Lawful and Accountable Personal Data Processing with GDPR-based Access Control

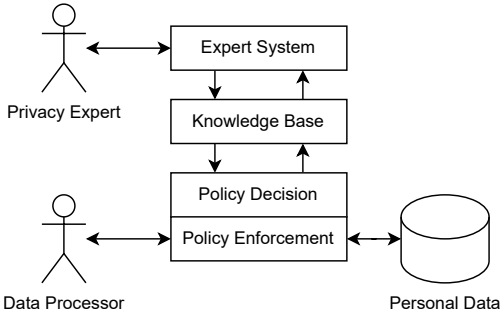
L. Thomas van Binsbergen, Marten Steketee, Milen Kebede, Heleen Janssen, Tom van Engers

Informatics Institute, University of Amsterdam
ltvanbinsbergen@acm.org

December 18, 2024

Contributions

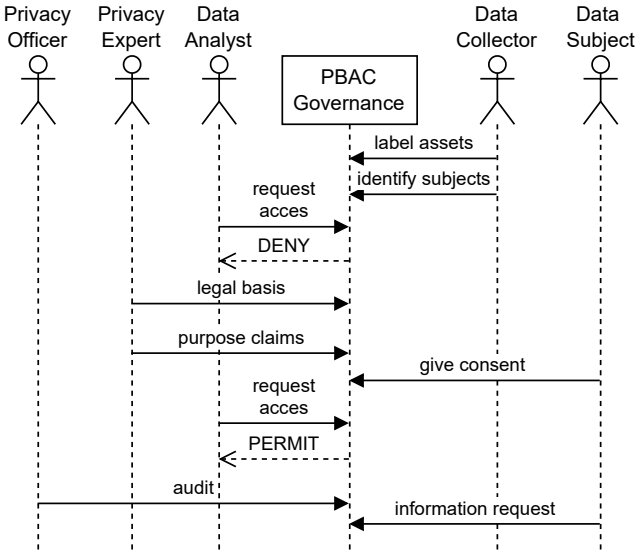
Goal: Develop a knowledge-based, expert system for reasoning with GDPR-compliance and generating authorisations in distributed access and usage control implementations.



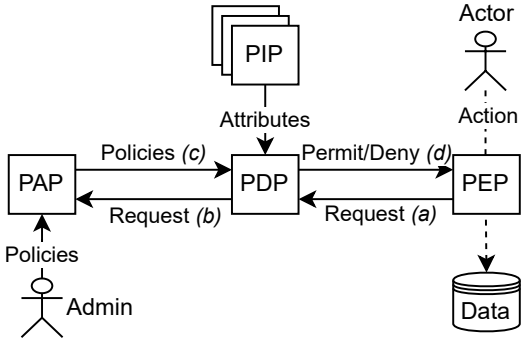
Contributions:

- Raising the level of *abstraction* of policy specification to the level of the *domain-expert*.
  Before: System administrator sets (low-level) access policies
  After: Privacy expert submits claims regarding purposes and legal bases
- Authorisations are generated only when processing of legal data is lawful (according to the GDPR) in a *certifiable* and *accountable* manner

