Engaging Content
Engaging People

A Semi-Automated Methodology for extracting access control rules from the EU- DPD

Dr. Kaniz Fatema
Research Fellow
ADAPT Centre

Trinity College Dublin, Ireland
E: Kaniz.Fatema@scss.tcd.ie

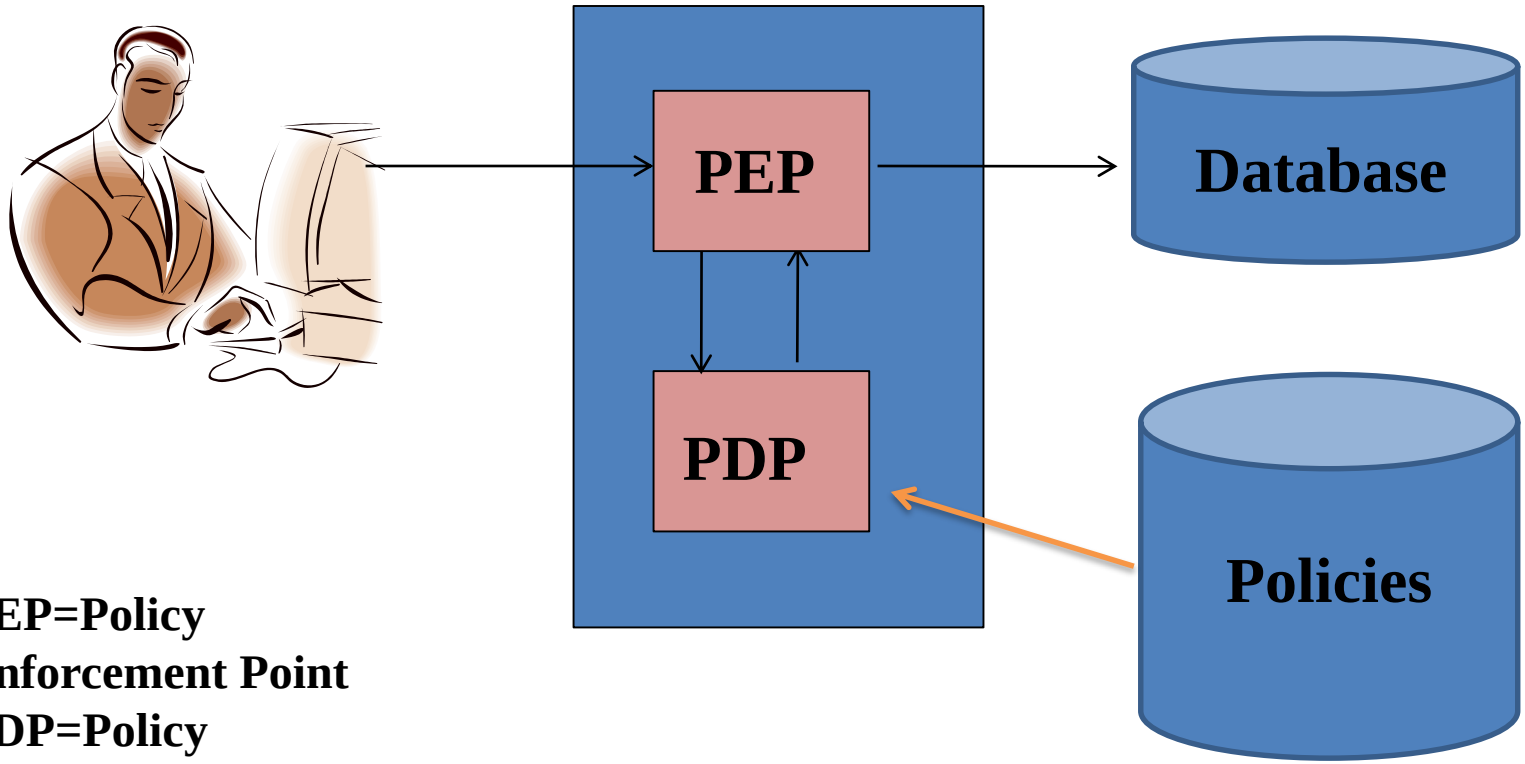
IWPE 16, San Jose, CA.

Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union
European Union
European Regional Development Fund
SFI Science Foundation Ireland

The ADAPT Centre is funded under the SFI Research Centres Programme (Grant 13/RC/2106) and is co-funded under the European Regional Development Fund.

Policy Based Authorisation System

Access to the resource is protected by policies.



PEP=Policy Enforcement Point
PDP=Policy Decision Point

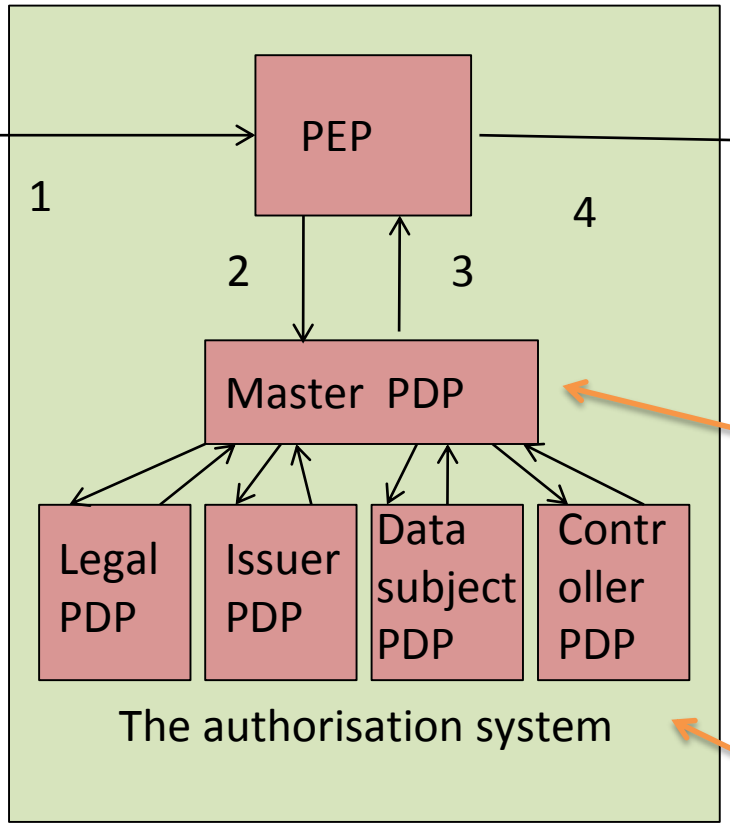
Authorisation system

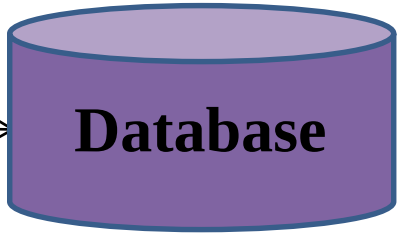
Authors of Privacy Policies

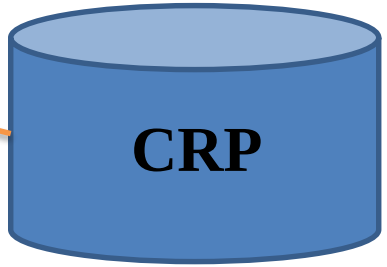
Privacy Policies may be defined by a number of authors.

- **Data subject,** - whose data is being accessed.
- **Issuer**, e.g.- The Doctor for medical note, University for degree certificate, data subject is the issuer of personal information such as favorite drink.
- **Controller,** e.g.- the health insurance company holding medical record of the data subject, or facebook for personal data.
- **Law**, e.g.- EU data protection directive.

