservation Technologies in Information Systems

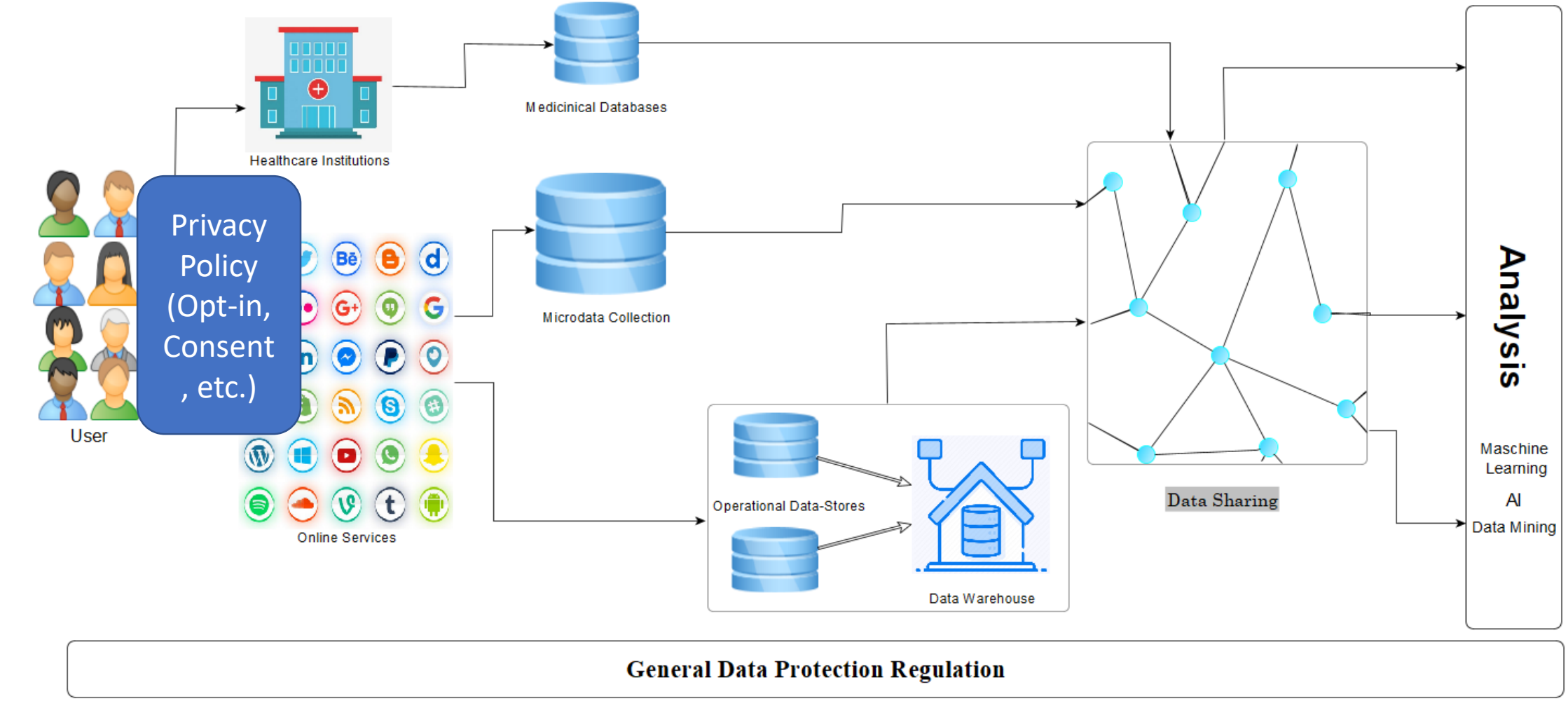
Dr. Armin Gerl

WS 2021/2022

Privacy Policies

- Art. 12 and Art. 13 GDPR define the required information in the Privacy Policy
- Privacy Policy is the “contract” between the User (Data Subject) and Service Provider (Controller) on how to use the personal data
- Transparency Requirements <-> Privacy Paradox

Privacy Policies in the Data Life-Cycle



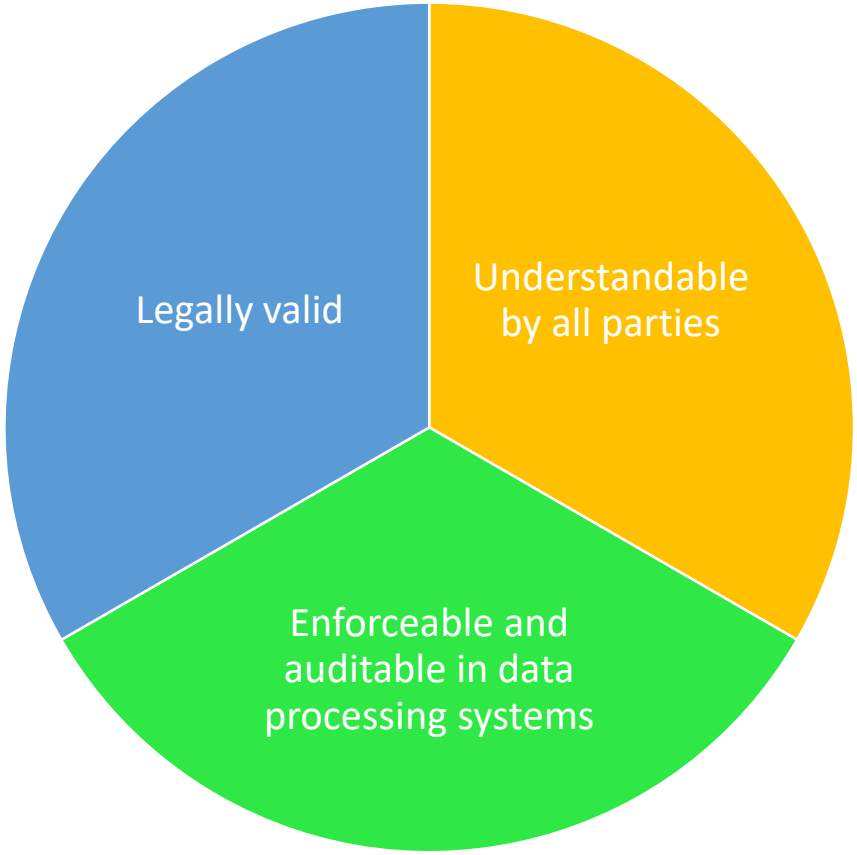
3 Facets of Privacy Policies

Privacy Policies must be…

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

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

- **Enforceable and auditable in data processing systems**
  - (Automatically) Enforce rules/consent of Privacy Policy
  - (Automatically) Detect violation of Privacy Policy
  - ➢ Machine-readable Privacy Policies -> Privacy Languages

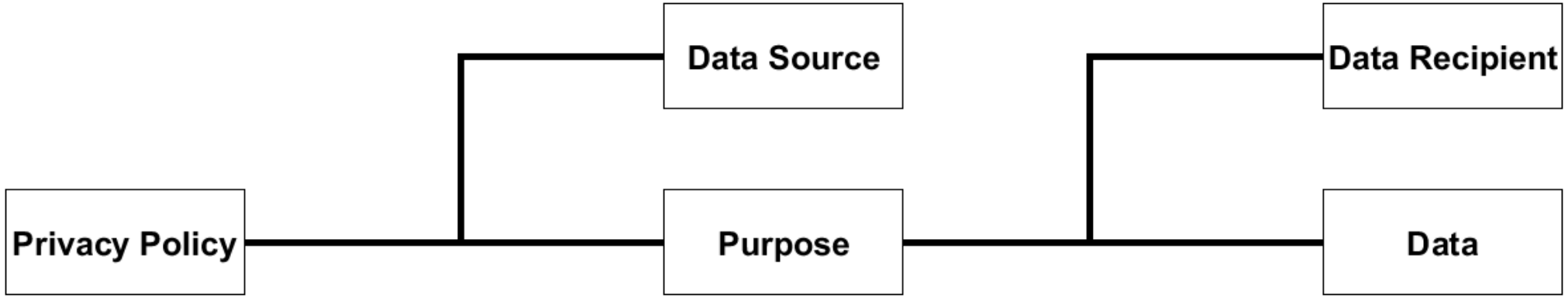


Victor Morel, Raúl Pardo. SoK: Three Facets of Privacy Policies. *Workshop on Privacy in the Electronic Society*, Nov 2020, Virtual, France. ⟨hal-02267641v4⟩

Privacy Language

- A Privacy Language can be denoted as a specialization of a domain specific language (DSL) in the context of privacy
- Privacy Languages specialise in modelling/representing legal privacy policies

Core structure and elements of a privacy policy.



Further Specialisations:

- Access Control Language
- Privacy Preference Language

Requirements (R) for a Privacy Language

- R*1:* The base structure of a policy language has to match the structure of legal privacy policies.
- R*2:* A privacy language has to comply with the intended legal framework.
- R*3:* A privacy language has to be human-readable.
- R*4:* A privacy language has to enable purpose-based access control.
- R*5:* A privacy language has to define de-identification methods.
- R*6:* A privacy language has to enable provenance.

Legally Valid

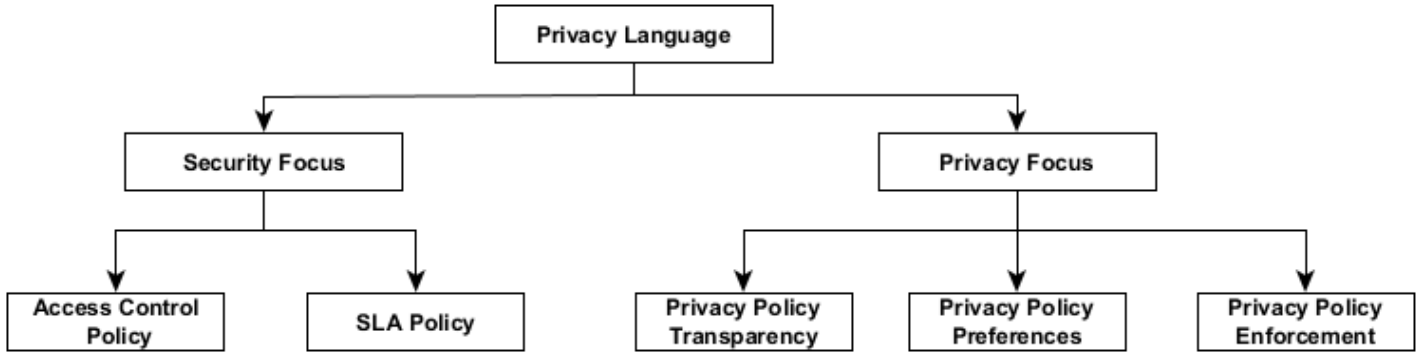
Understandable

Enforceable & Auditable

Taxonomy of Privacy Languages

Security Focus:

- **Access Policies:** Formulate rules that define which entities can access which resources, such that only authorized accesses are possible.
- **Service Level Agreement (SLA) Policy** languages: Formulate agreements or contracts for B2B processes.



Privacy Focus:

- **Privacy Policy Transparency**: Specialize in informing about the services' privacy policy.
- **Privacy Policy Preferences**: Expression of the users' privacy preferences regarding services.
- **Privacy Policy Enforcement**: Implementation and enforcement of privacy, either in terms of the users' privacy preferences or services' privacy policies.

