Privacy: bridging the gap between regulations and technical solutions

Thibaud Antignac
Chalmers University of Technology

September 28, 2016

- Privacy regulation
- Privacy by design
- Data minimisation

Data protection is heavy

General Data Protection Regulation

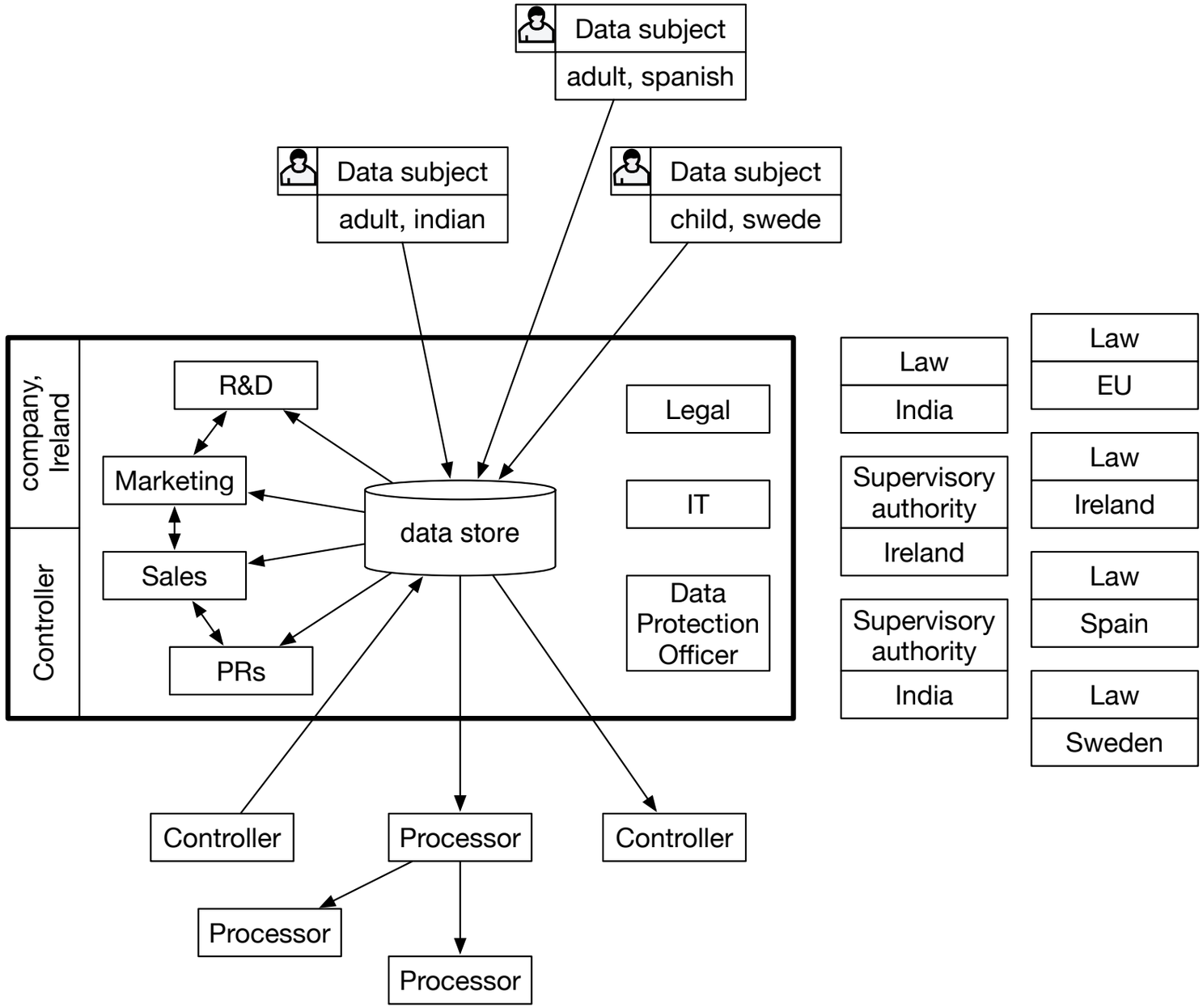
I	General provisions
II	Principles
III	Rights of the data subject
IV	Controller and processor
V	Transfer of personal data to third countries or international organisations
VI	Independent supervisory authorities
VII	Cooperation and consistency
VIII	Remedies, liability and penalties
IX	Provisions relating to specific processing situations
X	Delegated acts and implementing acts
XI	Final provisions

Data protection is heavy (very)

General Data Protection Regulation

I	General provisions	
	1	Subject matter and objectives
	2	Material scope
	3	Territorial scope
	4	Definitions
II	Principles	
	5	Principles relating to processing of personal data
	6	Lawfulness of processing
	7	Conditions for consent
	8	Conditions applicable to child's consent in relation to information society services
	9	Processing of special categories of personal data
	10	Processing of personal data relating to criminal convictions and offences
	11	Processing which does not require identification
III	Rights of the data subject	