The Proposed System (in a Simplified Form)







CRP=Conflict Resolution Policy
CRR=Conflict Resolution Rule {condition, DCR}
DCR=Decision Combining Rule

The Methodology for Obtaining Legal Policies

- **Step1.** **Listing the Legal provisions that are directly related to access control.**
- **Step2.** **Analysing and Extracting the Legal Access Control Policy**
- **Step3.** **Refining the Access Control Policies**
- **Step4.** **The formalization of the access control rules using CNL**
- **Step 5.** **Convert the controlled natural language rules into executable rules**
- **Step 6.** **Validate the obtained Legal rules.**

Step1. Listing the Legal Provisions Related to Access Control.

The European Union Data Protection Directive consists of eight chapters and 34 articles. For our implementation we considered only the articles directly related to access control.

Keywords: **process**, **prohibit**, **access**, **collect**, **block**, **transfer** (i.e. mentions an action on personal data)

Step 1 (continued…)

For example, Article 8.4 states that “Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those **laid down in paragraph 2** either by national law or by decision of the supervisory authority.”

Step2. Analysing and Extracting the Legal Access Control Policy

Access control rules are those that are capable of answering **who** is allowed to do **what** on personal data under what **condition/s**.

or

On **what** conditions the personal data can be accessed.

Analysing the Legal Texts in Step 2

The article 6.1 (a) says
“personal data must be processed fairly and lawfully”

–This legal rule is too vague to form an automated access control rule.

Later in article 7 the criteria for making data processing legitimate are described,
these are converted into access control rules.

Analysing the Legal Texts in Step 2 (Cont...)

Article 12(b) states that "as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive"

This is not possible to convert into an automated rule as it requires human judgement to ensure that the processing complies with the directive or not.

Analysing the Legal Texts in Step 2 (Cont...)

Article 7(f) “processing of personal data for legitimate interest are allowed **except** where such interests are **overridden by the fundamental rights and freedom of data subject”**

It presents an extremely complex condition where the balance of interests are not feasible to be presented in an access control policy.

Step3. Refining the Access Control Policies

- Grouping similar rules together.
- Ordering them in terms of the exceptions that need to be evaluated before the ones without exceptions.

For example, data subjects are allowed unconditional access to their personal data that are held by a data controller, but not if law enforcement would be jeopardised by this. Consequently the rule that concerns law enforcement must be evaluated before the rule that grants the data subject unconditional access.