Taxonomy of Privacy Languages

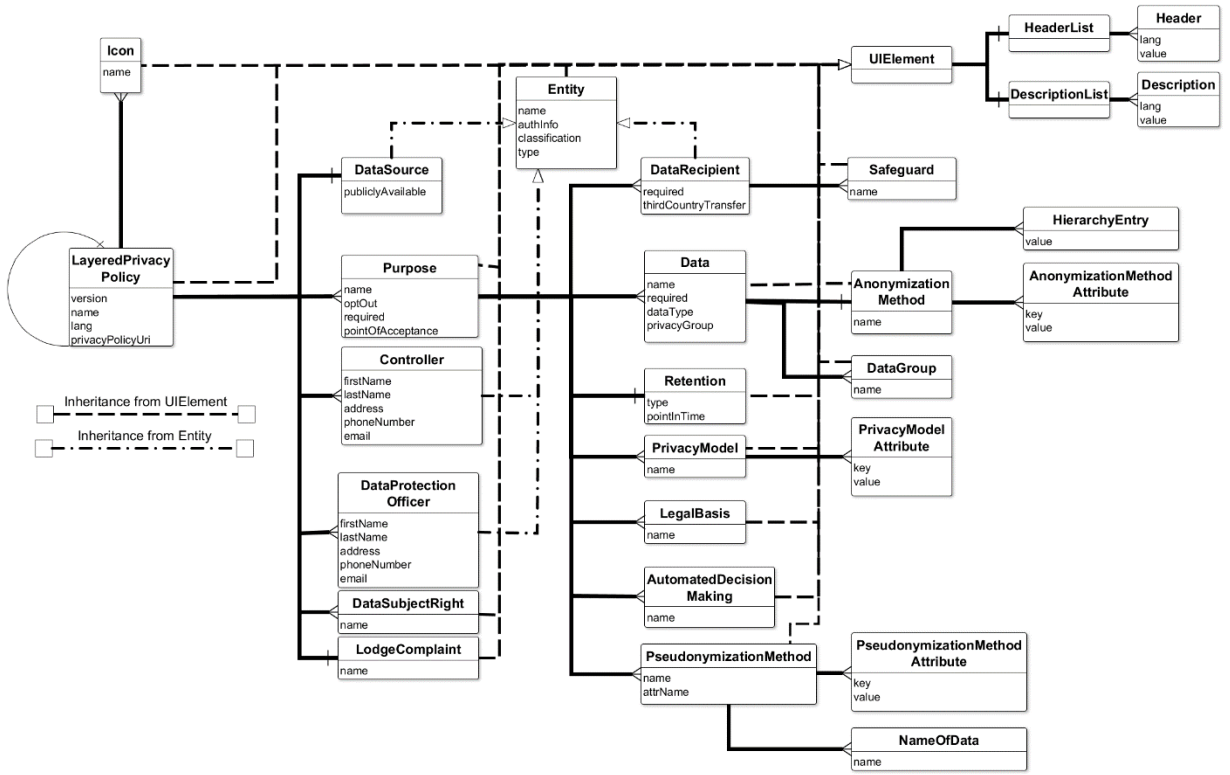
- Well-covered Requirements:
  - **R1** *Privacy Policy Structure*
  - **R4** *Access Control*
- Underrepresented Requirements:
  - **R5** *De-identification Capabilities*
  - **R6** *Provenance*

Category	Privacy Language	Privacy Policy Structure	Legal Compliance (GDPR)	Human-readability	Access Control	De-identification Capabilities	Provenance
Access Control Policy	XACL [2]	X	-	-	(X)	-	-
	Ponder [3]	(X)	-	-	(X)	-	-
	Rei [4]	(X)	-	-	(X)	-	-
	Polymer [5]	(X)	-	-	-	-	-
	SecPAL [6]	(X)	-	-	(X)	-	-
	AIR [7]	X	-	X	(X)	-	-
	XACML [8]	X	-	-	(X)	-	-
	ConSpec [9]	(X)	-	-	(X)	-	-
SLA Policy	SLAng [10] [11]	X	(X)	-	-	-	-
	USDL [12]	(X)	(X)	X	-	-	-
Privacy Policy Transparency	P3P [13]	X	(X)	(X)	X	-	-
	CPExchange [14]	X	(X)	(X)	X	-	-
Privacy Policy Preferences	APPEL [15]	X	-	-	-	-	-
	Xpref [16]	X	-	-	-	-	-
	XPACML [17]	X	(X)	-	X	-	-
	S4P [18] [19]	(X)	-	-	X	-	-
	YaPPL [20]	(X)	(X)	X	X	-	-
Privacy Policy Enforcement	DORIS [21]	(X)	-	-	X	-	-
	E-P3P [22]	(X)	(X)	-	X	-	-
	EPAL [23]	X	-	-	X	-	-
	PPL [24]	X	(X)	X	X	-	(X)
	SPECIAL [25] [26]	X	(X)	X	X	(X)	(X)
	P2U [27] [28]	X	(X)	-	X	-	-
	PrivPolicy [29}	X	(X)	-	X	(X)	-

X : Fulfilled | (X) : Partially Fulfilled | - : Not Fulfilled

Layered Privacy Language (LPL)

- Privacy Language that intends to incorporate all given requirements:
  - R*1:* The base structure of a policy language has to match the structure of legal policies.
  - R*2:* A privacy language has to comply with the intended legal framework.
  - R*3:* A privacy language has to be human-readable.
  - R*4:* A privacy language has to enable purpose-based access control.
  - R*5:* A privacy language has to define de-identification methods.
  - R*6:* A privacy language has to enable provenance.
- Generic formalization using mathematical tupels
- Can be realized in XML, JSON, or other common formats
- Adaptation of previous “best practices” for the design and extending it by R5 and R6 requirements

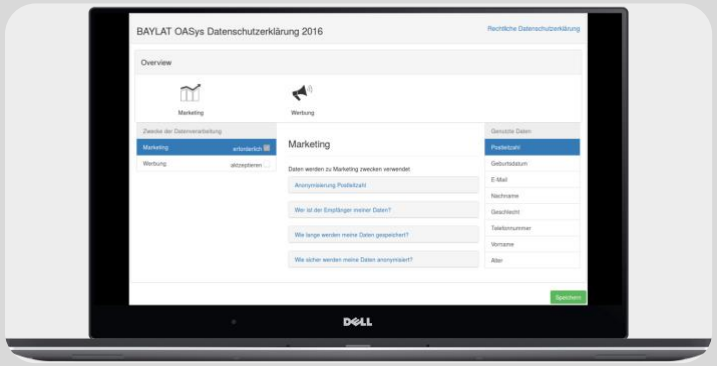


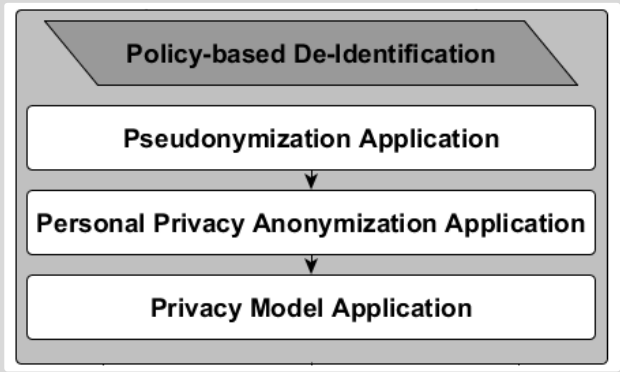
Layered Privacy Language (LPL)

Personalization of Privacy Policy

Layered Privacy Language (LPL)

Policy-based De-Identification

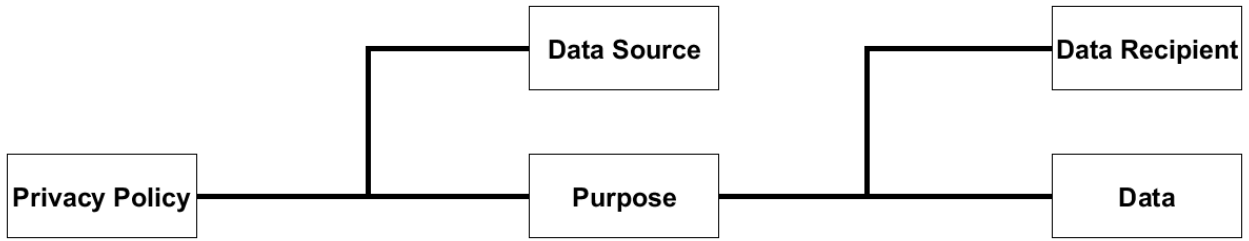




R1: Privacy Policy Structure

R*1:* The base structure of a policy language has to match the structure of legal privacy policies.

- **Privacy Policy**: Denotes all purposes of processing of personal data of an individual
- **Data Source**: The individual from which the personal data originates
- **Data Recipient**: The entity which processes the personal data
- **Purpose**: Denotes the reason and extent of the processing of personal data
- **Data**: Denotes the personal data that is subject to processing
- A Privacy Policy denotes the processing of personal **Data** of a **Data Source** for **Purposes** by **Data Recipients**
  - A privacy policy regulates what personal information is processed by whom for which reason



Core structure and elements of a privacy policy.

R2: Legal Framework Compliance

R2: A privacy language has to comply with the intended legal framework.

- **Privacy Language has to represent legally required information:**

Requirements GDPR Art. 13	
Clear and Plain Language	Written or Electronic Information
Data Subject Rights Realization	Third Country Transfer
Standardised Icons	Storage Period
Contact Details of Controller	Information: Data Subject Rights
Contact Details of Data Protection Officer (DPO)	Information: Withdraw Consent
Purpose and Legal Basis	Information: Lodge a Complaint
Legitimate Interest	Information: Required Data
Categories of Personal Data	Source of Personal Data
Recipients of Personal Data	Automated Decision-Making

Legal Framework = GDPR for this lecture

R2: Legal Framework Compliance

R2: A privacy language has to comply with the intended legal framework.

Legal Framework = GDPR for this lecture

Privacy Language has to model information to allow Enabling/Creation of Processes to implement Data Subject Rights:

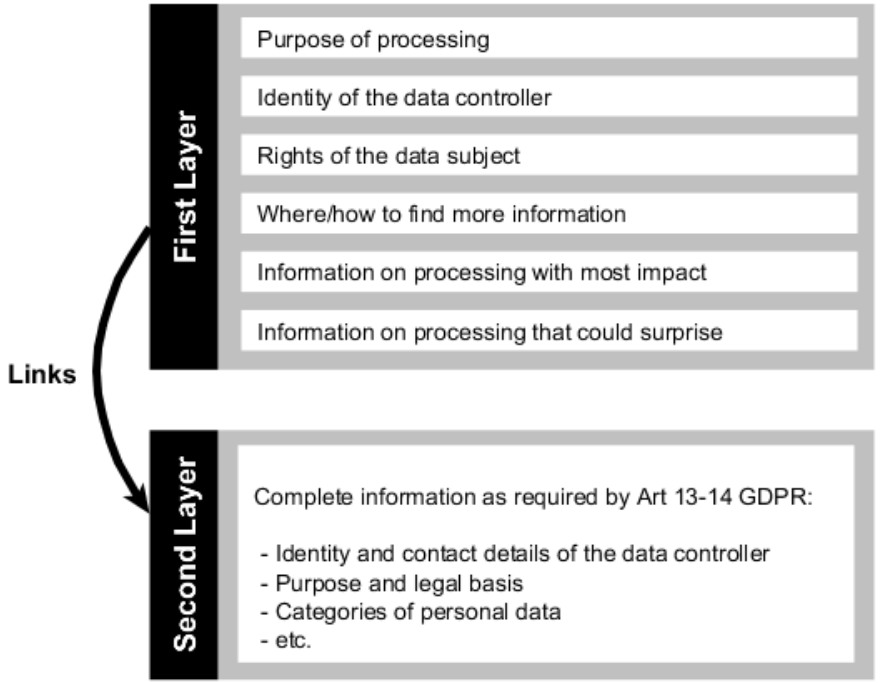
- Trivial
  - Right of Access (Store Pointers to Data)
- Deep Integration in Controller Prozesses
  - Right to Rectification
  - Right to Erasure
  - Right to Restriction of Processing
  - Right to Object
- Global Standardization (Hard Problem)
  - Right to Data Portability

Data Subject Rights
Right of Access
Right to Rectification
Right to Erasure
Right to Restriction of Processing
Notification Obligation
Right to Data Portability
Right to Object
Automated Individual Decision-making

R3: Human-Readability

R*3:* A privacy language has to be human-readable.