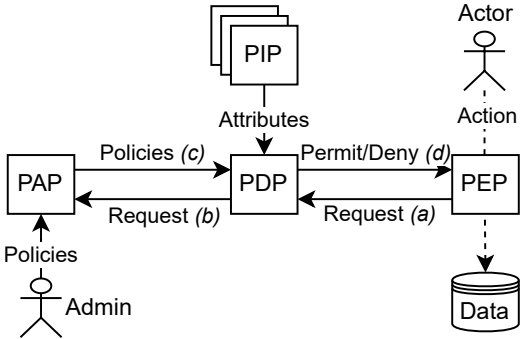
System interactions



Access Control (AC) revisited

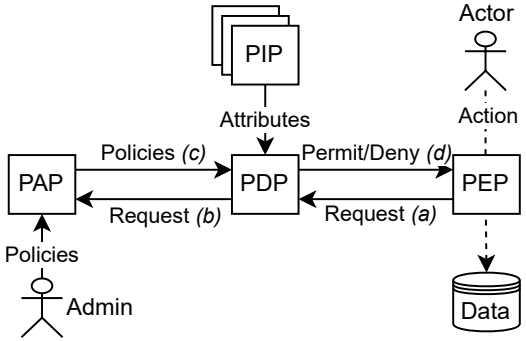


Access Control (AC) revisited



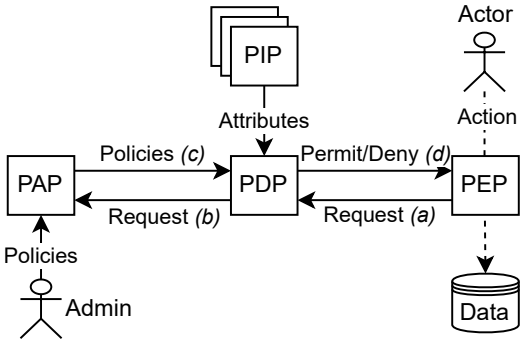
- Request consists of *Actor*, *Action*, *Asset*

Access Control (AC) revisited



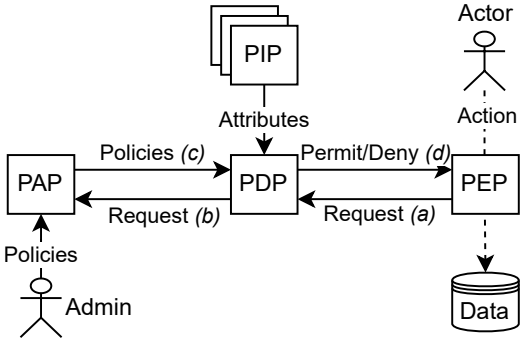
- Request consists of *Actor*, *Action*, *Asset*
- Role-Based AC: $Role(Actor) \leq RolePermitted(Action, Asset)$

Access Control (AC) revisited



- Request consists of *Actor*, *Action*, *Asset*
- Role-Based AC: $Role(Actor) \leq RolePermitted(Action, Asset)$
- Purpose-Based AC: $Purpose(Role(Actor), Action) \leq PurposePermitted(Asset)$

Access Control (AC) revisited



- Request consists of *Actor*, *Action*, *Asset*
- Role-Based AC: $Role(Actor) \leq RolePermitted(Action, Asset)$
- Purpose-Based AC: $Purpose(Role(Actor), Action) \leq PurposePermitted(Asset)$
- GDPR-Based AC: $Purpose(Actor, Action) \lesssim Purpose(LegalBasis(...))$

Overview

1. Legal analysis
2. Ontology
3. Semantic specification (inference rules)
4. Semantic implementation (eFLINT)
5. Policy specification (purpose details, consent)
6. System integration (XACML, AMdEX)
7. Reflections

Legal Analysis (1)

Definition

A controller can claim a *legal basis* for processing for a specific lawful purpose if the processing is lawful according to the GDPR (Art. 6), in which case one of the following applies:

- the data subject has given consent (Art. 6(1)(a)), or
- the processing is necessary for:
  - the performance of a contract with the data, or subject (Art. 6(1)(b)), or
  - compliance with a legal obligation (Art. 6(1)(c)), or
  - the vital interest of subject or natural person (Art. 6(1)(d)), or
  - public interest or vested authority (Art. 6(1)(e)), or
  - the controller has a legitimate interest (Art. 6(1)(f)).

And all data subjects involved must be informed about the legal basis and purpose, prior to the processing.

Legal Analysis (2)