Step4. The Formalization Rules Using CNL

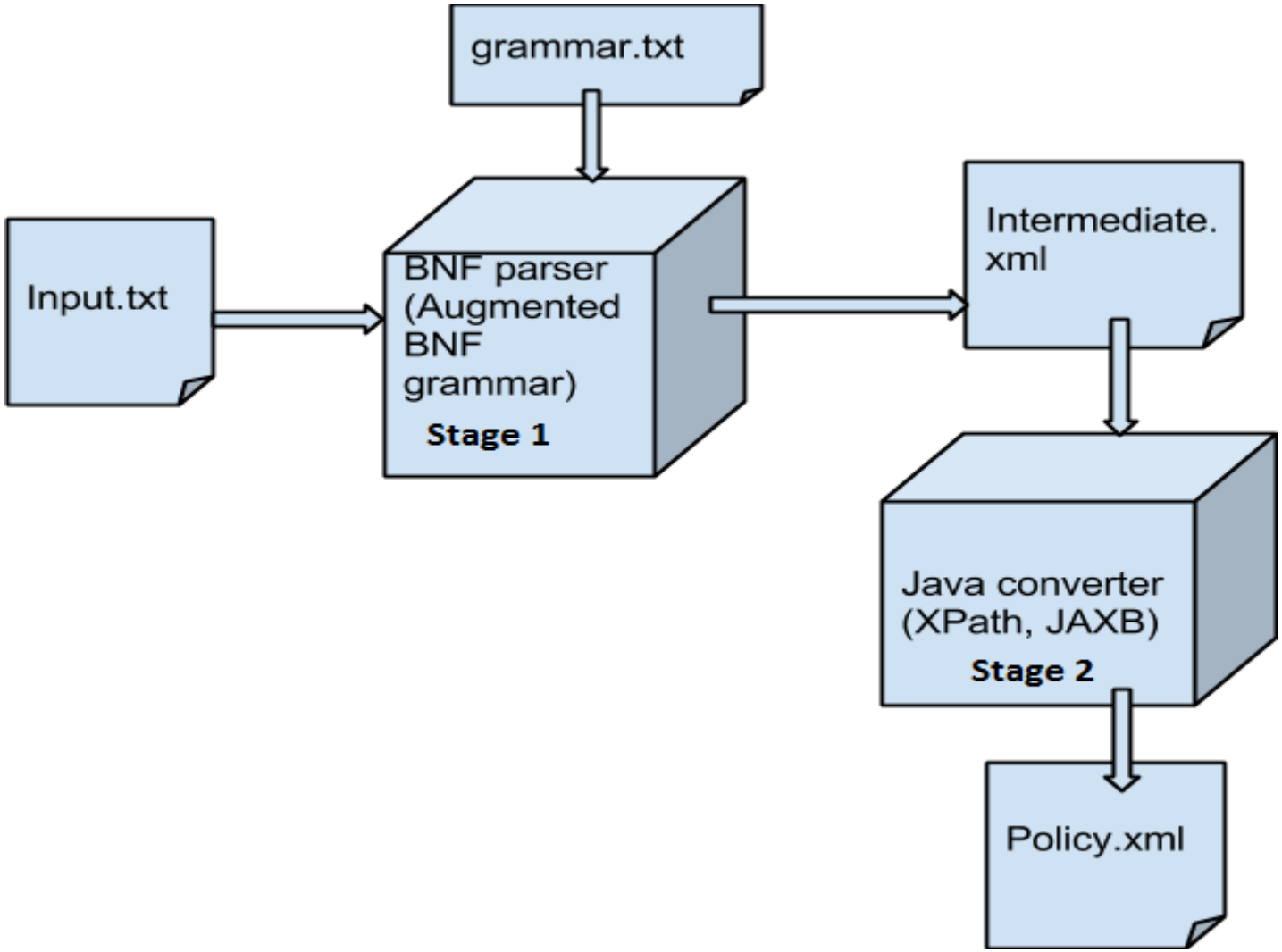
- **Subject** (who)
- **Action** (can/cannot perform what)
- **Resource** (on which data item)
- **Condition** (under which conditions)
- **Effect** (grant/deny/BreakTheGlass)
- **Obligation** (subject to these actions being carried out)

Example of CNL Converted Rules

Policy No.	Articles	Legal Natural Language Policies
1.	Article 6.1 (b)	If the requested purpose of processing does not match with any of the original purposes of collection or is not for a historical purpose/statistical purpose / scientific purpose deny the request.

No. of rule	Controlled Natural Language Rule in ABNF
1.	ACR 1: If the Action:Purpose:string is not the Resource:PurposesOfCollection:string OR the Action:Purpose:string is not a "historical purpose" / "statistical purpose" / "scientific purpose" then Deny the Access to the PersonalData.

Step 5. Convert the CNL into Executable Rules



Example of intermediate.xml

“ACR 3: If the Environment:RequestTime: date is less than Resource:ValidityTime:date then Deny the Access to the PersonalData.”

CNL rules

```
<rule-definition>ACR
<rule-id><STRING>3</STRING></rule-id>:
<rule-statement>If
<conditions><condition>
<article>the</article>
<attributes><attribute>
<category>Environment</category>:
<name><STRING>RequestTime</STRING>
</name>:<type>date</type>
</attribute></attributes>
<relationalOperator>is less than</relationalOperator>
<attributes><attribute>
<category>Resource</category>:
<name><STRING>ValidityTime</STRING>
</name>:<type>date</type></attribute></attributes>
</condition></conditions> then
<GrantOrDeny>Deny</GrantOrDeny><article>the</arti
cle>
<actions><action><word>Access</word></action></ac
tions>
<prep>to</prep><article>the</article>
<ResourceType><word>PersonalData</word></Resour
ceType></rule-statement>.</rule-definition>
```