- The textual representation of the privacy policy shall facilitate the user to understand its contents
  - ❖ A privacy language has to define human-readable text
  - ❖ How the text is written is not defined by the privacy language
- Transparency and Understandability Dimensions (Bertino et al.):
  - Record Transparency: What is collected by whom?
  - Use Transparency: What is the data used for?
  - Disclosure and Data Provisioning Transparency: Is the data transferred or sold?
  - Algorithm Transparency: What algorithms used for automated decisions?
  - Law and Policy Transparency: Which laws and rights apply?
- Information Representation Methods
  - Layered Approach
  - Privacy Icons
  - Consent and Control UIs



Visualization of the Layered approach as proposed by the Article *29* Working Party

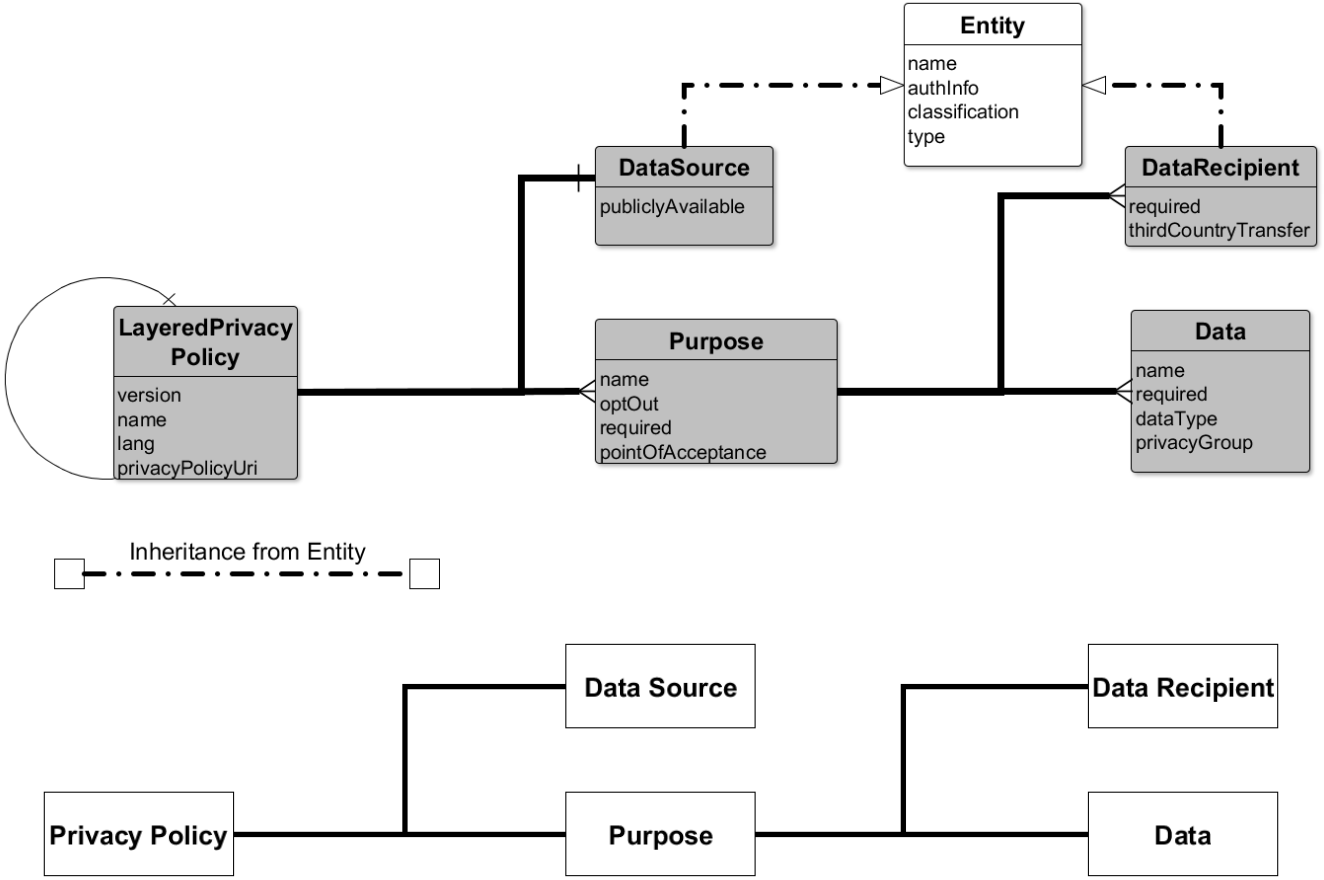
R1-R3: Layered Privacy Language

R*1:* The base structure of a policy language has to match the structure of legal privacy policies.

Core Structure

- The root-element of LPL is the LayeredPrivacyPolicy-element, which represents a legal privacy policy
- The DataSource-element represents the entity granting the rights to process data
- The DataRecipient-element represents the entity receiving the rights to process data
- The Purpose-element represents the purpose of the processing
- The Data-element represents a data field

➢ A LayeredPrivacyPolicy has 1 DataSource and n Purposes, each Purpose has n DataRecipients and n Data

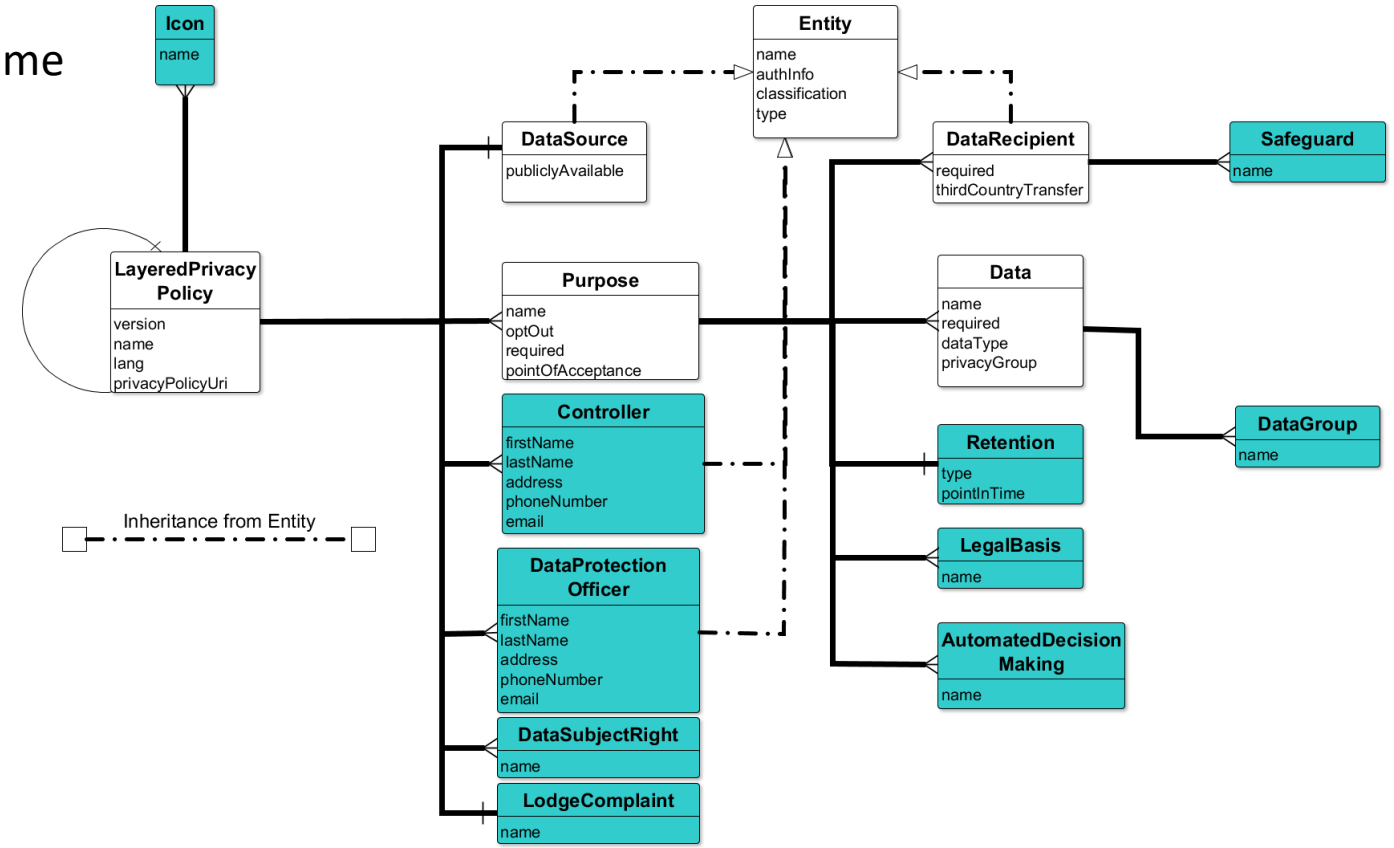


R1-R3: Layered Privacy Language

R2: A privacy language has to comply with the intended legal framework.

- Required information modelled as elements or integrated as attributes in given elements
- Data Subject Rights realization enabled, although some open issues have to be addressed/implemented

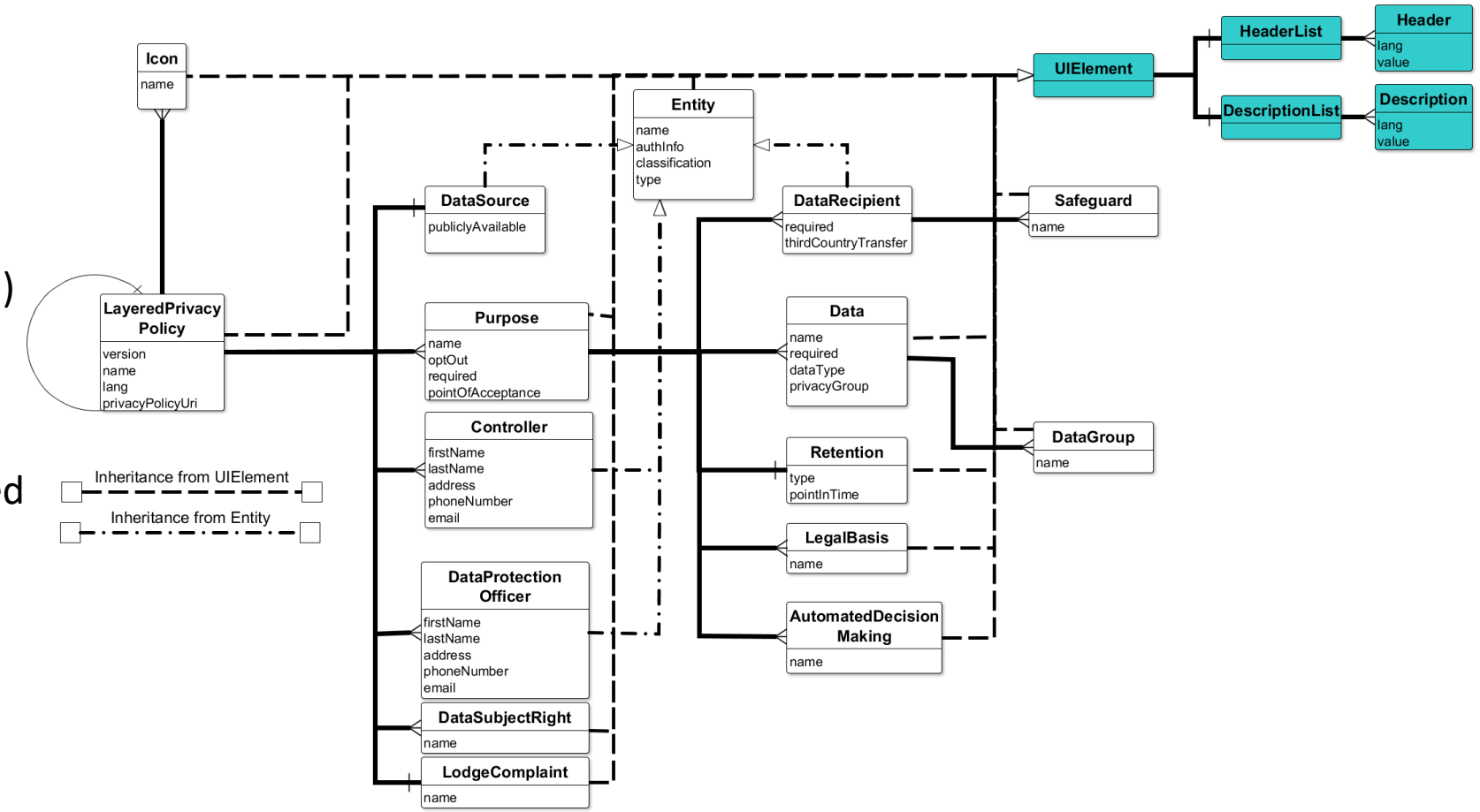
Standardised Icons	*Icon* i
Contact Details of Controller	*Controller* c
Contact Details of DPO	*DataProtectionOfficer* dpo
Purpose and Legal Basis	*Purpose* p, *LegalBasis* lb
Legitimate Interest	*LegalBasis* lb
Categories of Personal Data	*DataGroup* dg
Recipients of Personal Data	*DataRecipient* dr
Third Country Transfer	*DataRecipient* dr, *Safeguard* sg
Storage Period	*Retention* r
Information: Data Subject Rights	*DataSubjectRight* dsr
Information: Withdraw Consent	*Purpose* p
Information: Lodge a Complaint	*LodgeComplaint* lc
Information: Required Data	*Data* d
Source of Personal Data	*DataSource* ds
Automated Decision-Making	*AutomatedDecisionMaking* adm



R1-R3: Layered Privacy Language

R*3:* A privacy language has to be human-readable.