Definition

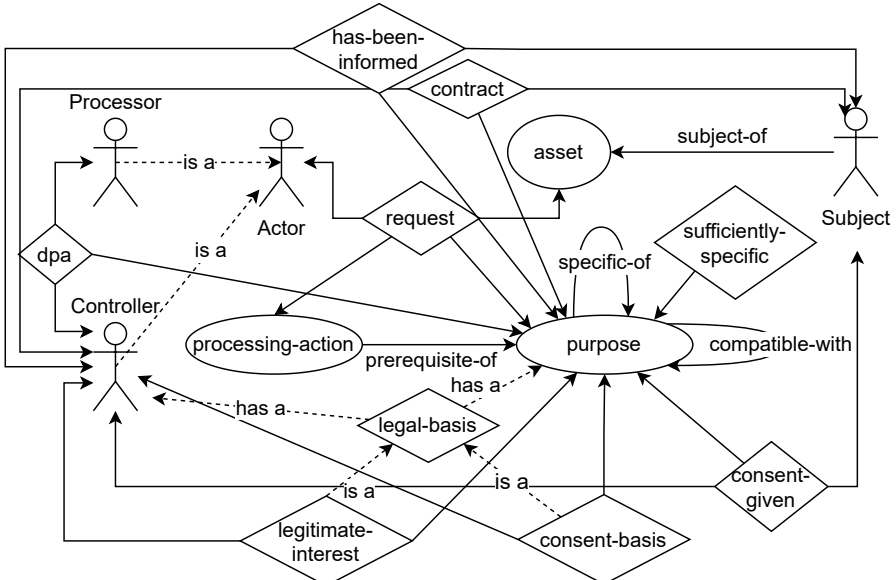
A *purpose-based processing request* connects an actor (a processor or controller) to a processing action, performed on an asset for a prescribed processing purpose. The request is considered lawful if:

- the action is prerequisite of the processing purpose, and
- the processing purpose is *sufficiently specific*, and
- the processing purpose:
  - coincides with a purpose that has a lawful legal basis, or
  - is more specific than a purpose that has a lawful legal basis, or
  - is not incompatible with a purpose that has a lawful legal basis.

Definition

A purpose is a *specific-of* of another purpose if it concretises a more abstract purpose without including elements not contained in the more abstract purpose.

Ontology of GDPR concepts



Examples of semantic specification rule

$$\frac{\textit{legitimate-interest}(C, P) \quad \textit{sufficiently-specific}(P) \quad \forall_S(\textit{subject-of}(S, D) \rightarrow \textit{has-been-informed}(S, C, P))}{\textit{legal-basis}(C, P, D)} \tag{1}$$

Examples of semantic specification rule

$$\frac{\textit{legitimate-interest}(C, P) \quad \textit{sufficiently-specific}(P) \quad \forall_S(\textit{subject-of}(S, D) \rightarrow \textit{has-been-informed}(S, C, P))}{\textit{legal-basis}(C, P, D)} \tag{1}$$

$$\frac{\textit{request}(U, A, P, D) \quad \textit{prerequisite-of}(A, P) \quad \textit{specific-of}(P, P') \quad \textit{legal-basis}(C, P', D) \quad \textit{processor-for}(U, C, P')}{\textit{lawful-request}(U, A, P, D)} \tag{2}$$

Examples of semantic specification rule

$$\frac{\textit{legitimate-interest}(C, P) \quad \textit{sufficiently-specific}(P) \quad \forall_S(\textit{subject-of}(S, D) \rightarrow \textit{has-been-informed}(S, C, P))}{\textit{legal-basis}(C, P, D)} \tag{1}$$

$$\frac{\textit{request}(U, A, P, D) \quad \textit{prerequisite-of}(A, P) \quad \textit{specific-of}(P, P') \quad \textit{legal-basis}(C, P', D) \quad \textit{processor-for}(U, C, P')}{\textit{lawful-request}(U, A, P, D)} \tag{2}$$

$$\frac{\begin{array}{c}\textit{request}(U, A, P, D) \quad \textit{prerequisite-of}(A, P) \quad \textit{sufficiently-specific}(P) \\ \textit{compatible-with}(P, P') \quad \textit{legal-basis}(C, P', D) \quad \textit{processor-for}(U, C, P') \\ \forall_S(\textit{subject-of}(S, D) \rightarrow \textit{has-been-informed}(S, C, P))\end{array}}{\textit{lawful-request}(U, A, P, D)} \tag{3}$$