Example of XACML policy produced from the input.txt


```
<attribute>
<category>Resource</category
>:
<name><STRING>ValidityTime
</STRING>
</name>:<type>date</type><
/attribute>
```

Intermediate.xml

```
<ResourceAttributeDesign
ator
AttributeId="ValidityTime"
DataType="http://www.w3.or
g/2001/XMLSchema#date"/>
```

XACML policy.xml

Step 6. Validate the Obtained Legal Rules

Use Cases

Subject

Chooses preferences

Authorisation system of Kent Health Centre

Preferences are converted into policies

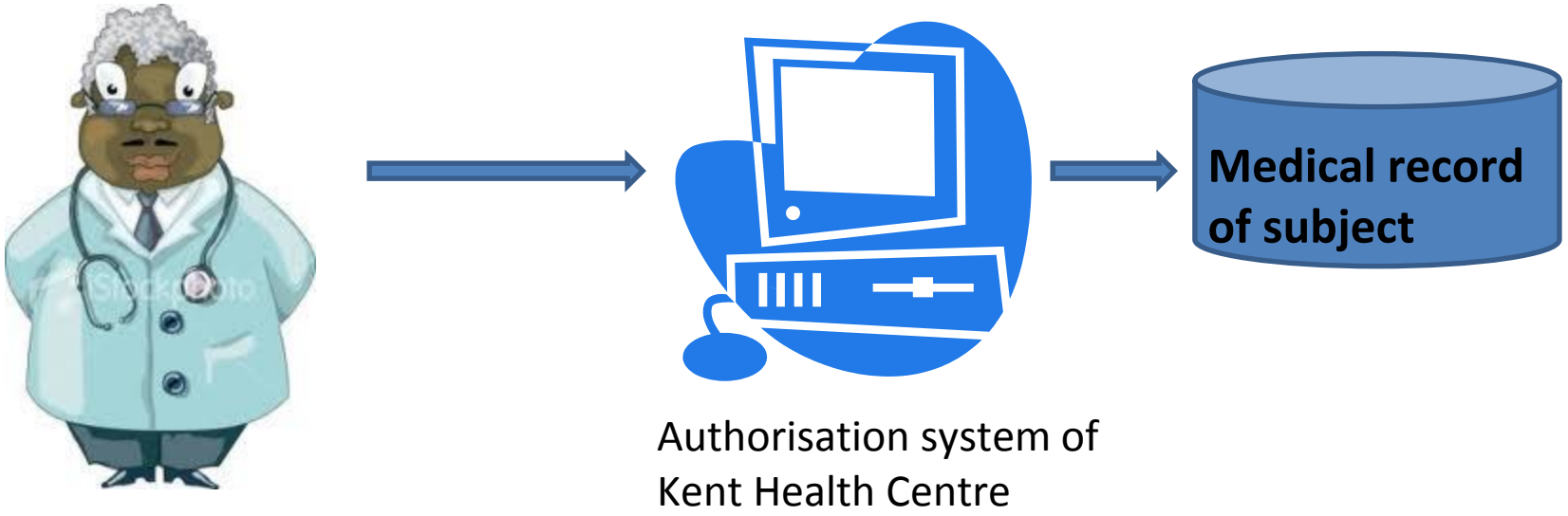
Data Subject's PDP

Data Subject's Policy

- **The Doctor of Kent Health centre can read / write /update my medical data.**

- **Researcher are allowed to read my medical data if the data can be anonymised.**

Use Cases (Continued …)



Treating Dr

Legal CRP returns DCR=GrantOverrides
Legal PDP returns decison = Grant

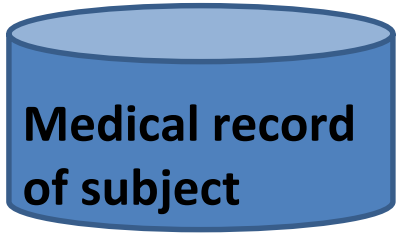
Use Cases (Continued …)

