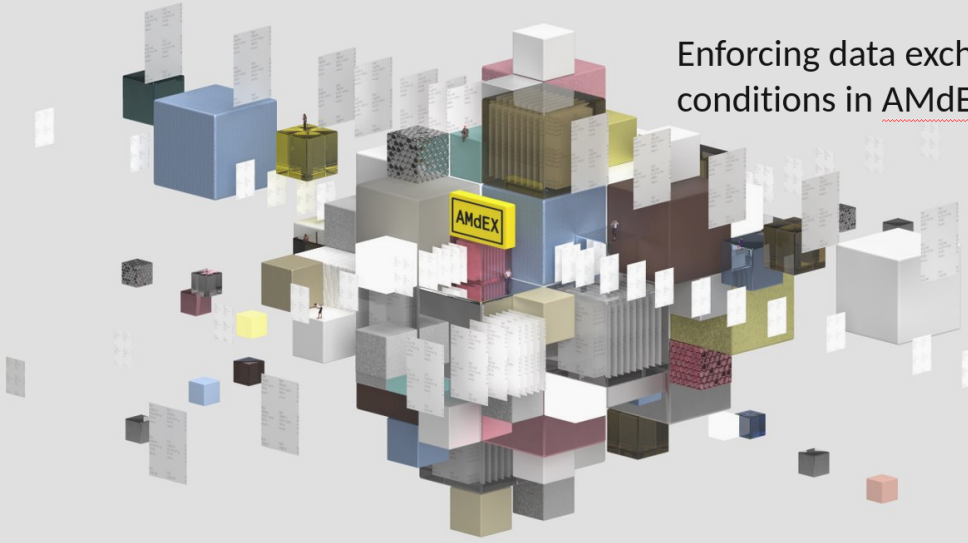
Enforcing data exchange conditions in AMdEX

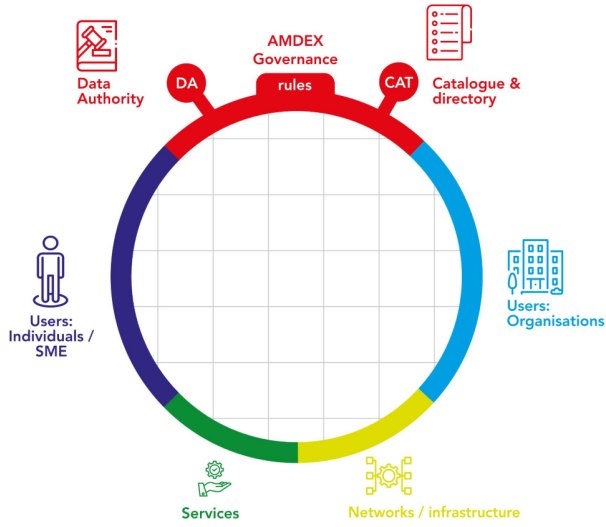


L. Thomas van Binsbergen – Informatics Institute, University of Amsterdam

European Union
European Regional Development Fund

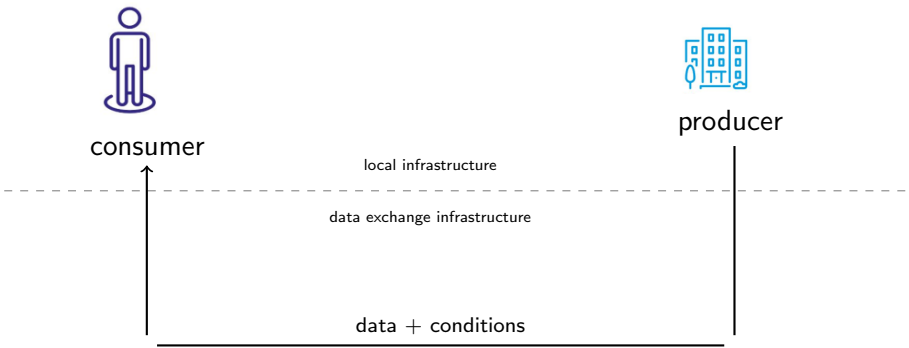
Data Authority:

> **Administer** *laws, agreements, and conditions regulating the access, exchange and processing of data and* **automatically enforcing compliance** *where possible, making available* **auditing** *information to participants*



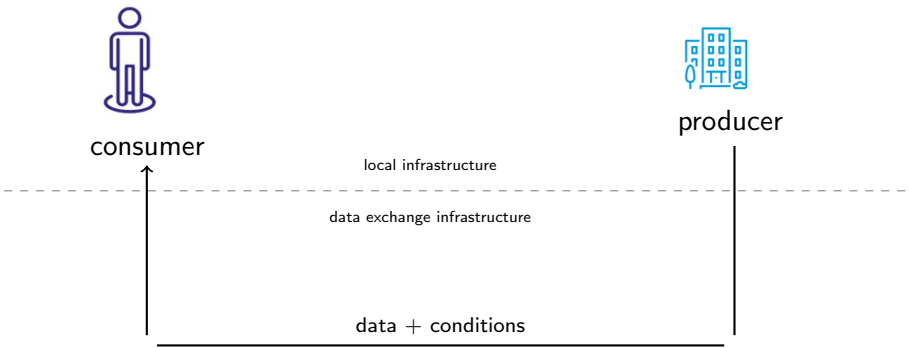
Enforcement

Signature enforcement: consumer digitally signs sharing conditions



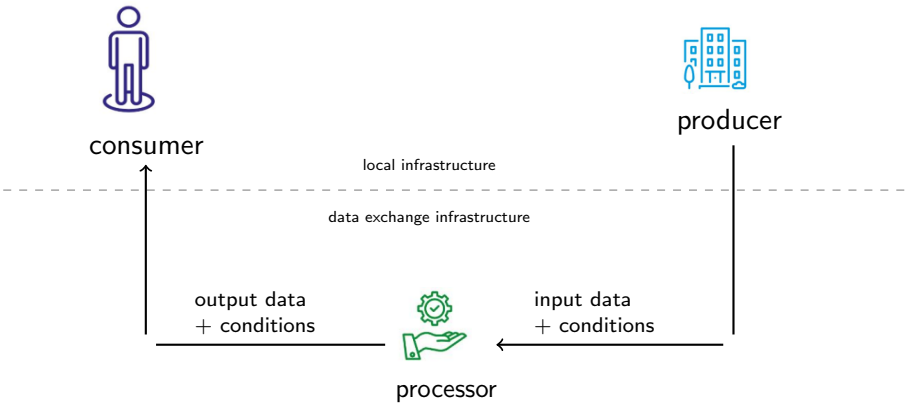
Enforcement

Access control: authorise or prevent exchange on the border between infrastructures



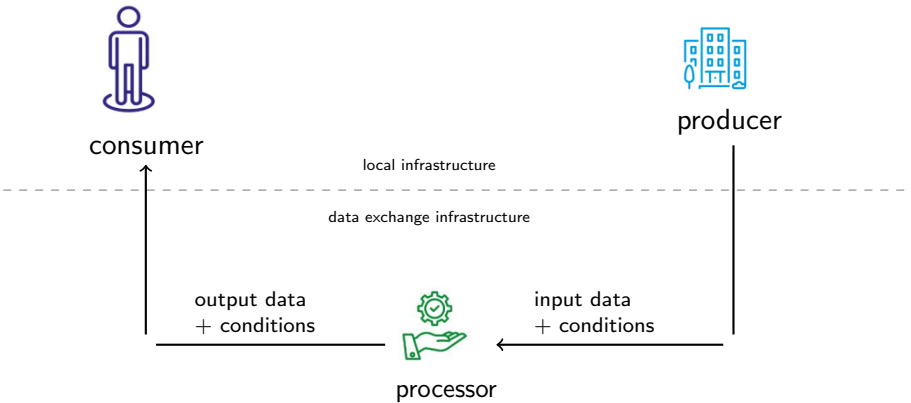
Enforcement

Usage control: authorise or prevent processing based on the data and processing service



Enforcement

Usage control: authorise or prevent processing based on the data and processing service



RQ: How to specify or infer conditions placed on the output data? Signature enforcement?