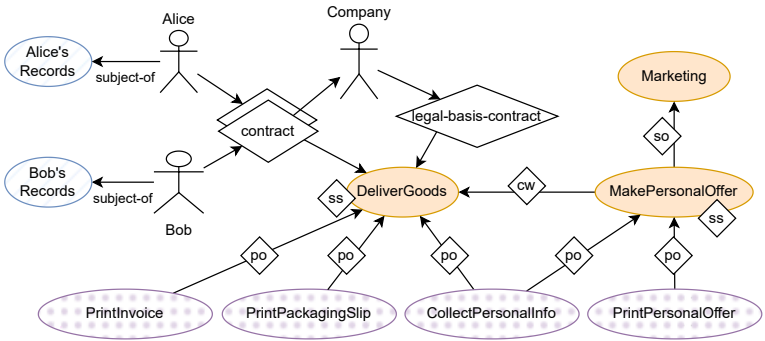
Example eFLINT fragments implementing semantics

```
Fact lawful-request
  Identified by actor * processing-action * purpose * asset
  Conditioned by request() // only considers created requests
```

```
Extend Fact lawful-request
  Holds when prerequisite-of(processing-action, purpose)
         && specific-of(purpose, purpose')
         && legal-basis(controller, purpose', asset)
         && processor-for(actor, controller, purpose')
```

```
Extend Fact lawful-request
  Holds when prerequisite-of(processing-action, purpose)
         && sufficiently-specific(purpose)
         && compatible-with(purpose, purpose')
         && legal-basis(controller, purpose', asset)
         && processor-for(actor, controller, purpose')
         && has-been-informed(subject, controller, purpose)
```

Example purpose graph and scenarios



(a.) The processing actions that are prerequisites of delivering goods are lawful, for each individual subject, if a contract exists with that subject and for that purpose.

(b.) The further processing of the data to print and include a personal offer may be lawful depending on whether this purpose is considered to be incompatible with the delivery.

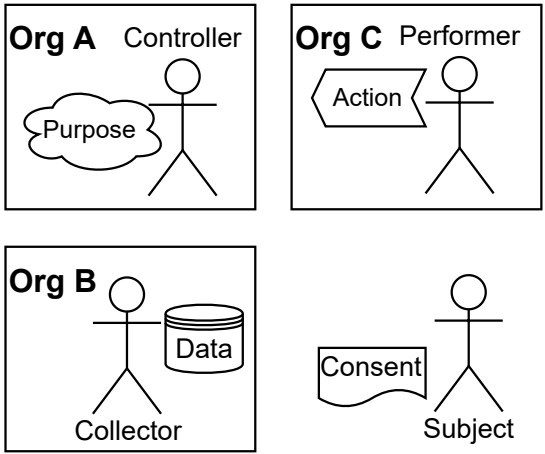
(c.) If, instead, the company asks for consent as a legal basis, the consent needs to state 'making a personal offer' and not 'marketing' as the latter is not deemed to be sufficiently specific.

Overview

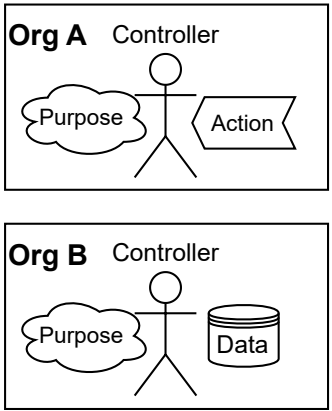
1. Legal analysis
2. Ontology
3. Semantic specification (inference rules)
4. Semantic implementation (eFLINT)
5. Policy specification (purpose details, consent)
6. System integration (XACML, AMdEX)
7. Reflections

Archetypical patterns of processing activities

Distributed Archetype



Independent Controllers Archetype



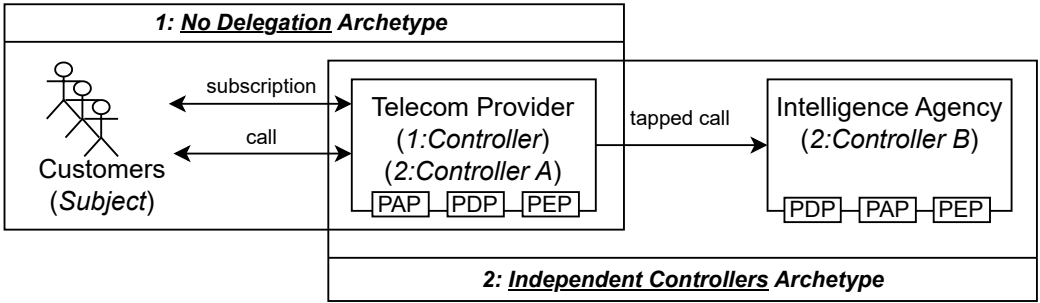
Policy administration capabilities and roles