Complex (personal) data flows



Business

Personal data	information	key	value	
Processing	operation	kind	computation	parameters

Business vs. compliance

Personal data	information	key	value		
Processing	operation	kind	computation	parameters	

Business vs. compliance

Personal data	information	key	value						
	privacy metadata	purpose	retention	< 13 years	< 18 years	EU	consent	category	
	provenance	processing							

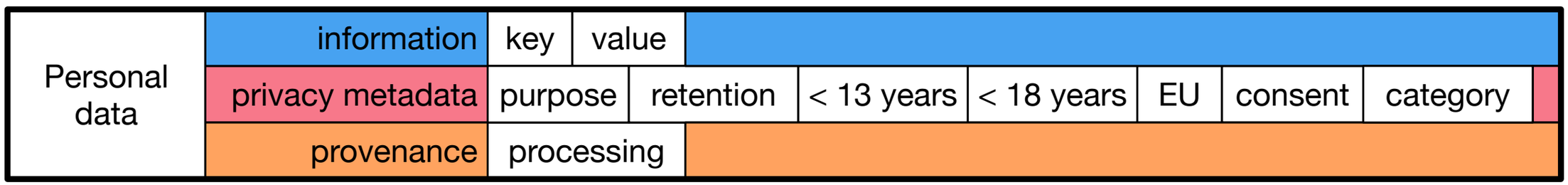
Processing	operation	kind	computation	parameters	

Business vs. compliance

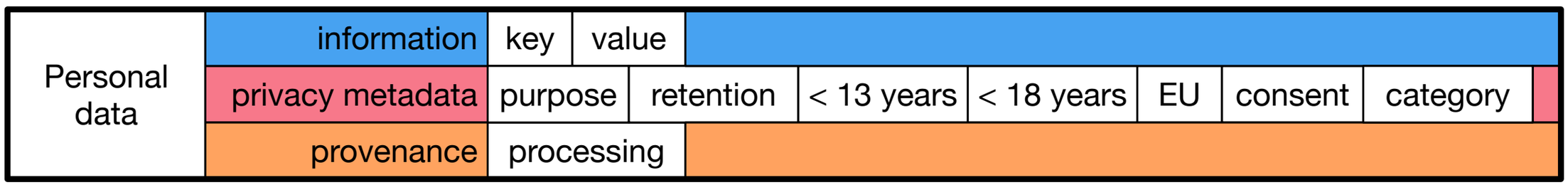
Personal data	information	key	value						
	privacy metadata	purpose	retention	< 13 years	< 18 years	EU	consent	category	
	provenance	processing							

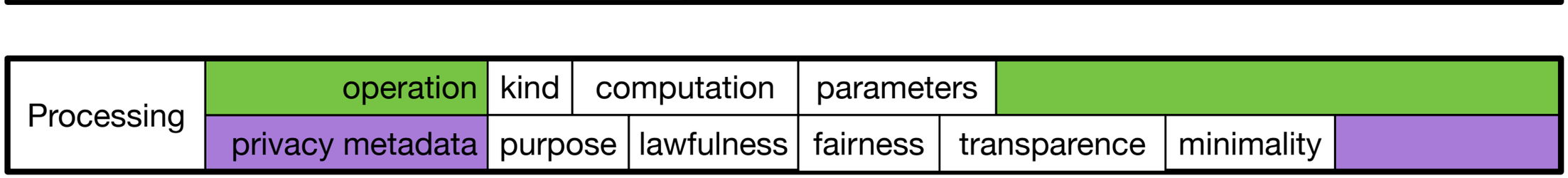
Processing	operation	kind	computation	parameters			
	privacy metadata	purpose	lawfulness	fairness	transparence	minimality	