Subject

Authorisation system of Kent Health Centre

Legal CRP returns DCR=GrantOverrides
Legal PDP returns decision = Grant

Use Cases (Continued …)



Authorisation system of
Kent Health Centre

Dr at London hospital

Legal CRP returns DCR=GrantOverrides
Legal PDP returns decision = BTG

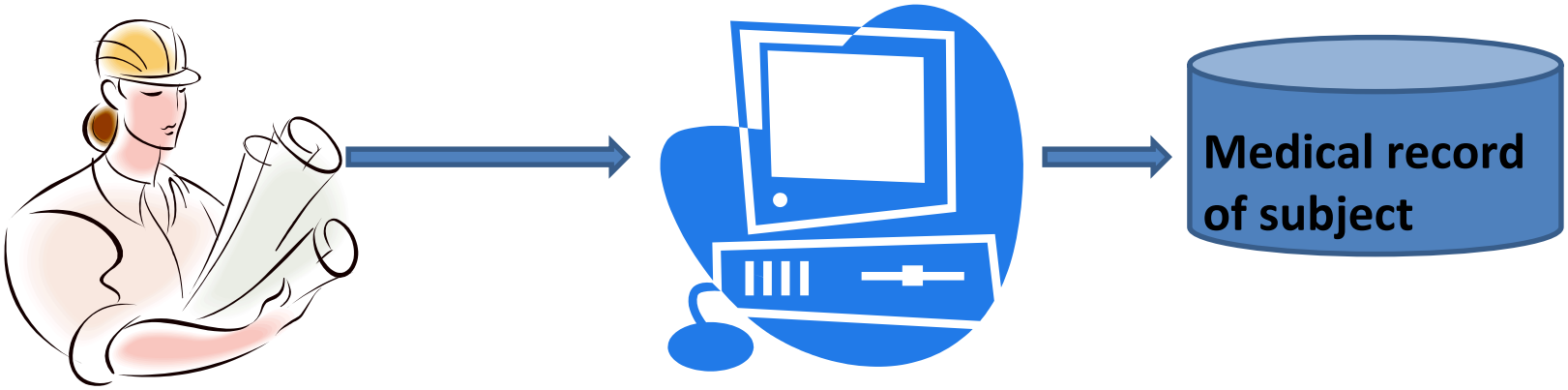
Use Cases (Continued …)

Subject

Authorisation system of Kent Health Centre

Therapeutic Exception=true
Legal CRP returns DCR=DenyOverrides
Legal PDP returns decision = Deny

Use Cases (Continued …)



Researcher

Authorisation system of Kent Health Centre

Legal CRP returns DCR=DenyOverrides Data Subject's PDP returns decision = Grant with obligation to anonymise data

Facts and Findings

We applied our approach on 53 rules of the EU DPD.

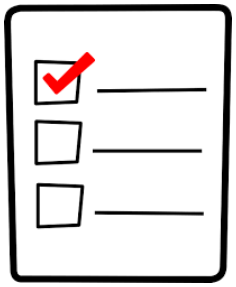
From the 53 rules of the EU DPD that were considered for analysis in step 2, 27 of them could contribute to the construction of enforceable authorisation rules.

However, 14 rules among these 53 are found to be guidelines or instructions only and did not therefore map into authorisation rules. 3 rules are supported by the system design.

The remaining 9 rules are found to be too dependent on other laws or human judgement to be turned into access control rules by themselves.