Capability	**Policy (purpose-graph) contributions**	**Assigned to**
Control	legal-basis, dpa, has-been-informed, contract(s) (if applicable)	Controller, Authority
Qualify	prerequisite-of, compatible-with, specific-of, sufficiently-specific	Controller, Authority
Collect	asset(s), subject-of	Collector
Perform	request	Performer Collector
Consent	consent-given (including withdrawal of consent)	Subject

Policy administration capabilities and roles

Processing Archetype	Organisation	Policy Administration Roles
No Delegation	Controller	Controller, Collector, Performer
Delegated Action	Controller	Controller, Collector
	Performer	Performer
Delegated Processing	Controller	Controller
	Performer	Collector, Performer
Delegated Collection	Controller	Controller, Performer
	Collector	Collector
Distributed	Controller	Controller
	Collector	Collector
	Performer	Performer
Independent Controllers	Controller A	Controller, Collector
	Controller B	Controller, Performer

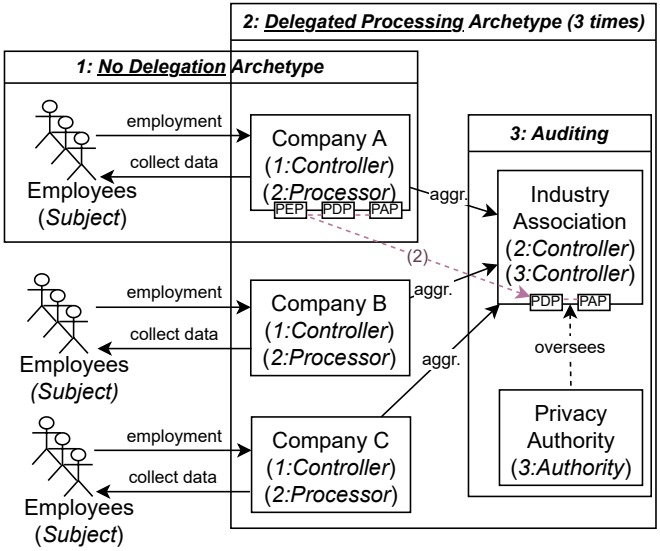
Example case: KPN and wiretapping



Scenario 2 checks:

- Upon sending: KPN's PEP confers with KPN PDP for *collecting*
- Upon receiving: Agency's PEP confers with Agency PDP for *performing*

Example case: industry benchmarking



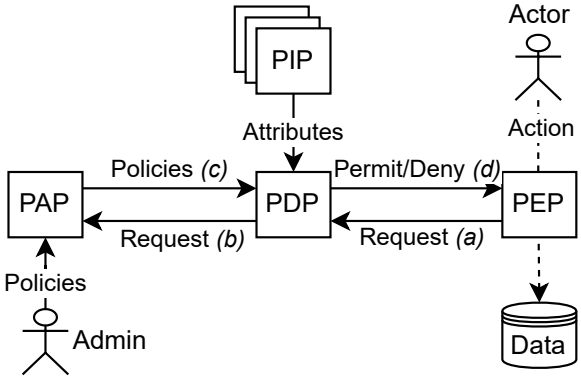
Scenario 1 checks:

- Company's PEP confers with local PDP for both collecting and performing (e.g., 'pay salary')