- Most elements inherent from UIElement, enabling a “Header” and “Description”
  - Human-readable Text
  - Multilingual-Support (lang = “en”)
- Privacy Icons can be set for LayeredPrivacyPolicy
  - Officially supported Icons required
- Layered Approach can easily realized via UIs visualizing the XML/JSON and enabling personalization



R4: Access Control

R*4:* A privacy language has to enable purpose-based access control.

- Communication Privacy Management (CPM) theory:
  - "privacy is perceived as a range from complete openness to complete closeness"
  - Not only completely "open" or "closed", but also everything between
- Fine-grained Access Control that considers
  - Data Source (each individual User)
  - Data Recipient (Service Provider)
  - Data (or parts or derivate of data)
  - Purpose
  - (Optional) Additional Conditions

Authentication

Authorization

- "Classical" Access Control Approaches:
  - Access Control Lists (ACLs)
  - Role-based Access Control (RBAC)
  - Attribute-based Access Control (ABAC)

Alice allows Online Shop B to use her **address data** for the **Purpose "Billing and Shipping"**, but only agrees to usage of the "state" for the usage for the **Purpose "Advertisement"**

See Chapter 5 for more details on Purpose-based Access Control!

R5: De-identification

R*5:* A privacy language has to define de-identification methods.

- De-identification Methods
  - Methods applied on data (-sets) to preserve Anonymity or Privacy
  - Anonymity: “Hide the identity of the user”
  - Privacy: “Hide the correlation between personal data and user”
- A privacy language has to be able to define methods to preserve anonymity and/or privacy that have to be enforced
- Typical Methods:
  - Generalization/Suppression: Chapter 3
  - Privacy Models: Chapter 4
  - Pseudonymization: Chapter 5

Anonymity is when you *want* people to see what you do, just not that it’s you doing it.

Example: You want to blow the whistle on abuse of power or other forms of crime in your organization without risking career and social standing in that group, which is why we typically have strong laws that protect sources of the free press. You could also post such data anonymously online through a VPN, the TOR anonymizing network, or both.

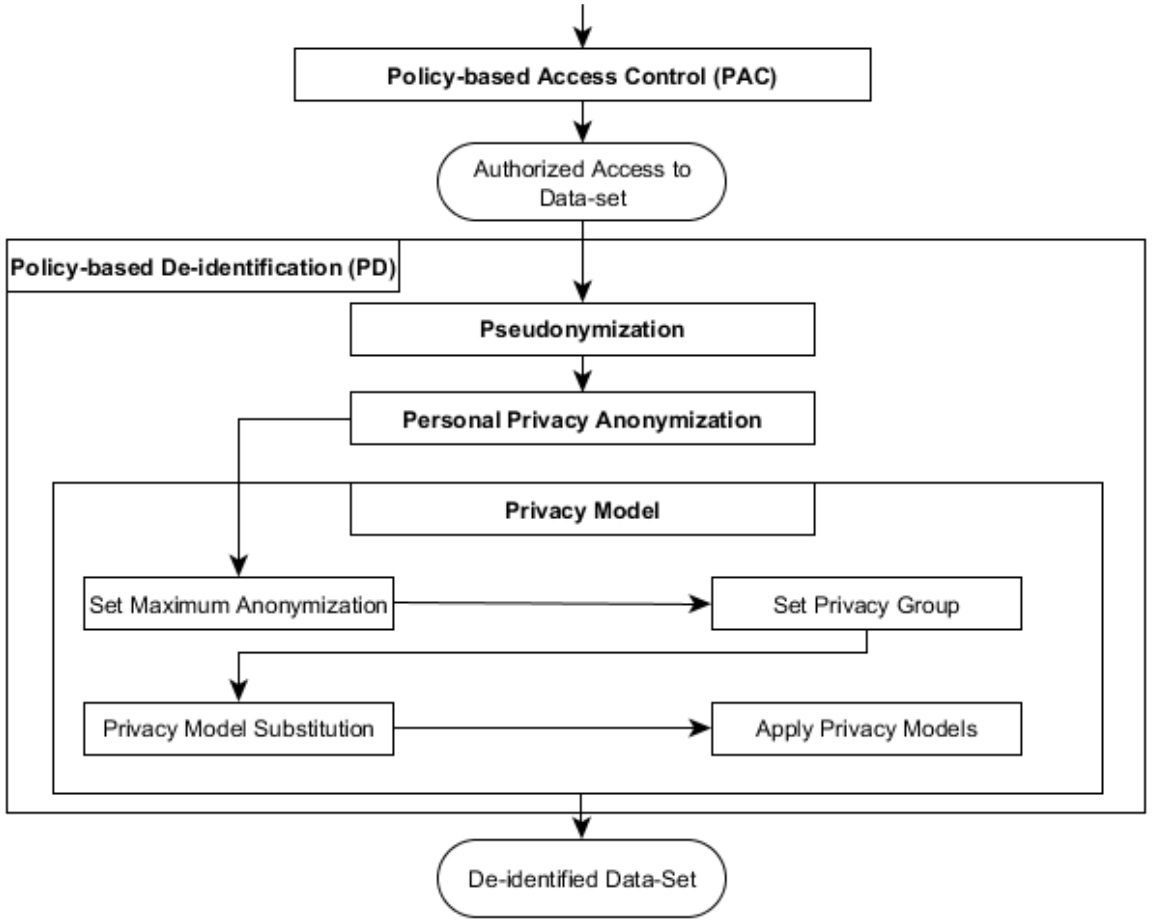
Privacy is the ability to keep some things to yourself.

Example: I lock the door when I go to the men’s room, because I want to keep the activity there to myself.

De-identification in LPL

R*5:* A privacy language has to define de-identification methods.

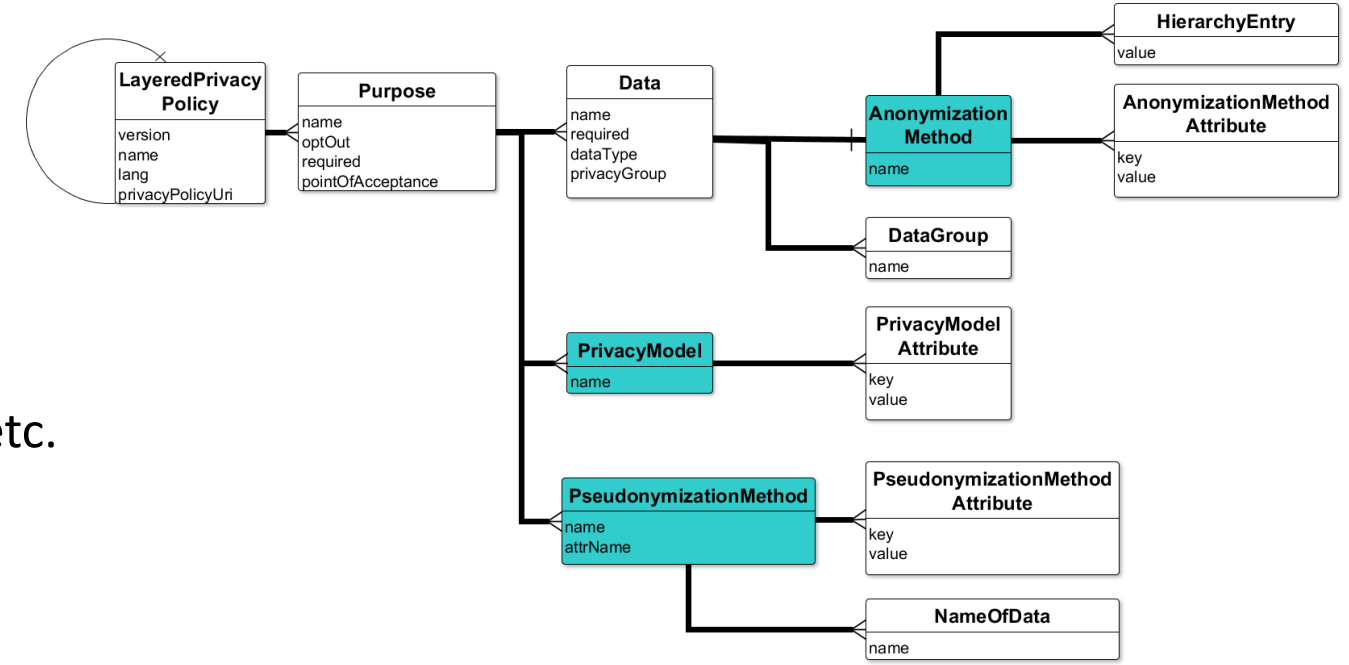
- LPL extends the authentication and authorication (compare XACML) with Policy-based De-identification process (PD)
- PD applies de-identification techniques in following order
  - Pseudonymization
  - Personal Privacy Anonymization (Localized Anonymization)
  - Privacy Model(s) on Data-Set



De-identification in LPL

Depending on **Purpose**

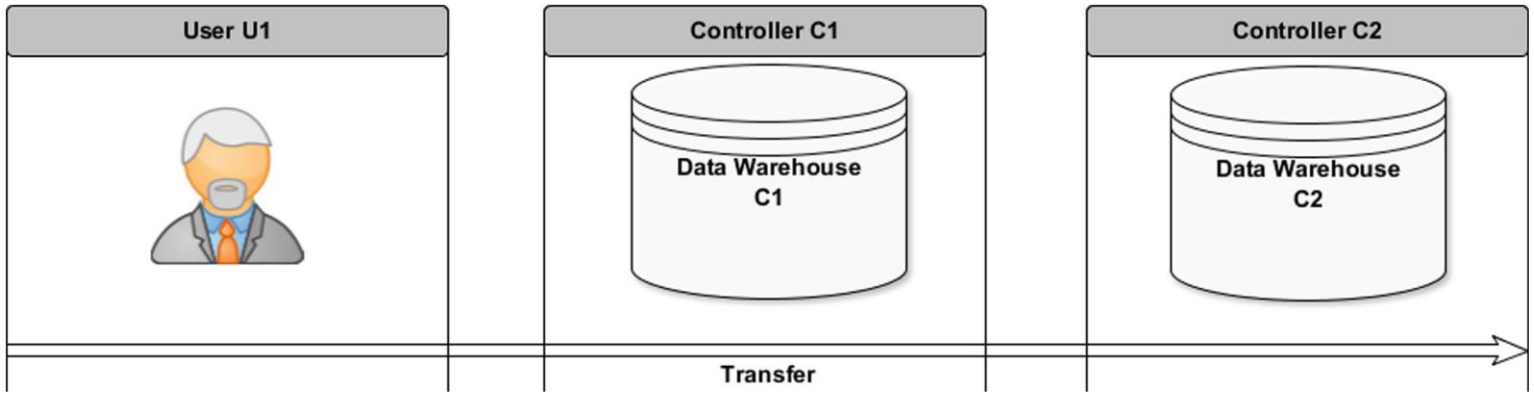
- Pseudonymization (Lokal)
  - **PseudonymizationMethod** defines Method
  - **NameOfData** defines target Attribute
- Personal Privacy Anonymization (Lokal) (Localized Anonymization)
  - **AnonymizationMethod** defines Method for **Data**
  - E.g., Suppression, Generalization, Deletion, etc.
- Privacy Model (Data-Set)
  - **PrivacyModel** defines Method
  - E.g., k-Anonymity, l-Diversity, etc.



R6: Provenance

R*6:* A privacy language has to enable provenance.