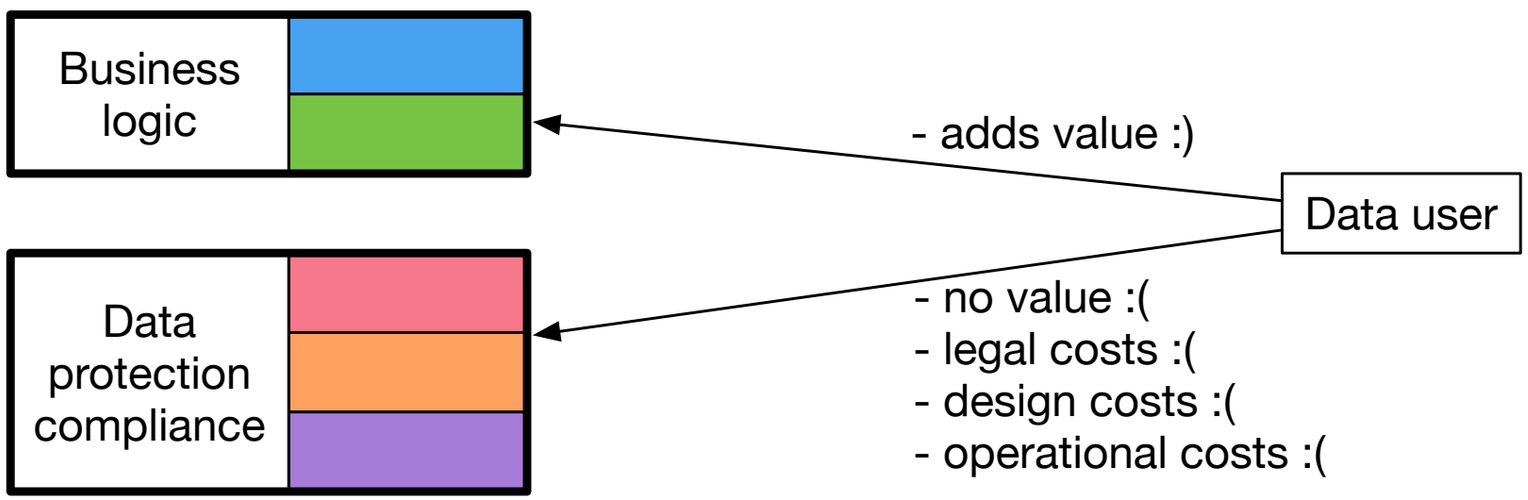
Business vs. compliance



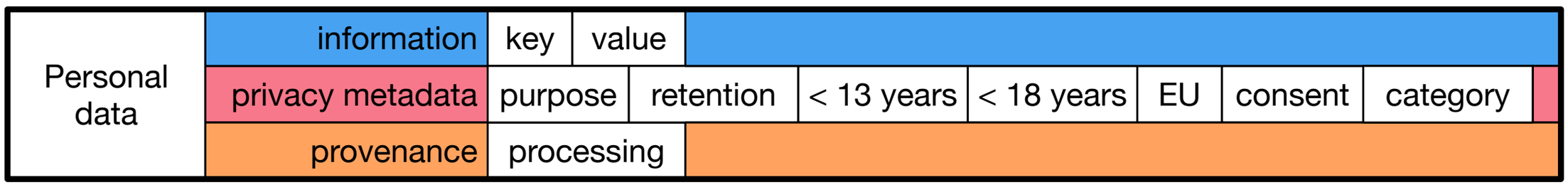
Business vs. compliance

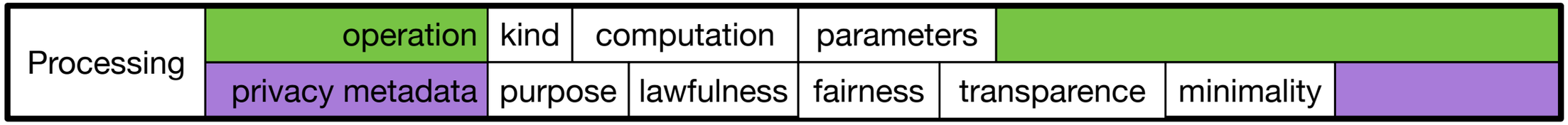


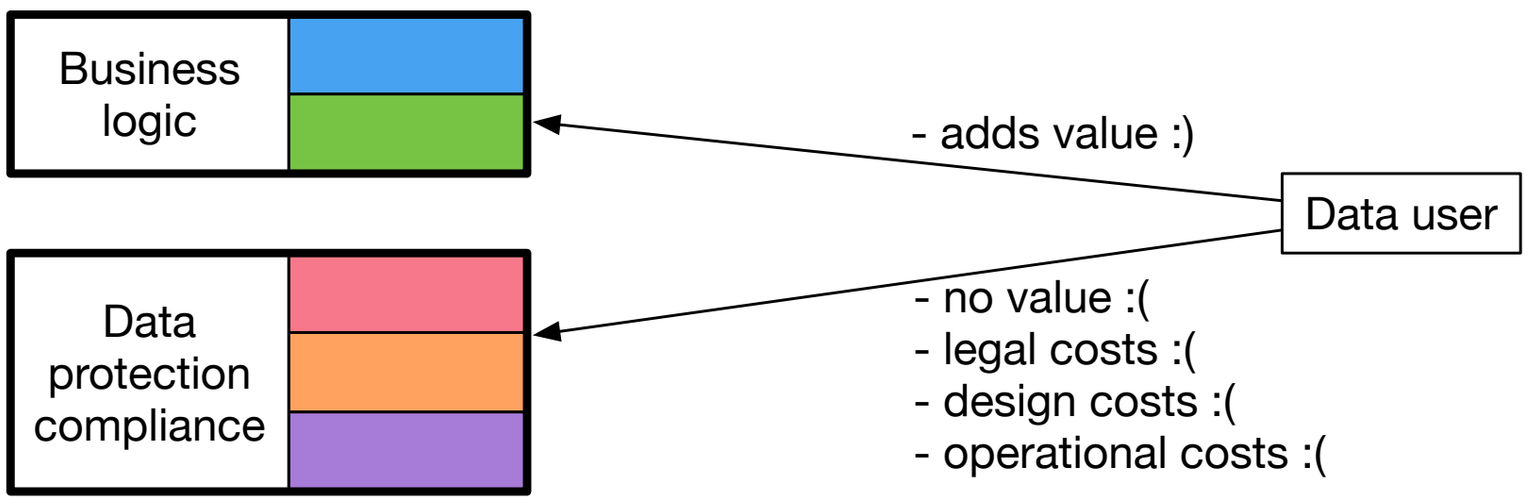




Business vs. compliance







Data protection compliance should be automated as much as possible.

Article 5
Principles relating to processing of personal data

- 1.
  - (a) lawfulness, fairness and transparency;
  - (b) purpose limitation;
  - (c) data minimisation;
  - (d) accuracy;
  - (e) storage limitation;
  - (f) integrity and confidentiality.
- 2. accountability.

Article 5
Principles relating to processing of personal data

- 1.
  - (a) **lawfulness**, fairness and transparency;
  - (b) purpose limitation;
  - (c) data minimisation;
  - (d) accuracy;
  - (e) storage limitation;
  - (f) integrity and confidentiality.
- 2. accountability.

Article 6
Lawfulness of processing

- 1. Processing shall be lawful only if and to the extent that at least one of the following applies:
    - (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
    - (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
    - (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
    - (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
    - (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
    - (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child
- Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

- 2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.
- 3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:
    - (a) Union law; or
    - (b) Member State law to which the controller is subject.
- The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

- 4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
    - (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
    - (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
    - (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
    - (d) the possible consequences of the intended further processing for data subjects;
    - (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 6
Lawfulness of processing

- **1. Processing shall be lawful only if and to the extent that at least one of the following applies:**

  - **(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;**

  - **(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;**

  - **(c) processing is necessary for compliance with a legal obligation to which the controller is subject;**

  - **(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;**

  - **(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;**