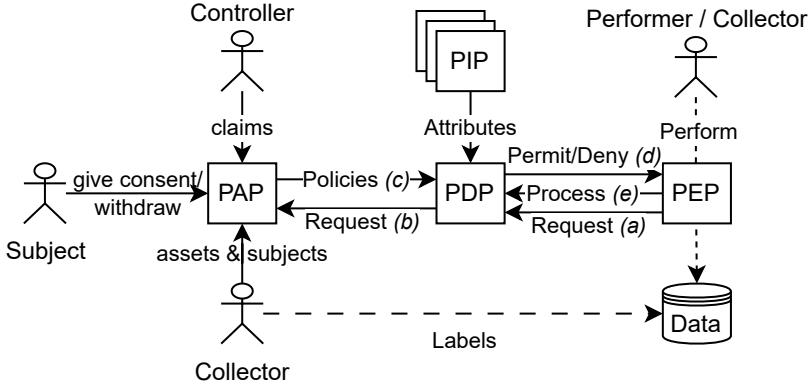
Scenario 2 checks:

- Company's PEP confers with Association's PDP for both collecting and performing (e.g., 'total salary, employee count')

Simplified XACML architecture (technical roles)

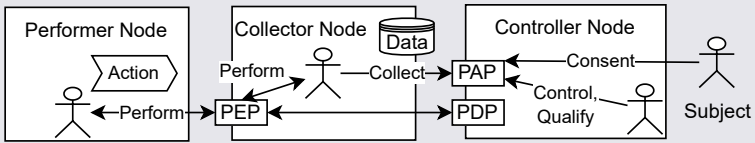


Simplified XACML architecture with PBAC policy administration



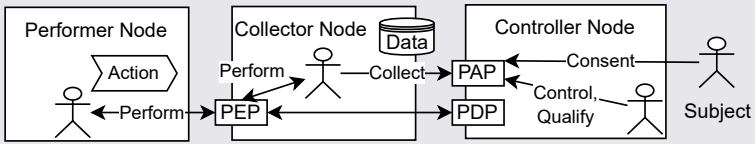
Mapping roles unto data exchange systems

Self-governed peer-to-peer system (distribution archetype)

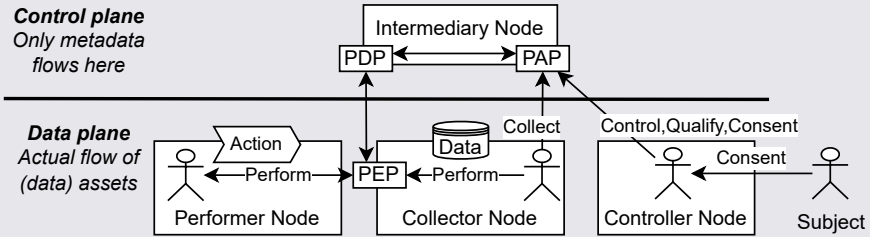


Mapping roles unto data exchange systems

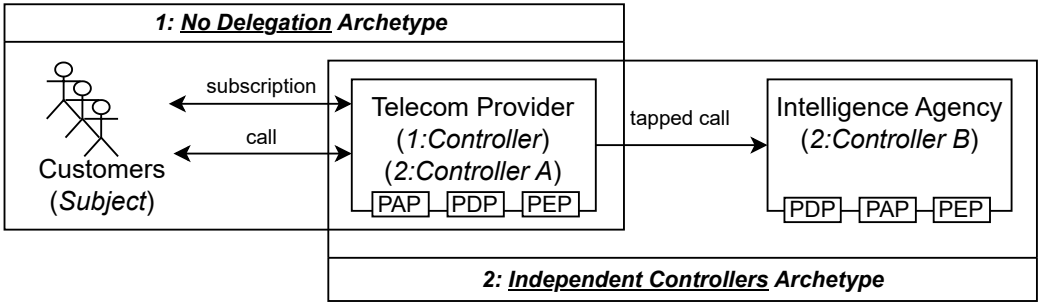
Self-governed peer-to-peer system (distribution archetype)



Peer-to-peer system governed by intermediary (AMdEX)