- Data Subject has to be identifiable (to claim his/her DSR) even after personal data is transferred from one Controller to another
- Privacy Language has always to be enforced during **Data Processing** and after **Data Transfer**
- Privacy Language has to be „coupled“ to Personal Data

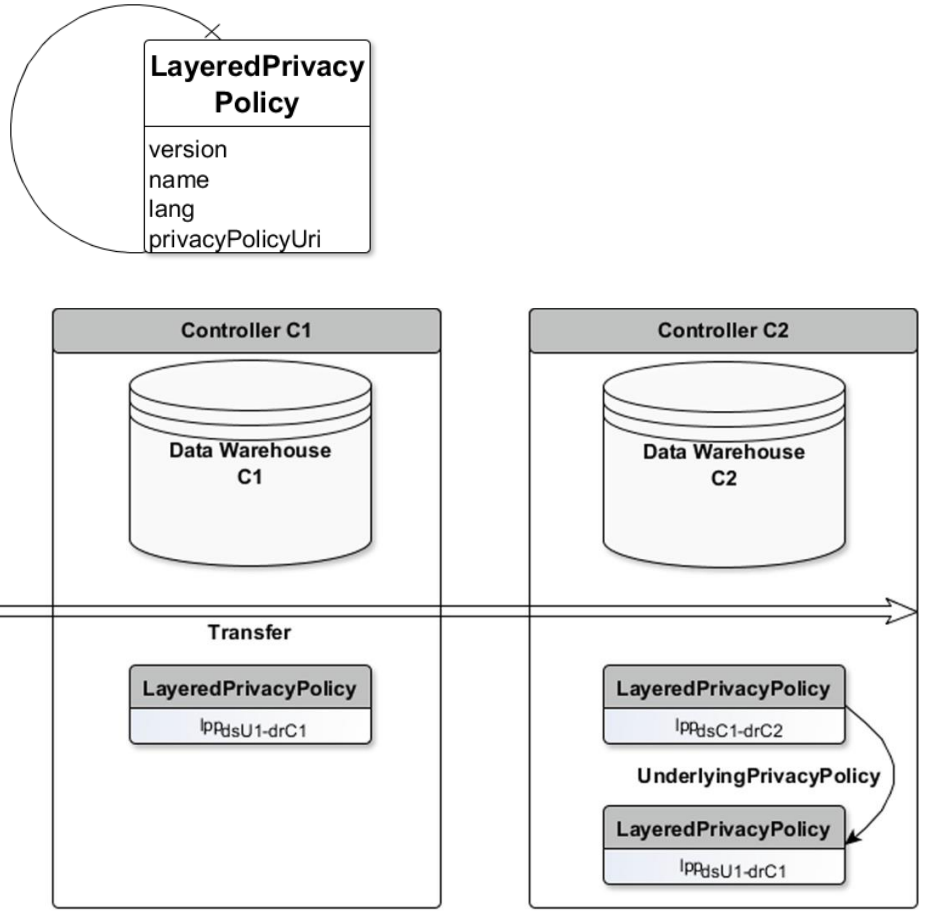


“Layered” in LPL

R*6:* A privacy language has to enable provenance.

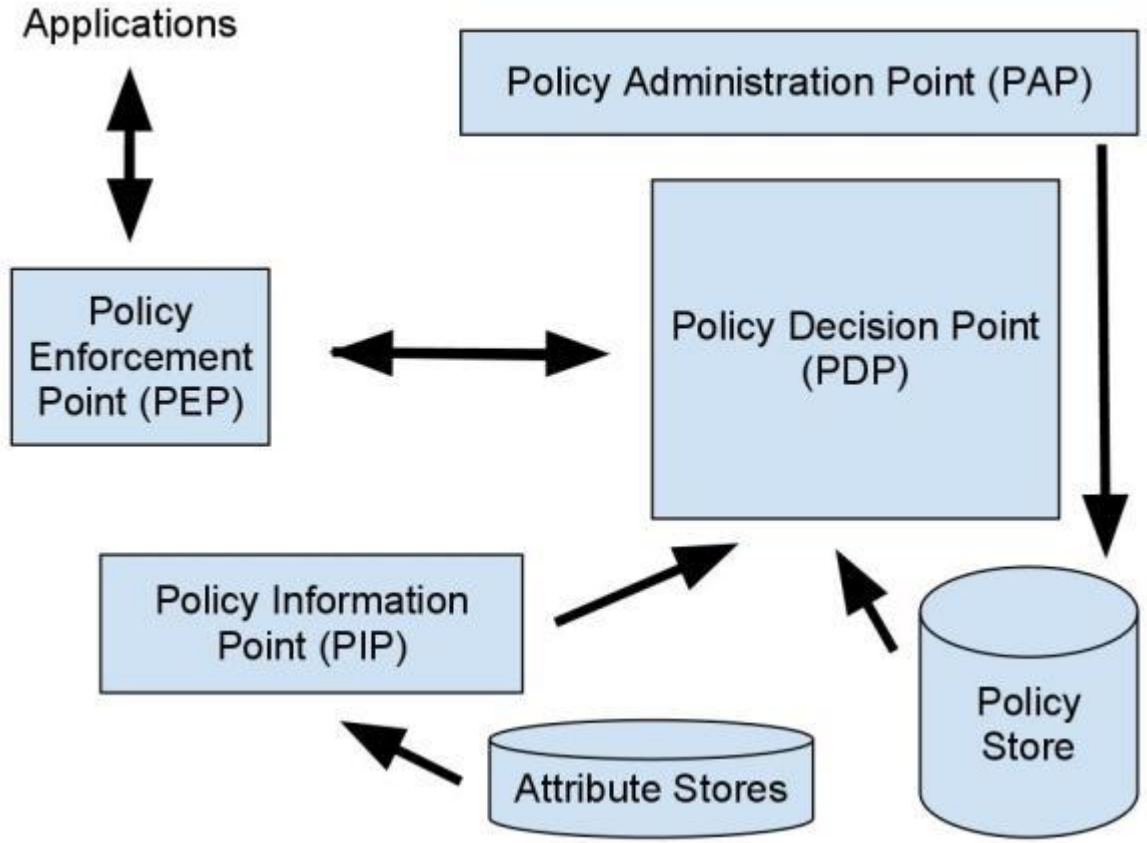
- LayeredPrivacyPolicy can reference other LayeredPrivacyPolicy-element
  - ➢ UnderlyingPrivacyPolicy
- Enables to „track“ previous agreed Privacy Policies
- Enables to create „stricter“ usage policies for third parties
  - ➢ Evaluate against original policy

❖ But: Enforcement of Policy not guaranteed by data structure



Policy Enforcement Process

- XACML Reference Architecture
- Policy Enforcement Point (PEP)
  - The system entity that performs access control, by making decision requests and enforcing authorization decisions. Basically the entity that sends the XACML request to the Policy Decision Point (PDP) and receives an authorization decision.
- Policy Decision Point (PDP)
  - The system entity that evaluates applicable policy and returns an authorization decision.
- Policy Information Point (PIP)
  - The system entity that acts as a source of attribute values. Basically if there are missing attributes in the XACML request which is sent by PEP, PIP would find them for the PDP to evaluate the policy
- Policy Administration Point (PAP)
  - The system entity that creates a policy or policy set and manages them

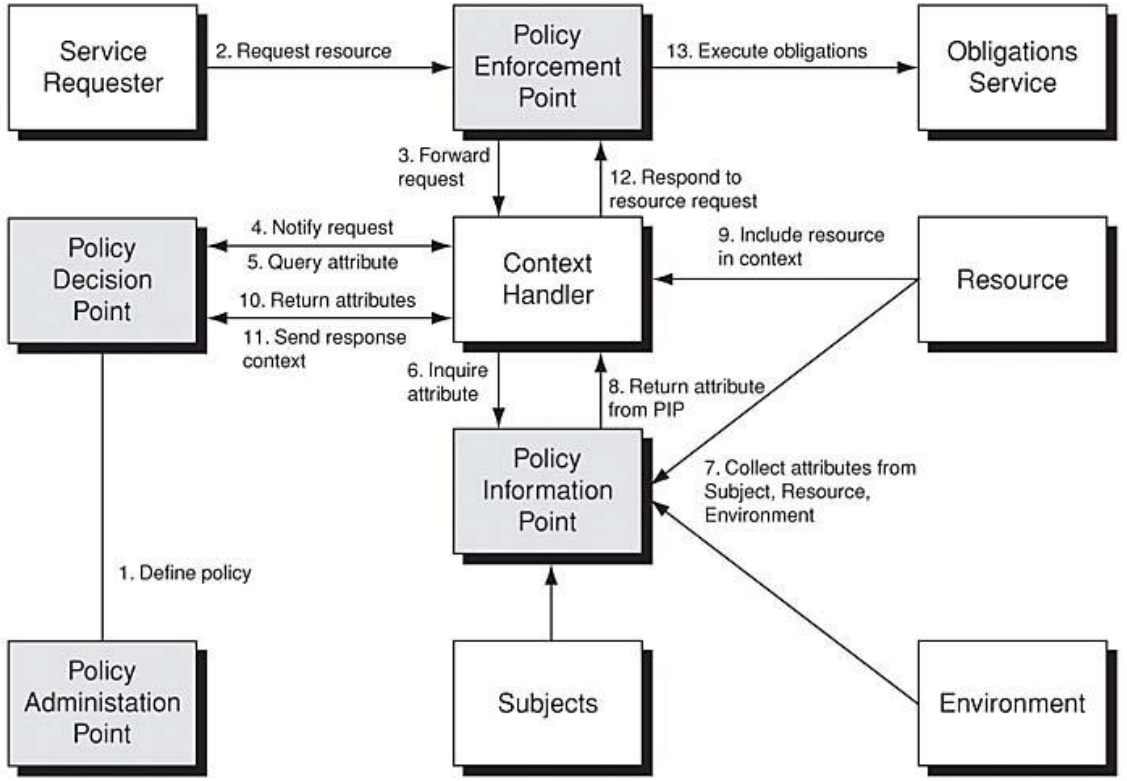


http://xacmlinfo.org/2011/10/30/xacml-reference-architecture/

Policy Enforcement Data Flow (XACML)

Processing of a service request to retrieve the attributes and policies. Chronological order:

1. Define Policy: The policy administrator defines policies and policy sets at the **Policy Administration Point (PAP)**.
2. Request Resource: The service requester issues a request to the **Policy Enforcement Point (PEP)** to access the specified resource. This requires fetching the attributes and policies associated with the *resource*, the *action*, the *environment*, and the *service requester*.
3. Forward Request: **PEP** sends the request for access to the **Context Handler (CH)**. This may include the details of attributes of the *subjects*, *resources*, *actions*, and *environment*.
4. Notify Request: **CH** creates an **request context** and sends a **policy evaluation request** to the **Policy Decision Point (PDP)**.
5. Query Attribute: The **PDP** queries the **CH** for attributes of the *subject*, *resource*, *action*, and *environment* needed to evaluate the policies.

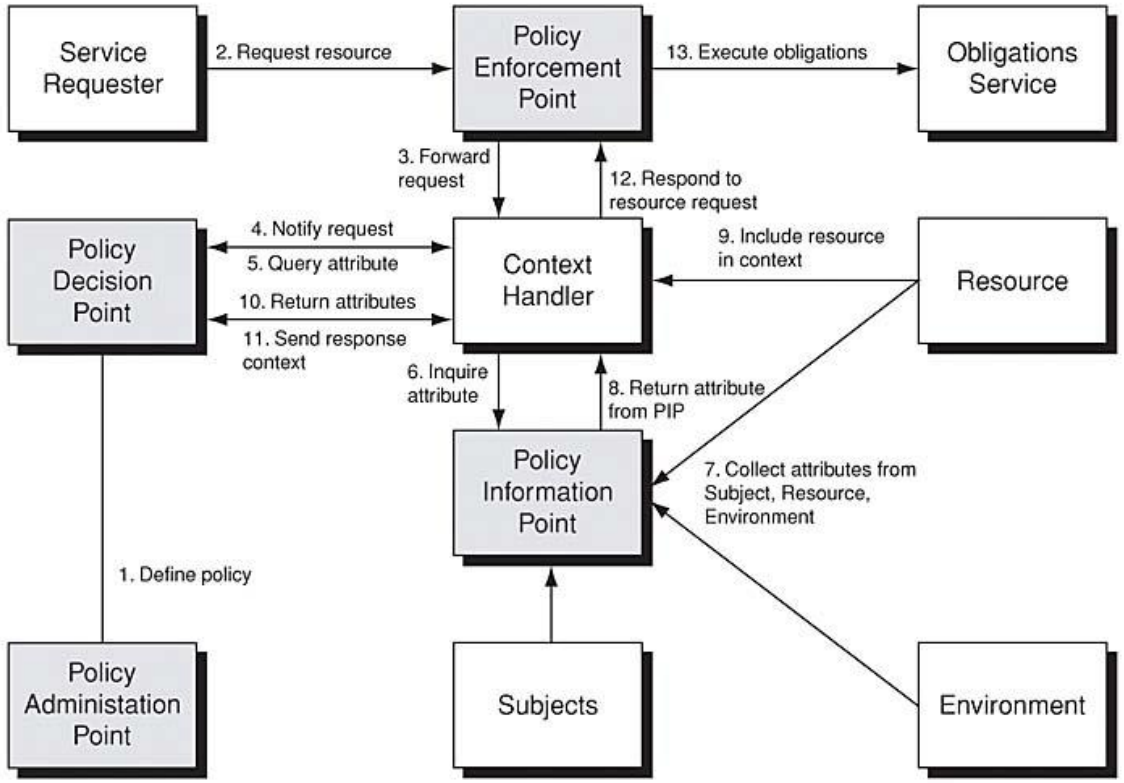


https://www.informit.com/articles/article.aspx?p=1398625&seqNum=12

Policy Enforcement Data Flow (XACML)

6. Inquire Attribute: The **CH** obtains the attributes either from the request context created in Step 4, or it queries a **Policy Information Point (PIP)** for the attributes.
7. Collect Attributes: The **PIP** collects the attributes *resource*, *action*, and the *environment*.
8. Return Attribute PIP: The **PIP** returns the requested attributes to the **CH**.
9. (Optional) Include Resource: The **CH** includes the resource in the context.
10. Return Attribute CH: The **CH** returns the requested attributes from **PIP**. The **PDP** continues evaluating the policy as attributes are made available.
11. Send Response Context: The **PDP** sends the response context (including the authorization decision) to the **CH**.
12. Send Response: The **CH** responds to the **PEP**.
13. The **PEP** executes any relevant **obligations**.