  - **(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child**

- **Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.**

- 2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

- 3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

  - (a) Union law; or

  - (b) Member State law to which the controller is subject.

- The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

- 4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

  - (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

  - (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

  - (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

  - (d) the possible consequences of the intended further processing for data subjects;

  - (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 6
Lawfulness of processing

- 1. Processing shall be lawful only if and to the extent that at least one of the following applies:
    - (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
    - (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
    - (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
    - (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
    - (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
    - (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
- Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Article 6
Lawfulness of processing

- Lawful(Processing(Data, Purpose)) →
  Consent(Data, Purpose) ∨
  Contract(Data) ∨
  LegalObligation(Data) ∨
  Contract(Data) ∨
  VitalInterests(Data) ∨
  (PublicInterest(Data) ∨ OfficialAuthority(Data)) ∨
  (LegitimateInterests(Data) ∧
    (¬ FundamentalRightsException(Data)) ∧
    (¬ PublicAuthority(Data)))

Article 6
Lawfulness of processing

- Lawful(Processing(Data, Purpose)) →
  Consent(Data, Purpose) ∨
  Contract(Data) ∨
  LegalObligation(Data) ∨
  Contract(Data) ∨
  VitalInterests(Data) ∨
  (PublicInterest(Data) ∨ OfficialAuthority(Data)) ∨
  (LegitimateInterests(Data) ∧
    (¬ FundamentalRightsException(Data)) ∧
    (¬ PublicAuthority(Data)))

Article 7
Conditions for consent

- 1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

- 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, 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. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

- 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

- 4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 5
Principles relating to processing of personal data

- 1.
  - (a) lawfulness, fairness and transparency;
  - (b) purpose limitation;
  - (c) data minimisation;
  - (d) accuracy;
  - (e) storage limitation;
  - (f) integrity and confidentiality.
- 2. accountability.