Previous Work in a Nutshell

Interface for preference selection

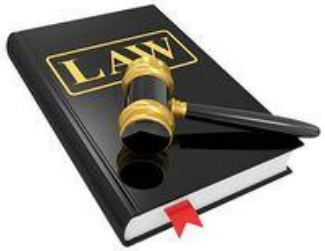


Data Subjects' preferences

↓

Enforceable Rules

EU DPD



Legal text

↓

CNL

↓

Enforceable Rules

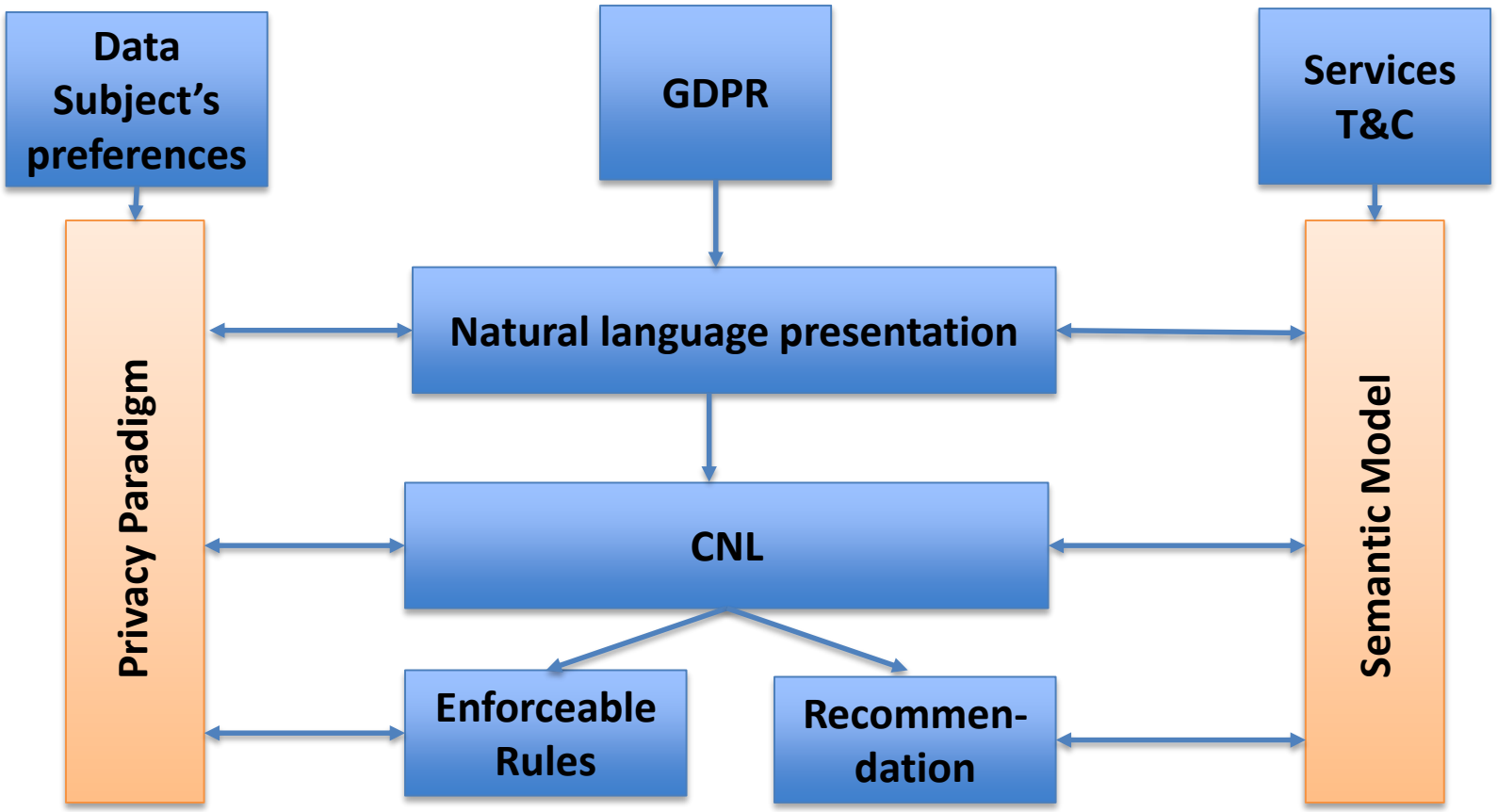
System Admin

Organisation's policy

↓

Enforceable Rules

Future Direction



CONSENT ⟷ COMPLIANCE

Question?

Thank You