➢ **PEP** will either grant access to targeted resource or deny access.



https://www.informit.com/articles/article.aspx?p=1398625&seqNum=12

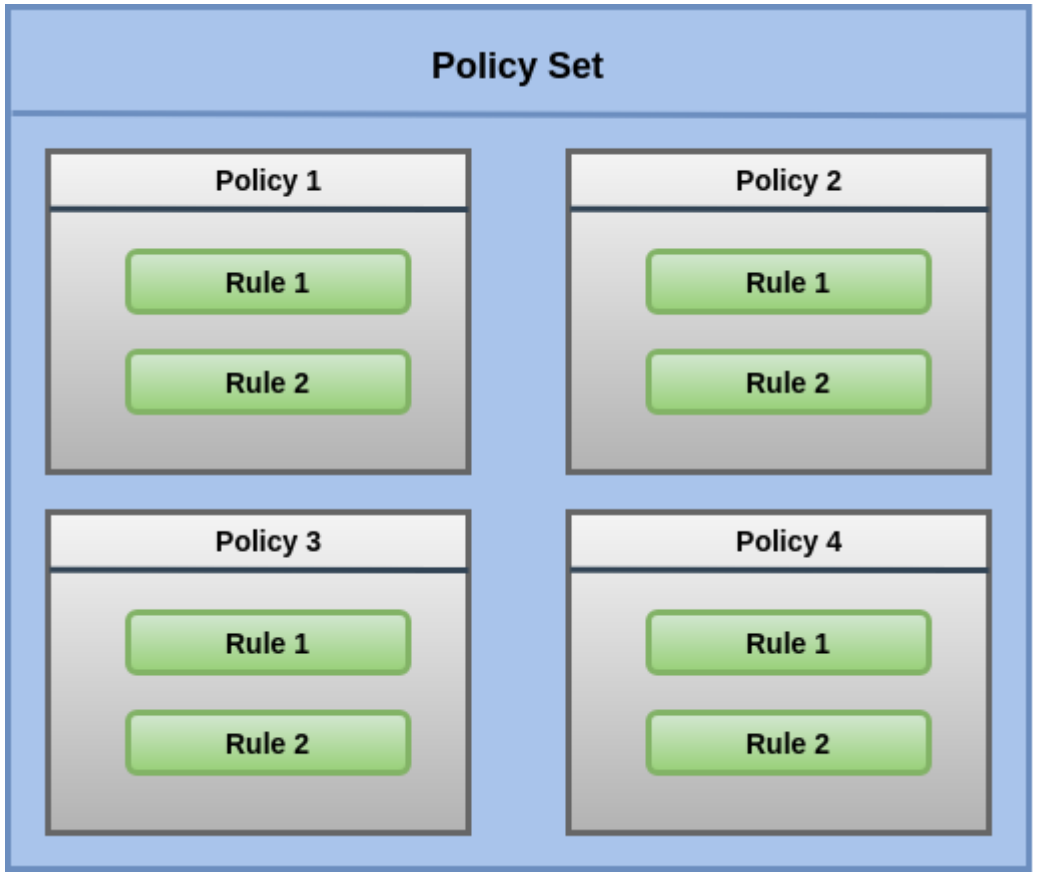
Extensible Access Control Markup Language (XACML)

- XACML is an OASIS standard that describes both a **policy language** and an **access control decision request/response language** (both written in XML).
- The **policy language** is used to describe general **access control requirements**, and has standard extension points for defining new functions, data types, combining logic, etc.
- The **request/response language** lets you form a query to ask whether or not a given action should be allowed, and interpret the result. The response always includes an answer:
  - Permit
  - Deny
  - Indeterminate (an error occurred or some required value was missing, so a decision cannot be made)
  - Not Applicable (the request can't be answered by this service)
- Advantages of XACML:
  - Standardized: Reviewed by large community and widely deployed (interoperability with other applications)
  - Generic: XACML can be used in any environment. One policy can be written which can then be used by many different kinds of applications, and when one common language is used, policy management becomes much easier.
  - Distributed: One policy can refer to other policies (in other locations). No monolithic policy to manage, but various sub-pieces of policies by various stakeholders. XACML combines the results in a single decision.
  - Powerful: Default XACML already supports a wide variety of data types, functions, and rules about combining the results of different policies. Furthermore, extensions and profiles are possible, e.g., that will hook XACML into other standards like SAML and LDAP.

Extensible Access Control Markup Language (XACML)

Three top-level policy elements

- **<Rule>:** contains a Boolean expression that can be evaluated in isolation, but that is not intended to be accessed in isolation by a PDP. So, it is not intended to form the basis of an authorization decision by itself. It is intended to exist in isolation only within an XACML PAP, where it may form the basic unit of management
- **<Policy>:** contains a set of <Rule> elements and a specified procedure for combining the results of their evaluation. It is the basic unit of the policy used by the PDP, and so it is intended to form the basis of an authorization decision
- **<PolicySet>:** contains a set of <Policy> or other <PolicySet> elements and a specified procedure for combining the results of their evaluation.



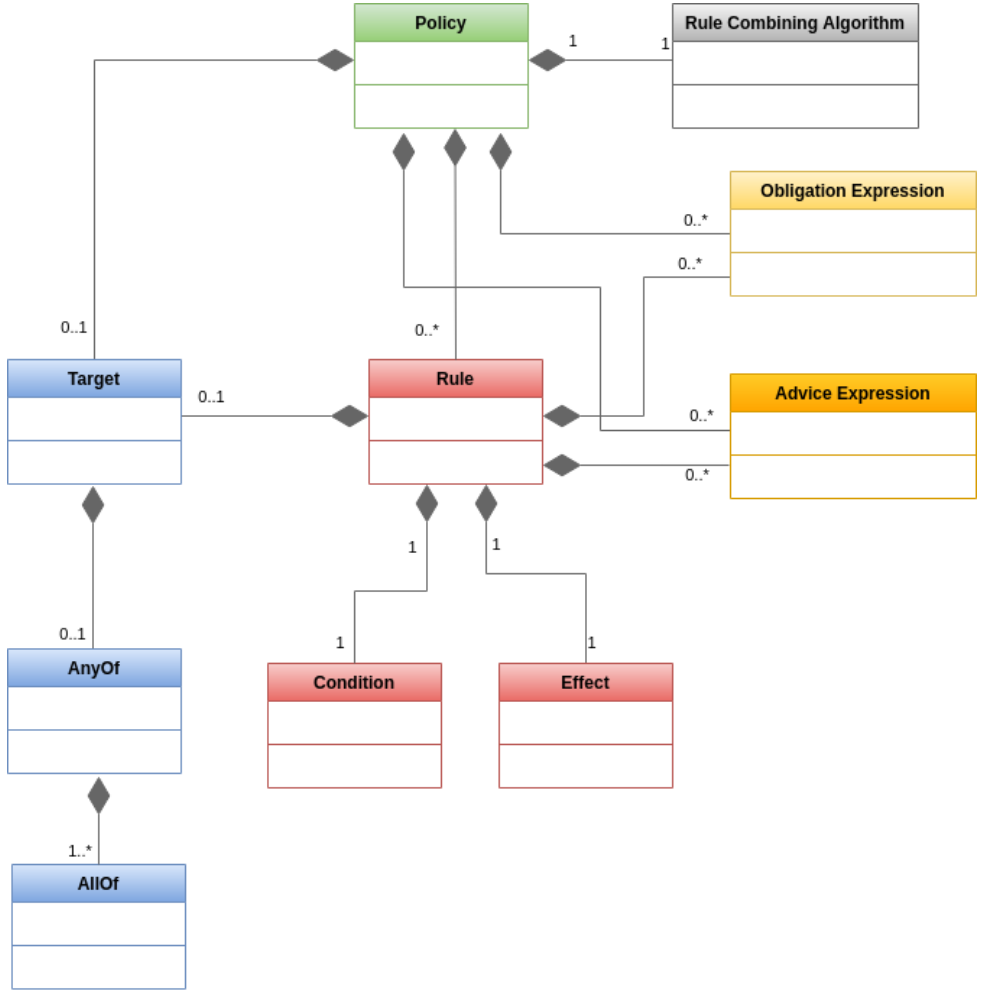
Extensible Access Control Markup Language (XACML)

Target

- An <PolicySet>, <Policy> or <Rule> element contains a <Target> element that specifies the set of requests to which it applies.
- An empty <Target> matches any request. Otherwise, target value is “Match” if all the specified “AnyOf”s are matched in the request.

Rule

- <Rule> is the most elementary unit of policy.
- <Condition> is a boolean function. If the condition evaluates to true, then the Rule’s Effect is returned.
- <Condition> uses **Deontic Logic** and can be quite complex, built from an arbitrary nesting of non-boolean functions and attributes.



Extensible Access Control Markup Language (XACML)

Rule-combining algorithms

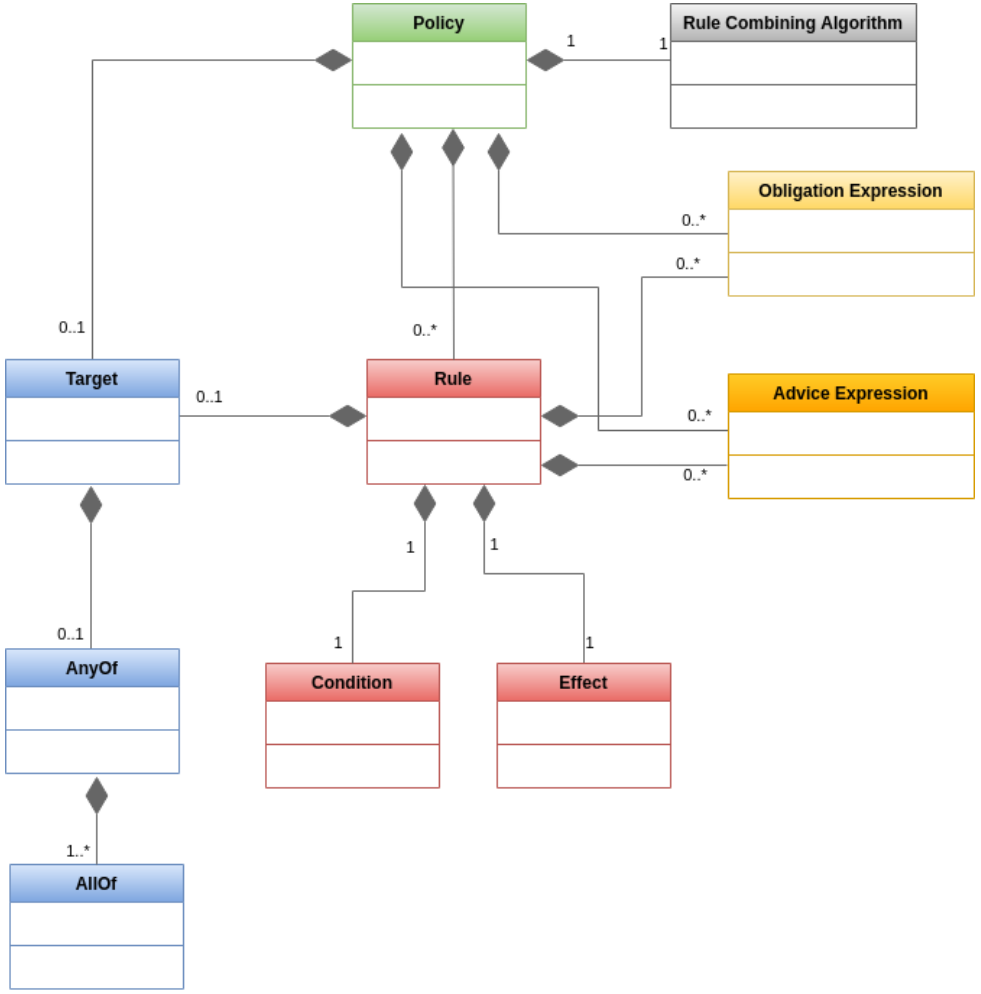
- Specifies the procedure by which the results of evaluating the component rules are combined when evaluating the policy, e.g.,…
  - Deny-overrides: If any decision is “Deny”, the result is “Deny”.
  - Permit-overrides: If any decision is “Permit”, the result is “Permit”.
  - First-applicable: Each rule is evaluated in the order in which it is listed in the policy.