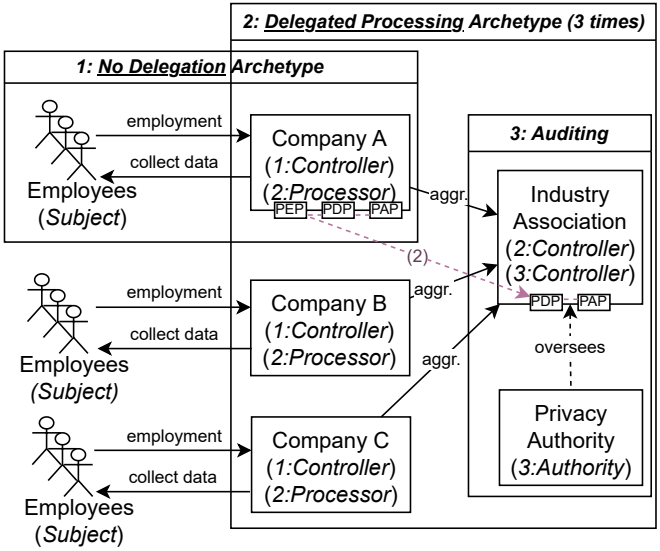
Example case: KPN and wiretapping



Scenario 2 checks:

- Upon sending: KPN's PEP confers with KPN PDP for *collecting*
- Upon receiving: Agency's PEP confers with Agency PDP for *performing*

Example case: industry benchmarking



Scenario 1 checks:

- Company's PEP confers with local PDP for both collecting and performing (e.g., 'pay salary')

Scenario 2 checks:

- Company's PEP confers with Association's PDP for both collecting and performing (e.g., 'total salary, employee count')

Reflections on accountability and explainability

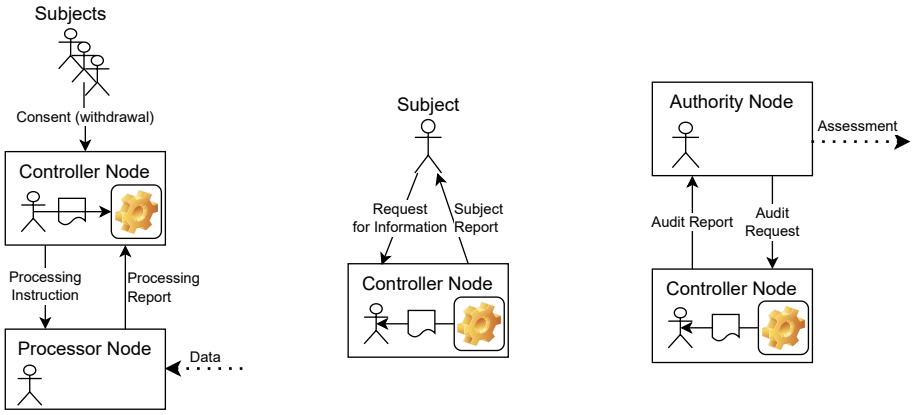


Figure: Different reasoning scenarios with different stakeholders.

Model Evolution

Reflected in current solution

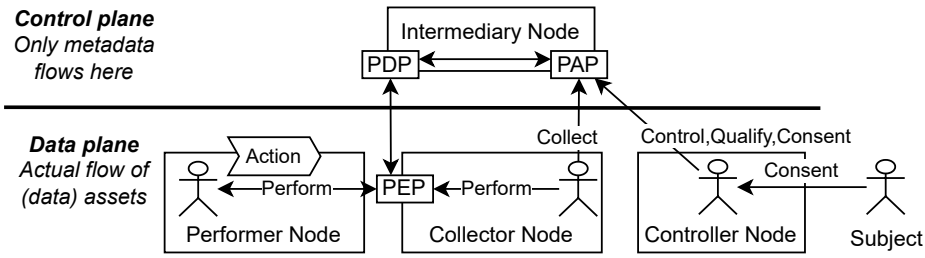
- Original and further processing purposes need to be *sufficiently specific*
- Requirement to *inform subjects* of legal bases, prior to processing
  $\hookrightarrow$ which in some cases can be inferred
- Requirement to specify *processing purpose*

Necessary updates to be made

- Cases with two or more *independent controllers* (Control vs Perform capability)
- Cases with *joint controllership*

Future Work – AMdEX integration

We aim to show feasibility within the current AMdEX-DMI project.



Lawful and Accountable Personal Data Processing with GDPR-based Access Control

L. Thomas van Binsbergen, Marten Steketee, Milen Kebede, Heleen Janssen, Tom van Engers

Informatics Institute, University of Amsterdam
ltvanbinsbergen@acm.org

December 18, 2024