Method

Connecting: **legal** with **formal** and **enforceable**

eFLINT: A Domain-Specific Language for Executable Norm Specifications

L. Thomas van Binsbergen
Centrum Wiskunde & Informatica
Amsterdam, The Netherlands
ltvanbinsbergen@acm.org

Lu-Chi Liu
University of Amsterdam
Amsterdam, The Netherlands
l.liu@uva.nl

Robert van Doesburg
Leibniz Institute, University of Amsterdam / TNO
Amsterdam, The Netherlands
robertvandoesburg@uva.nl

Tom van Engers
Leibniz Institute, University of Amsterdam / TNO
Amsterdam, The Netherlands
vanengers@uva.nl

Method

Connecting: **legal** with **formal** and **enforceable**

eFLINT: A Domain-Specific Language for Executable Norm Specifications

L. Thomas van Binsbergen
Centrum Wiskunde & Informatica
Amsterdam, The Netherlands
ltvanbinsbergen@acm.org

Lu-Chi Liu
University of Amsterdam
Amsterdam, The Netherlands
l.liu@uva.nl

Robert van Doesburg
Leibniz Institute, University of Amsterdam / TNO
Amsterdam, The Netherlands
robertvandoesburg@uva.nl

Tom van Engers
Leibniz Institute, University of Amsterdam / TNO
Amsterdam, The Netherlands
vanengers@uva.nl

Connecting: **interpretations** with **system policies** and **enforcement mechanisms**

Dynamic generation of access control policies from social policies

L. Thomas van Binsbergen[1,a], Milen G. Kebede[a], Joshua Baugh[b], Tom van Engers[a], Dannis G. van Vuurden[b]

[a]*Informatics Institute, University of Amsterdam, 1090GH Amsterdam, The Netherlands*
[b]*Princess Maxima Center for Pediatric Oncology, Department of Neuro-oncology, Utrecht, The Netherlands*

Lessons learnt

- Need for **staging** interpretation, specification, and specialisation processes

Lessons learnt

- Need for **staging** interpretation, specification, and specialisation processes

Lessons learnt

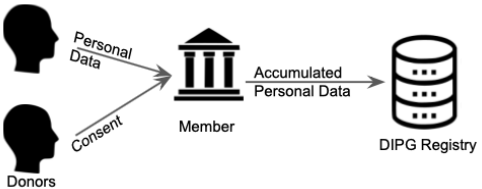
- Need for **staging** interpretation, specification, and specialisation processes

- Importance of **modularity**: extensibility, reuse, separation of concerns, building blocks

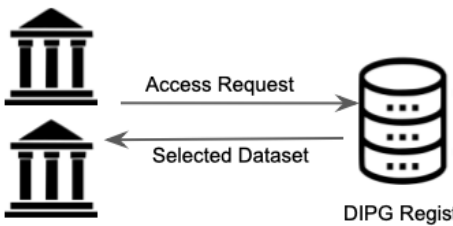
DIPG use case – compliance questions

According to the GDPR and the DIPG regulatory document:

1. What conditions need to be fulfilled by a member before making data available?



2. What conditions need to be fulfilled when accessing data from the registry?



GDPR Example

GDPR – Article 6(1)(a):

Personal data can be collected for a specific purpose if consent has been given for that purpose

GDPR – Article 5(1)(d):

Data must be accurate for purpose specified

```
Act collect-personal-data
  Actor controller
  Recipient subject
  Related to data, processor, purpose
  Conditioned by accurate-for-purpose(data, purpose), subject-of(subject,data)
  Creates processes(processor, data, controller, purpose)
  Holds when consent(subject, controller, purpose)
```

Compliance Question 1

DIPG Regulatory document – Article 4(2):

Members should transfer data to the DIPG registry in a coded form only

```
Fact coded Identified by dataset
Act make-data-available
  Actor institution
  Recipient  dcog
  Related to  dataset
  Conditioned by  coded(dataset) Holds when member(institution)
```