Obligation

- <PolicySet>, <Policy> or <Rule> may contain one or more <obligation>
- obligation is passed up to the next level of evaluation only if the result of the <PolicySet>, <Policy> or <Rule> being evaluated matches the value of the FulfillOn attribute of the <Obligation>

Advice

- <Advice> is similar to <Obligation> in syntax
- But, PEP can disregard any <Advice> it receives



Extensible Access Control Markup Language (XACML)

Attributes, Attribute Values, and Functions

- XACML uses Attribute-Based Access Controlling (ABAC)
  - **Subject:** is the entity requesting access. A subject has one or more attributes.
  - **Resource:** is a data, service or system component. A resource has one or more attributes.
  - **Action:** defines the type of access requested on the resource. Actions have one or more attributes.
  - **Environment:** can optionally provide additional information.

A <Policy< resolves attribute values from the request or retrieves values from the PIP.

- **<AttributeDesignator>:** lets the policy specify an attribute with a given name and type, and optionally an issuer as well. <AttributeDesignator> can return multiple values.
- **<AttributeValue>:** contains a literal attribute value
- **<Apply>:** denotes the application of a function to its arguments, thus encoding a function call.

XACML comes with a powerful system of functions. Functions can work on any combination of attribute values and can return any kind of attribute value supported in the system. Functions can also be nested, so we can have functions that consume the output of other functions, and this hierarchy can be arbitrarily complex.

Extensible Access Control Markup Language (XACML)

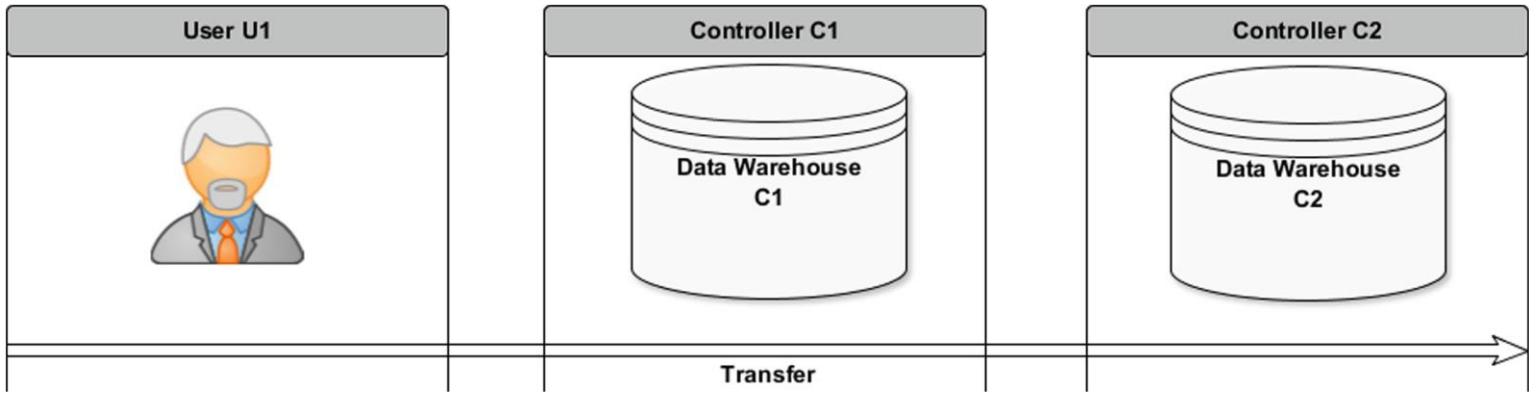
Example Rule 'Permit if single String of Subject-ID equals Attribute Value "Alice"':

```
<Rule Effect="Permit" RuleId="Alice Rule">
        <Condition>
                <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
                                <AttributeDesignator
        AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
        Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
        DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
                        </Apply>
                        <AttributeValue
        DataType="http://www.w3.org/2001/XMLSchema#string">Alice</AttributeValue>
                </Apply>
        </Condition>
</Rule>
```

Sticky Policy Concept

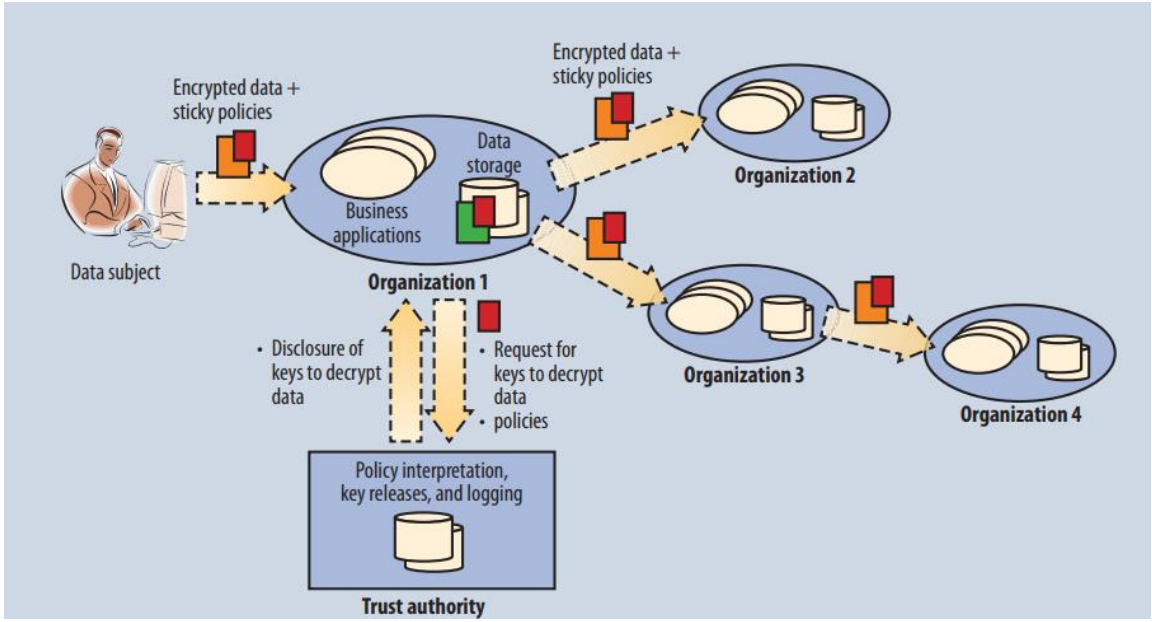
Problems in Data Transfer:

- No Verification of Consent to Data Processing
- No Verification of Consent to Aggregated Data Processing from Different Sources
- No Verification of Consent State Changes



Sticky Policy Concept

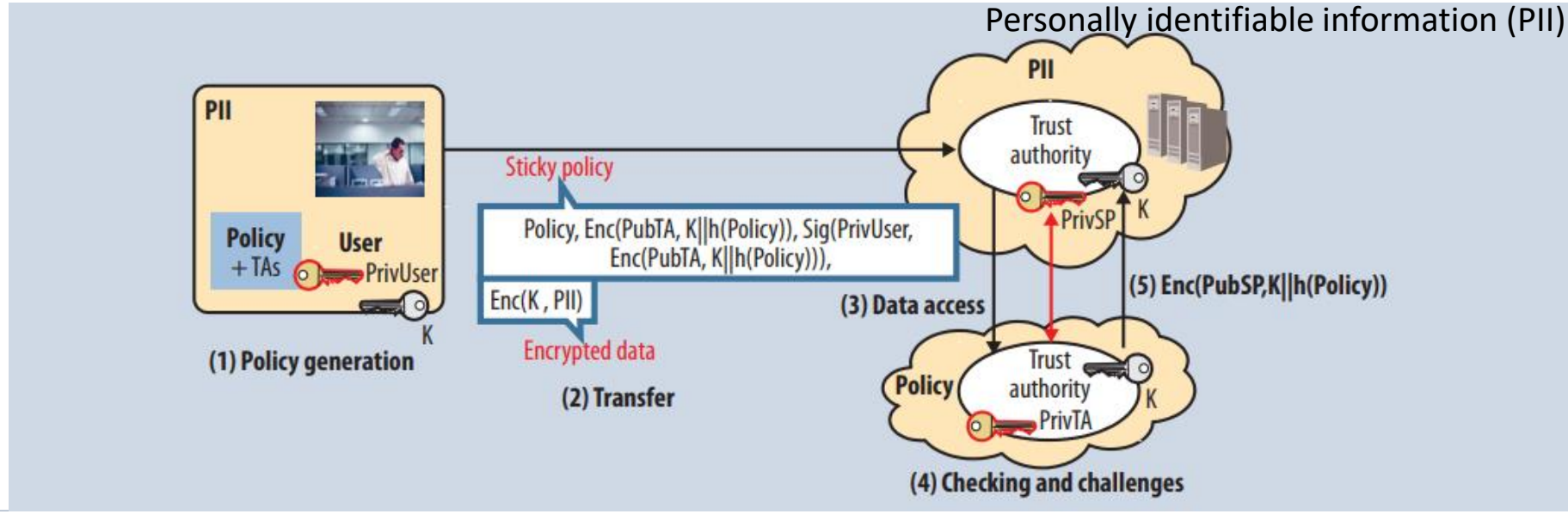
- Setup:
  - A user (Data Subject) can interact with an Service Provider (SP) to personalize the privacy policy
  - The user selects a subset of TAs that are to be trusted
  - Creation of Sticky Policy: bundling of policies, preferences, data, and TAs on client-side
  - (Optional) Storage of Personally identifiable information (PII) at third party, instead of storing encrypted data directly to SP
  - Encrypted data with sticky policies is send to the SP
- Data Access:
  - SP needs to interact with one of the selected TAs. SP has to fulfill the personalized sticky policies
  - Only after satisfying all these requirements and checking additional contextual information will the TA decide to release the keys for decrypting data.
  - The TA will be able to decrypt and access the data regardless of whether it was directly disclosed or if only a reference to it was provided. In the latter case, the SP would need to fetch the data



Sticky Policy Concept

Example with Public-Key Cryptography Standard (PKCS)

- 1. The sender generates the policy, together with a symmetric key K used to encrypt the data (for efficiency, a symmetric key is used rather than an asymmetric key). If desired, this process can be generalized to allow encrypting different attributes separately—that is, using different symmetric keys generated at this stage—revealing only part of the information when an attribute is decrypted.
- 2. The sender generates a message to the SP. One part of the message is the data encrypted with K. The other part is a sticky policy, in which K, appended to the policy's hash, is encrypted with the TA's public key and then is signed using the user's private key. This makes it possible to verify the policy's source and integrity and binds K to the data and the policy. The system sends the resultant sticky policy together with the encrypted data to the SP.