Privacy engineering

- Design
- Implementation
- Adaptation
- Evaluation

- Theories
- Methods
- Techniques
- Tools

Bridging the gap

- **Privacy by techies**
  - confidentiality
  - unlinkability
  - anonymity
  - unobservability
- **Privacy by lawyers**
  - consent
  - purpose
  - retention
  - identification

Policies

Static Policies [SEFM'14, JLAMP`16]

We enrich the social graph with the knowledge of the agents

Including a reasoning engine which captures inferred knowledge

Using a knowledge based logic to specify the privacy policies of each user

E.g., "*Nobody can know my location*" or "*Only my friends can see my pictures*"

Dynamic (*Evolving*) Policies

Runtime monitoring of events using automata [RV'16]

As events are executed, static policies are activated or deactivated

E.g., "*My location can only be disclosed 3 times per day*"

Temporal and Real-time knowledge based logic [TIME'16]

Inherently temporal or real time logic

E.g., "*My supervisor cannot see my pictures from 20:00 to 8:00*"

Privacy by design

A Privacy-Aware Conceptual Model for Handling Personal Data
Thibaud Antignac, Riccardo Scandariato, Gerardo Schneider
In Leveraging Applications of Formal Methods, Verification and Validation, ISoLA 2016, LNCS, Volume XXX, pages XX-XX, Springer, 2016.

Article 25
Data protection by design and by default

- 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

- 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

- 3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 25
Data protection by design and by default

- 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

- 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

- 3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Privacy by design?

- What does it mean?
- How can it be ensured?

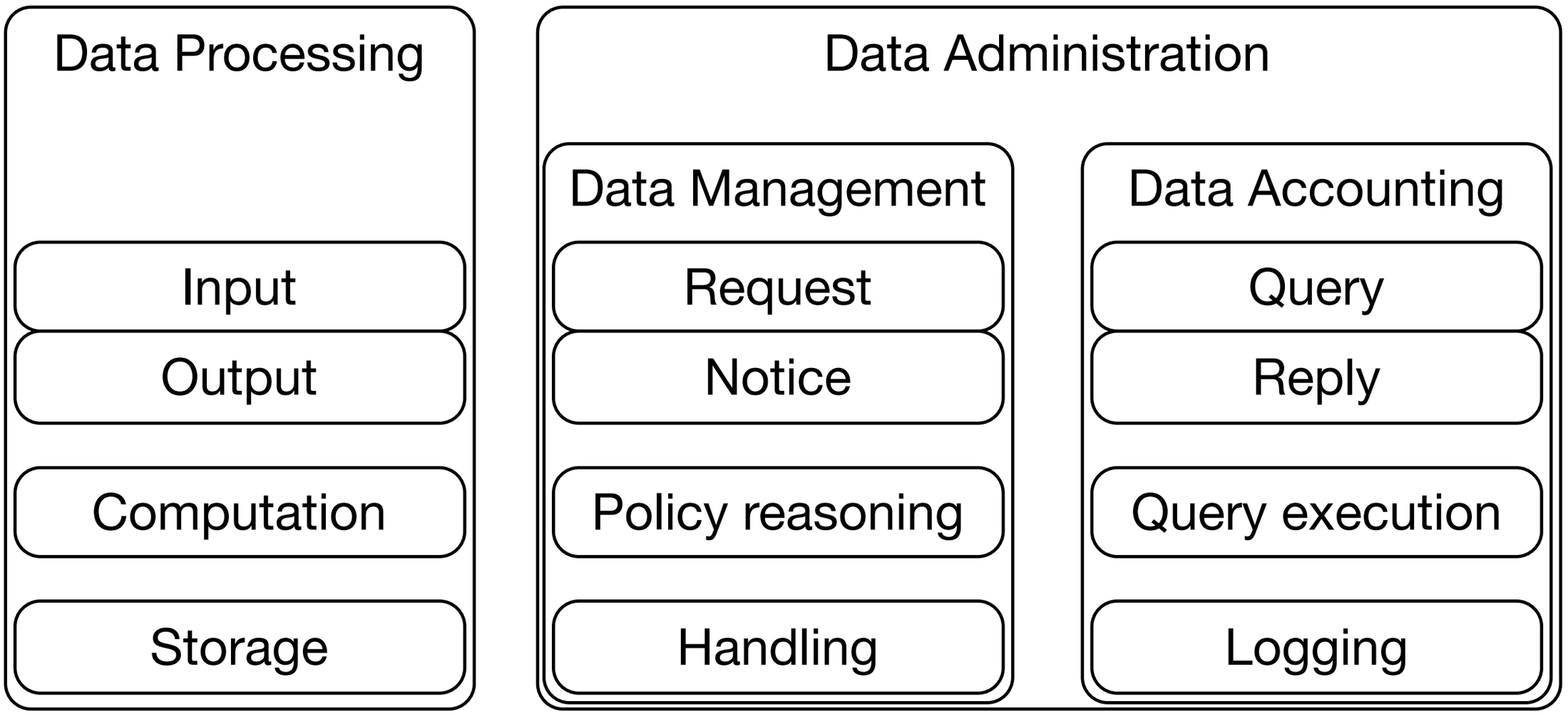
with Riccardo Scandariato & Gerardo Schneider