Compliance Question 1

```
Extend Act make-data-available Syncs with (Foreach donor:
  collect-personal-data(controller = institution
                        ,subject    = donor
                        ,data       = dataset
                        ,processor  = "DCOG"
                        ,purpose    = "DIPGResearch")
    When subject-of(donor, dataset))
```

An institution can make a dataset available when (for each donor (subject) in the dataset):

- The institution should be a member of the consortium
- Data should be coded
- Consent is given by the donor for the processing of their personal data by the DCOG for the purpose of DIPGResearch
- Data should be accurate for the purpose DIPGResearch

Compliance Question 2

DIPG Regulatory document – Article 5(9):

> *Upon receipt of the Letter of Approval signed by the Researcher, the Data necessary to perform the Project will be selected from the DIPG Registry and sent to the Researcher.*

```
Extend Act read Holds when (Exists project, institution:
  selected(asset,project) && approved(project,institution)
                          && affiliated(actor,institution))
```

An actor can *read* an asset when (there exists a project and an institution for which):

- The asset is selected for the project
- The project is approved for the institution
- The actor is affiliated with the institution

Method

Connecting: **legal** with **formal** and **enforceable**

- RQ: How to formalise interpretations of legal texts? Who are involved?
- Requires a normative specification language → eFLINT
- Requires a process to specify interpretations of norms → TNO & FLINT/eFLINT

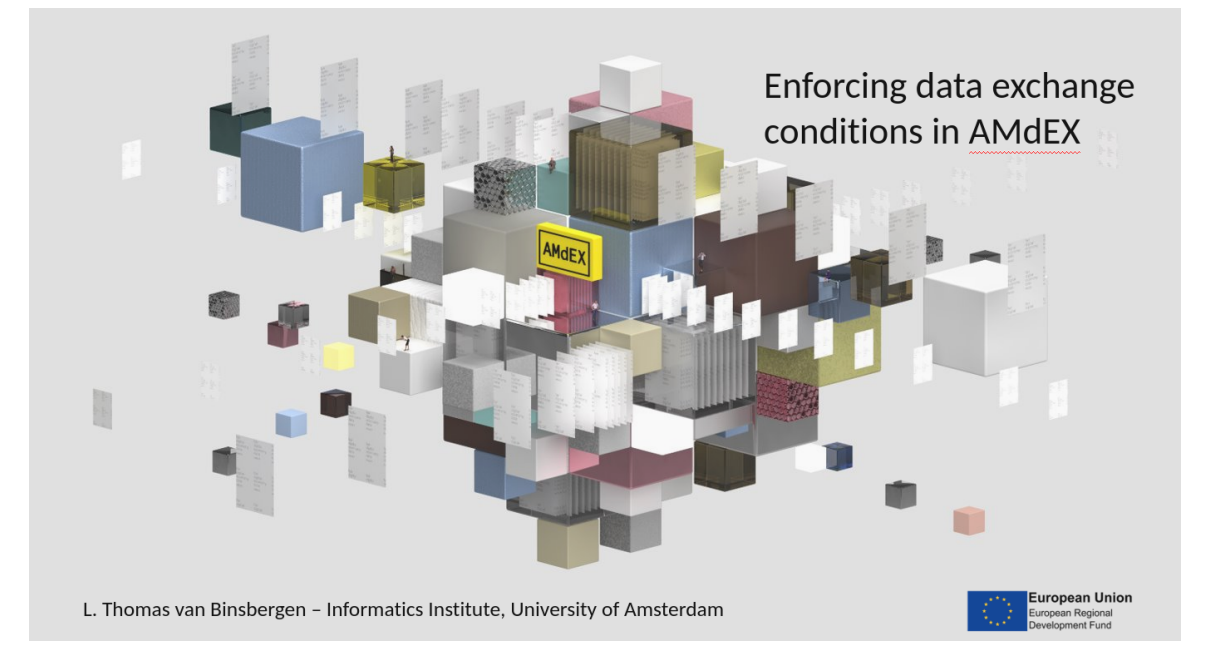
Method

Connecting: **legal** with **formal** and **enforceable**

- RQ: How to formalise interpretations of legal texts? Who are involved?
- Requires a normative specification language → eFLINT
- Requires a process to specify interpretations of norms → TNO & FLINT/eFLINT