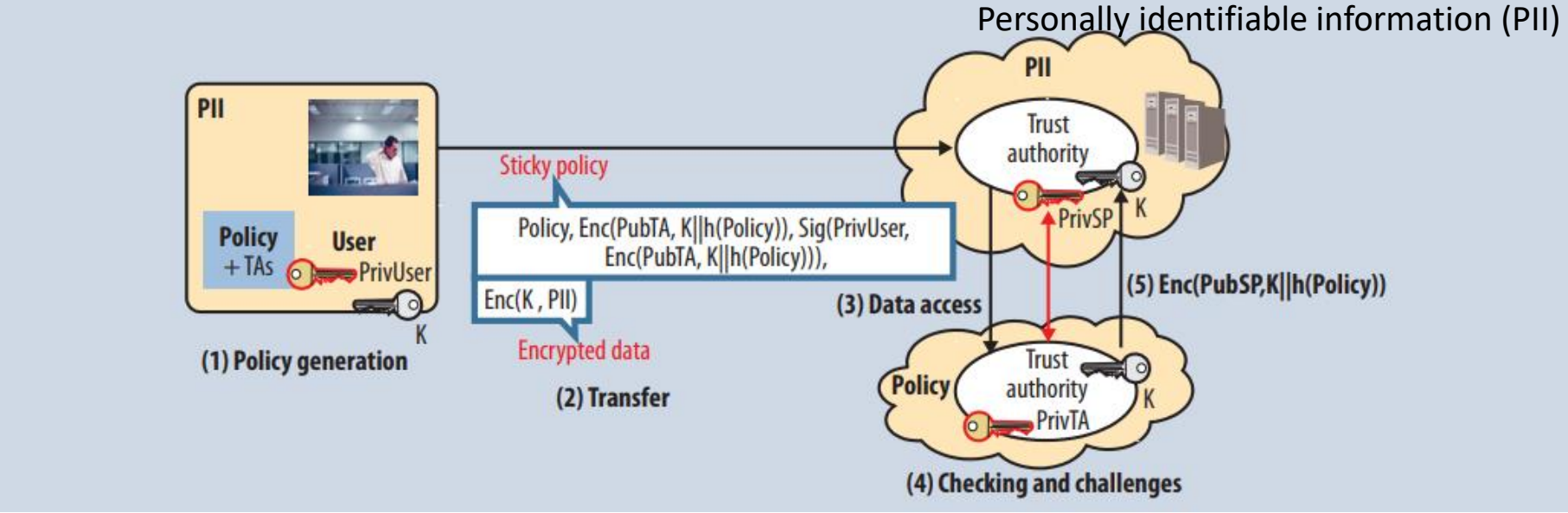


M. Mont and S. Pearson, "Sticky Policies: An Approach for Managing Privacy across Multiple Parties" in *Computer*, vol. 44, no. 09, pp. 60-68, 2011. doi: 10.1109/MC.2011.225 url: https://doi.ieeecomputersociety.org/10.1109/MC.2011.225

Sticky Policy Concept

Example with Public-Key Cryptography Standard (PKCS)

- 3. The SP generates a message to the TA, which involves passing on just the sticky policy and encrypted shared keys.
- 4. The TA checks policies, potentially including challenges to the SP. The SP might need to provide signed statements about its policies.
- 5. If all checks are fulfilled, the TA releases the shared key. This generates a message from the TA to the SP, which involves encrypting K appended to the policy's hash with the SP's public key. The SP can get access to K to check the policy's integrity and then decrypt the PII.6



M. Mont and S. Pearson, "Sticky Policies: An Approach for Managing Privacy across Multiple Parties" in *Computer*, vol. 44, no. 09, pp. 60-68, 2011. doi: 10.1109/MC.2011.225 url: https://doi.ieeecomputersociety.org/10.1109/MC.2011.225

Sticky Policy Concept

- Summary: Machine-readable policies are sticked to data to define allowed usage and obligations as it travels across multiple parties, enabling users to improve control over their personal information.

- Advantage:
  - Policies can be propagated throughout the cloud to trusted organisations
  - strong enforcement of the policies
  - traceability.
- Disadvantage:
  - Scalability: policies increase size of data.
  - Practicality may not be compatible with existing systems.
  - It may be difficult to update the policy after sharing of the data and existence of multiple copies of data.
  - It requires ensuring data is handled according to policy e.g. using auditing.

R6: Provenance

R*6:* A privacy language has to enable provenance.

- **Data Processing** can be solved by **Policy Enforcement Data Flow**
- **Data Transfer** can be solved by **Sticky Policies**

- But…
  - No adaptation of both concepts in „Real Life“ to the best of our knowledge to date
  - No „Best Practice“ implementation for Sticky Policies

Privacy Languages are the solution?

- Requirements (R1 to R6) can be addressed by privacy languages

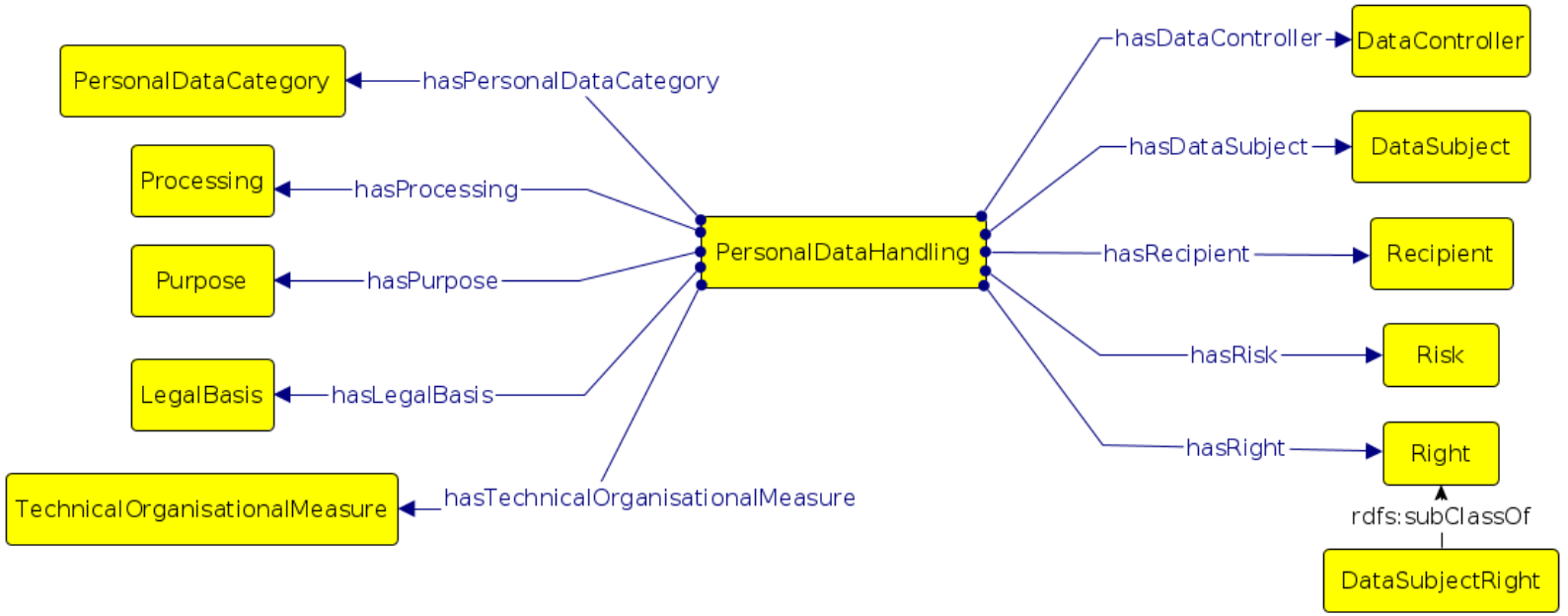
Additional Problem:

- Communication 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!

Data Privacy Vocabulary (DPV)

- W3C Draft (v0.2)
- The Data Privacy Vocabulary (DPV) provides terms (classes and properties) to describe and represent information related to processing of personal data based on established requirements such as for the EU General Data Protection Regulation (GDPR).
- Concept can be used with semantic technologies (e.g., RDF, OWL, etc.)

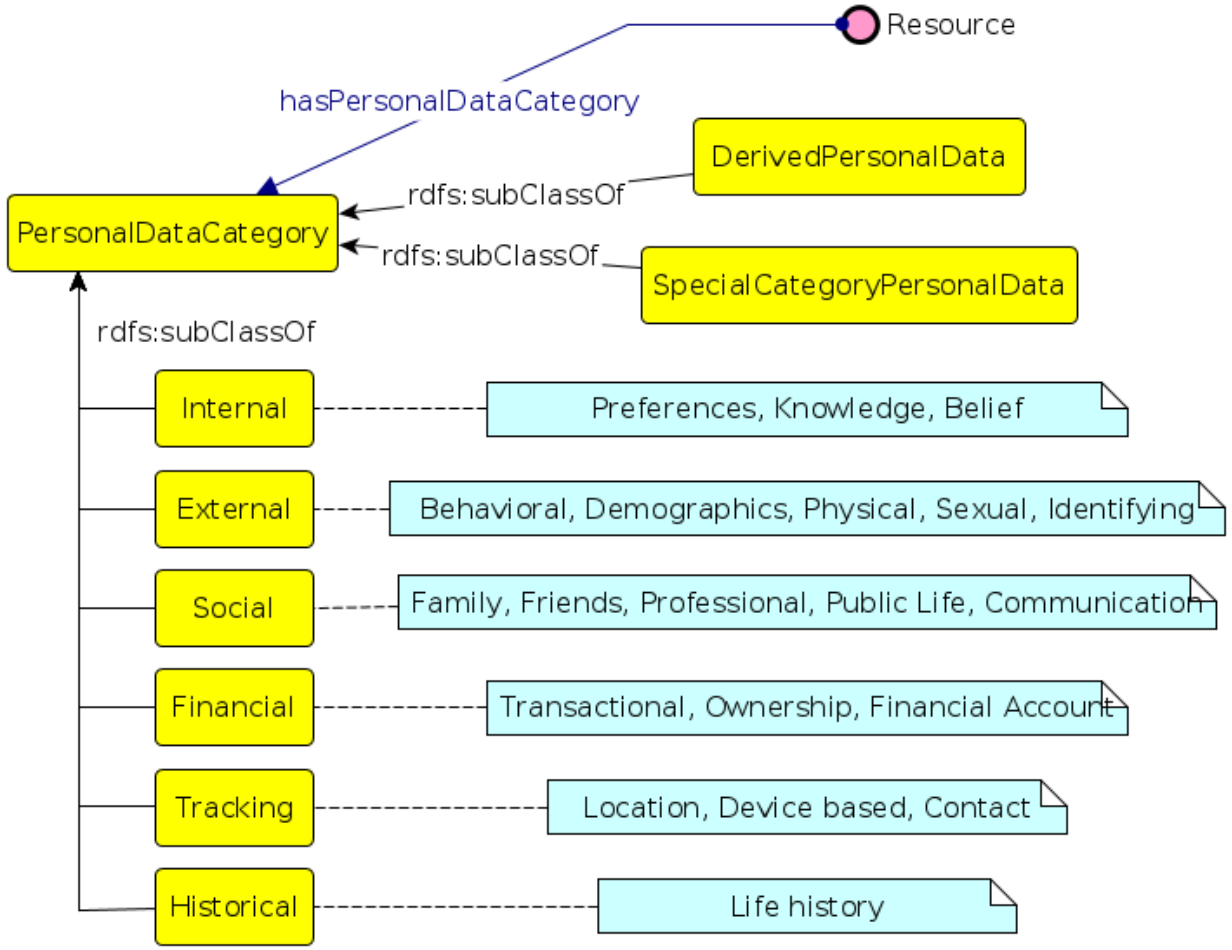


https://www.w3.org/TR/dpv/

Data Privacy Vocabulary (DPV)

- Example Personal Data Categories
- DPV provides broad top-level personal data categories
  - nature of information (financial, social, tracking)
  - inherent source (internal, external)
- Each top-level concept is represented in the DPV vocabulary as a Class
- Subclasses for referring to specific categories of information
  - E.g., preferences or demographics.

Complete? Correct? -> Community Work and Standardization required



2.4
Summary

Dr. Armin Gerl

Recap of Chapter

- Privacy is a Human Right
- General Data Protection Regulation (GDPR)
  - Core Principles
  - Legal Terminology
  - Data Subject Rights
- GDPR has very good intentions, but
  - not all laws are easy to implement with current technologies
  - Check if laws are all complied to is hard and only relativ few fines have been issued
- Privacy Languages are the „glue“ between legal frameworks and IT
  - Requirements for privacy languages
  - Example: LPL and XACML (access control language)

Overview of Lecture Topics

Chapter	Est. Extent
Chapter 1: Introduction	~1 Lecture
Chapter 2: From GDPR to Privacy Languages	~3 Lecture
Chapter 3: Basics on Data Anonymization in IS	~2 Lecture
Chapter 4: Privacy Risks and Anonymization Techniques	~4 Lectures
Chapter 5: Privacy in Health-Care	~2 Lectures
Chapter 6: Privacy in Data Warehouses	~2 Lectures
Chapter 7: Privacy in Social Networks	~2 Lectures
Chapter 8: Current Research and Outlook	
Exam Preparation Lecture	1 Lecture