From the early stages

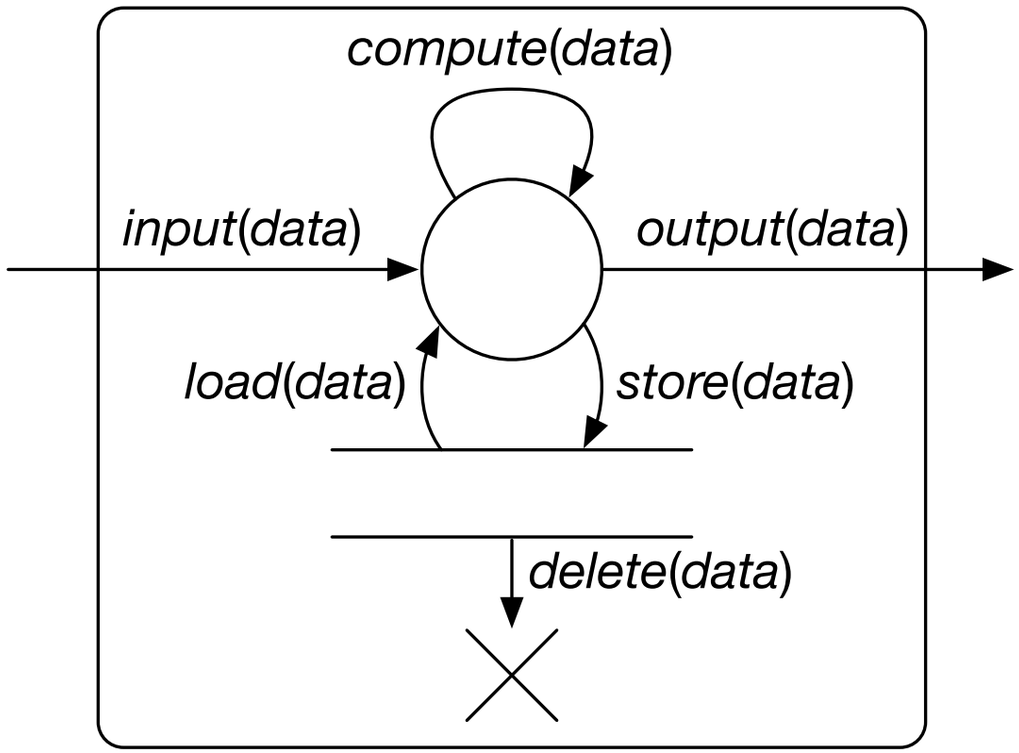
- prevention rather than cure
- embedded within the entire life cycle
  - early design stage
  - deployment
  - use
  - final disposal

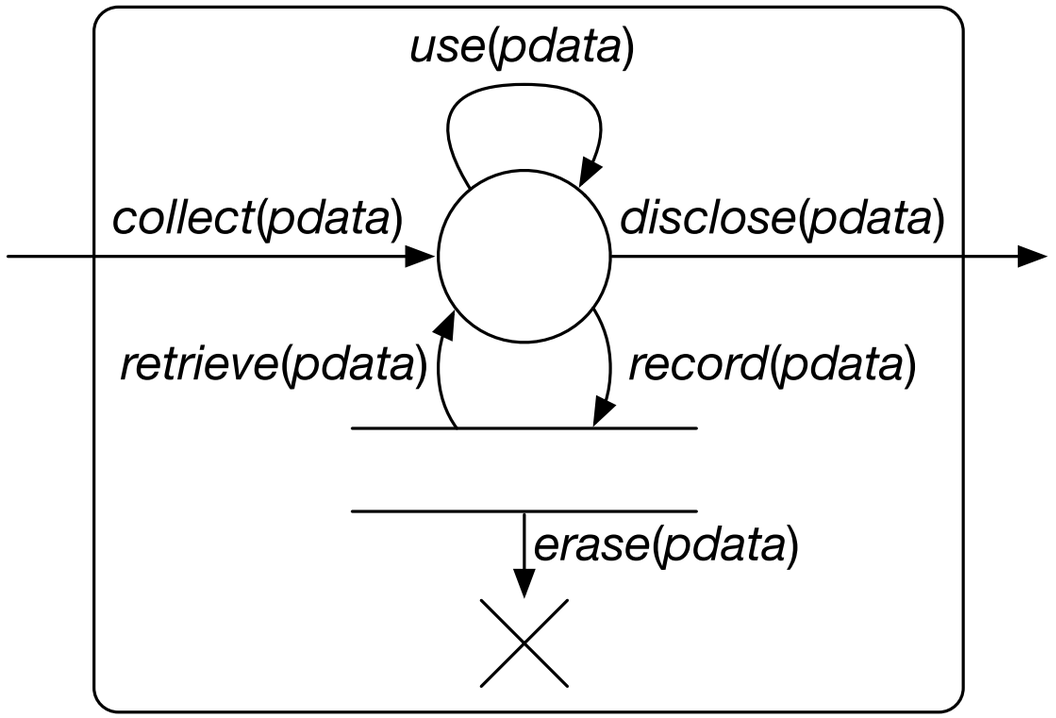
[Privacy by Design: The 7 Foundational Principles, Cavoukian, 2009]
[Article 25, EU General Data Protection Regulation, European Commission, 2016]