Connecting: **interpretations** with **system policies** and **enforcement mechanisms**

- RQ: How to enforce social policies in (data exchange) infrastructures?
- Successful lab demonstrations on top of access control
- Case studies to demonstrate versatility, e.g. infrastructure configuration and usage control


Enforcing data exchange conditions in AMdEX
AMdEX
L. Thomas van Binsbergen – Informatics Institute, University of Amsterdam
European Union
European Regional Development Fund

Building blocks | Assemble | Run specification | Testing

DIPG Simplified Consortium Agreement

https://dipgregistry.eu/Content/files/2018-10-10SIOPEDIPGRegistry-RegulatoryDocument_v%202.0_final.pdf

This document is a simplified version of the original Regulatory Document as related to the DIPG Registry and Imaging Registry

Section 1: DEFINITIONS

In this consortium agreement the following terms have the meanings ascribed to them below:

Access: Access to certain Datasets in accordance to the conditions laid out in this document.

Coded: processed through pseudonymisation pursuant to the GDPR i) by or on behalf of the Member making available Data to the DIPG Registry and ii) by or on behalf of the DIPG Network making available a Dataset to a Researcher.

...

s1

Section 2: PROVIDING DATA

This section describes the conditions under which members can make data available to the Registry.

Article 1

A member of the consortium can make data available to the Registry.

s2_1_a

Placeholder patient For donor.

Fact consented Identified by patient * dataset.

Act transfer-dataset Actor member Recipient patient Related to dataset, project Conditioned by consented(patient,dataset) && coded(dataset) Creates project, project-data(project,dataset), in-registry(dataset) Holds when True.

Invariant all-data-for-research: (Forall in-registry: (Exists project-data: in-registry.dataset == project-data.dataset)).

s2_1_b

Fact patient.

Fact consented Identified by patient * dataset.

Act transfer-dataset Actor member Recipient patient Related to dataset, project Conditioned by consented(patient,dataset) && coded(dataset) Creates project, project-data(project,dataset), in-registry(dataset) Holds when True.

Invariant all-data-for-research: (Forall in-registry: (Exists project-data: in-registry.dataset == project-data.dataset)).

Article 2

Data can be made available to the Registry in Coded form only.

s2_2_a

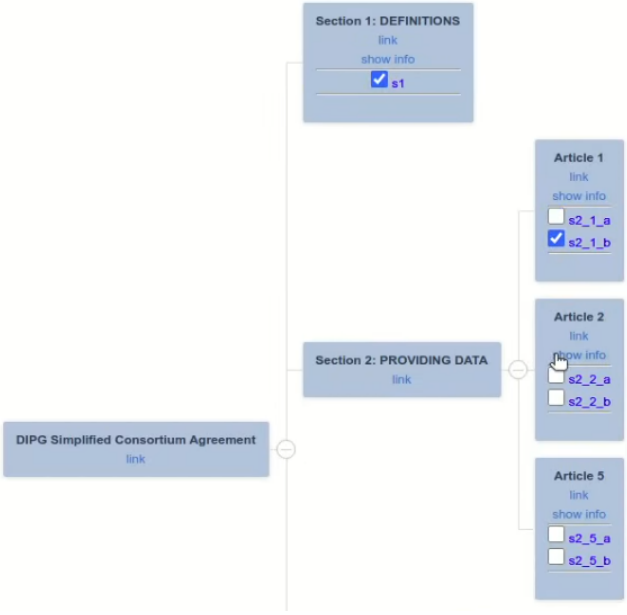
s2_2_b

Article 5

Data shall only be made available from the DIPG Registry on behalf of the DIPG Network for Projects after approval has been obtained for the Proposal in accordance with Section 5 hereof.

s2_5_a

s2_5_b


Section 1: DEFINITIONS
link
show info
s1
Article 1
link
show info
s2_1_a
s2_1_b
Article 2
link
show info
s2_2_a
s2_2_b
Section 2: PROVIDING DATA
link
DIPG Simplified Consortium Agreement
link
Article 5
link
show info
s2_5_a
s2_5_b