Architecture

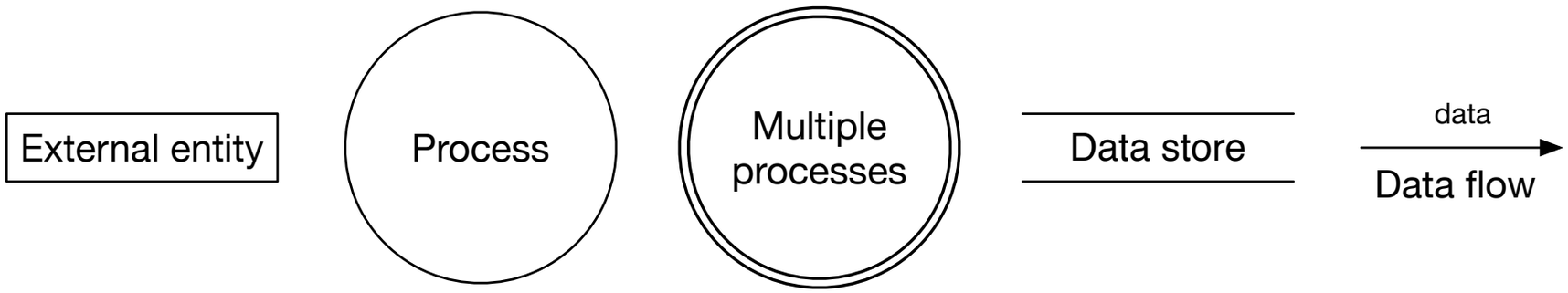


(Personal) data lifecycle

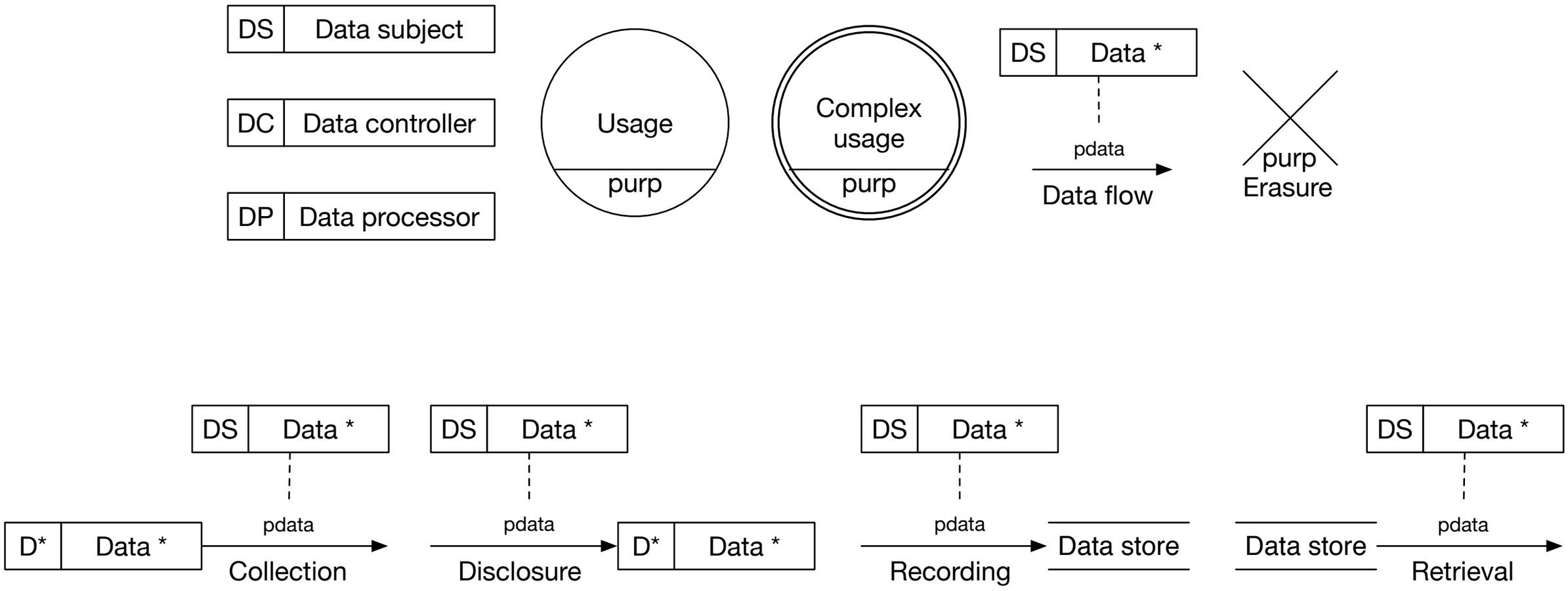




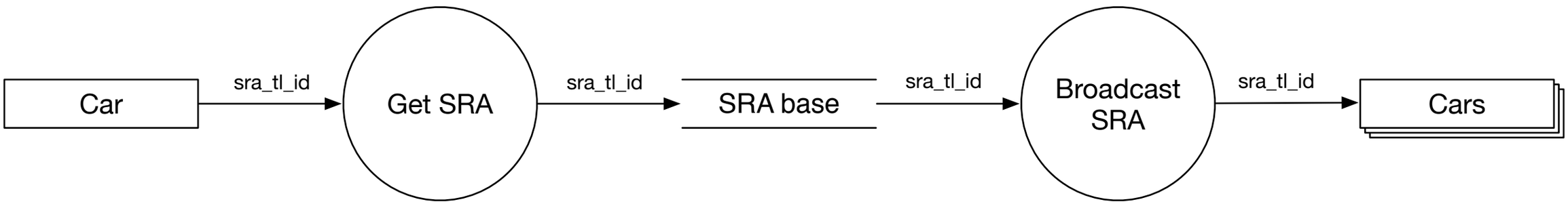
Data flow diagrams



Privacy-aware DFDs

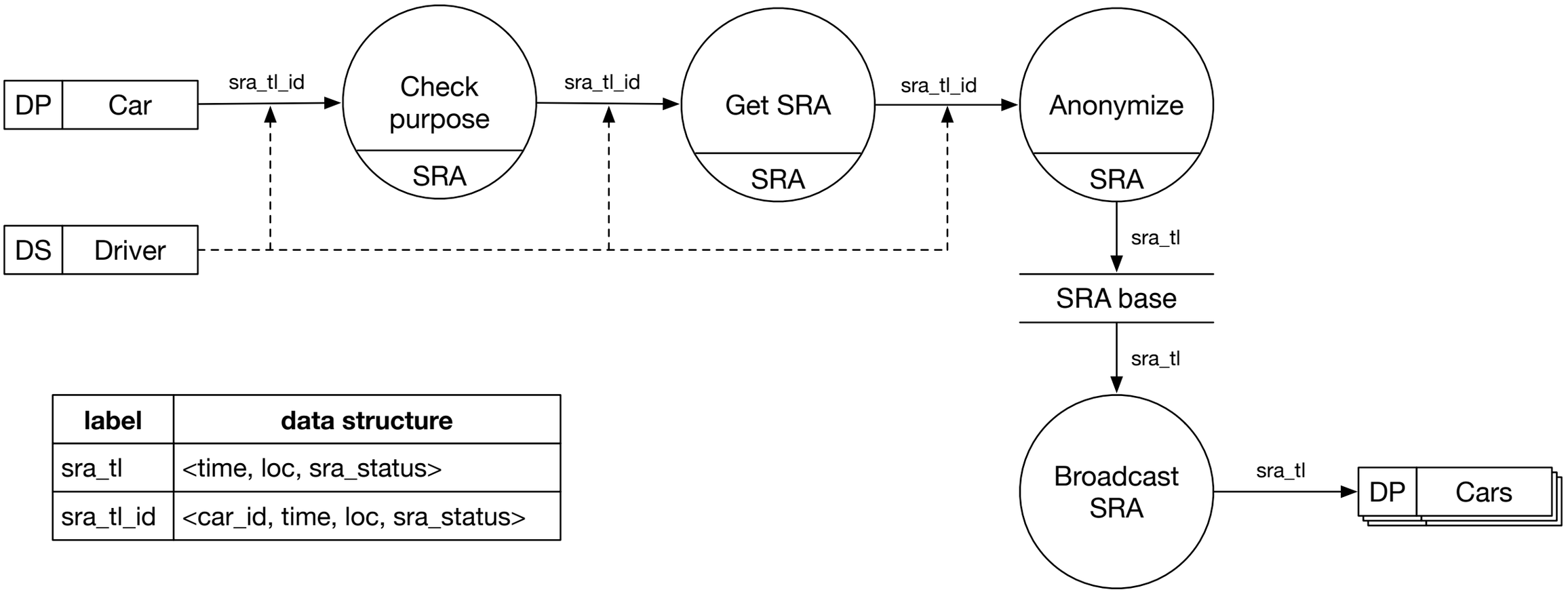


Business SRA



label	data structure
sra_tl_id	<car_id, time, loc, sra_status>

Privacy-aware SRA



label	data structure
sra_tl	<time, loc, sra_status>
sra_tl_id	<car_id, time, loc, sra_status>