Modelling
the General Data Protection Regulation

Sushant Agarwal, Sabrina Kirrane and Johannes Scharf

Analysing & Modelling the GPDR

Relations make it complex for the developers

Actionable instructions

Analysing the GDPR

I: General provisions

II: Principles

III: Rights of the data subject

IV: Controller and processor

V: Transfers 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

11 chapters
99 articles
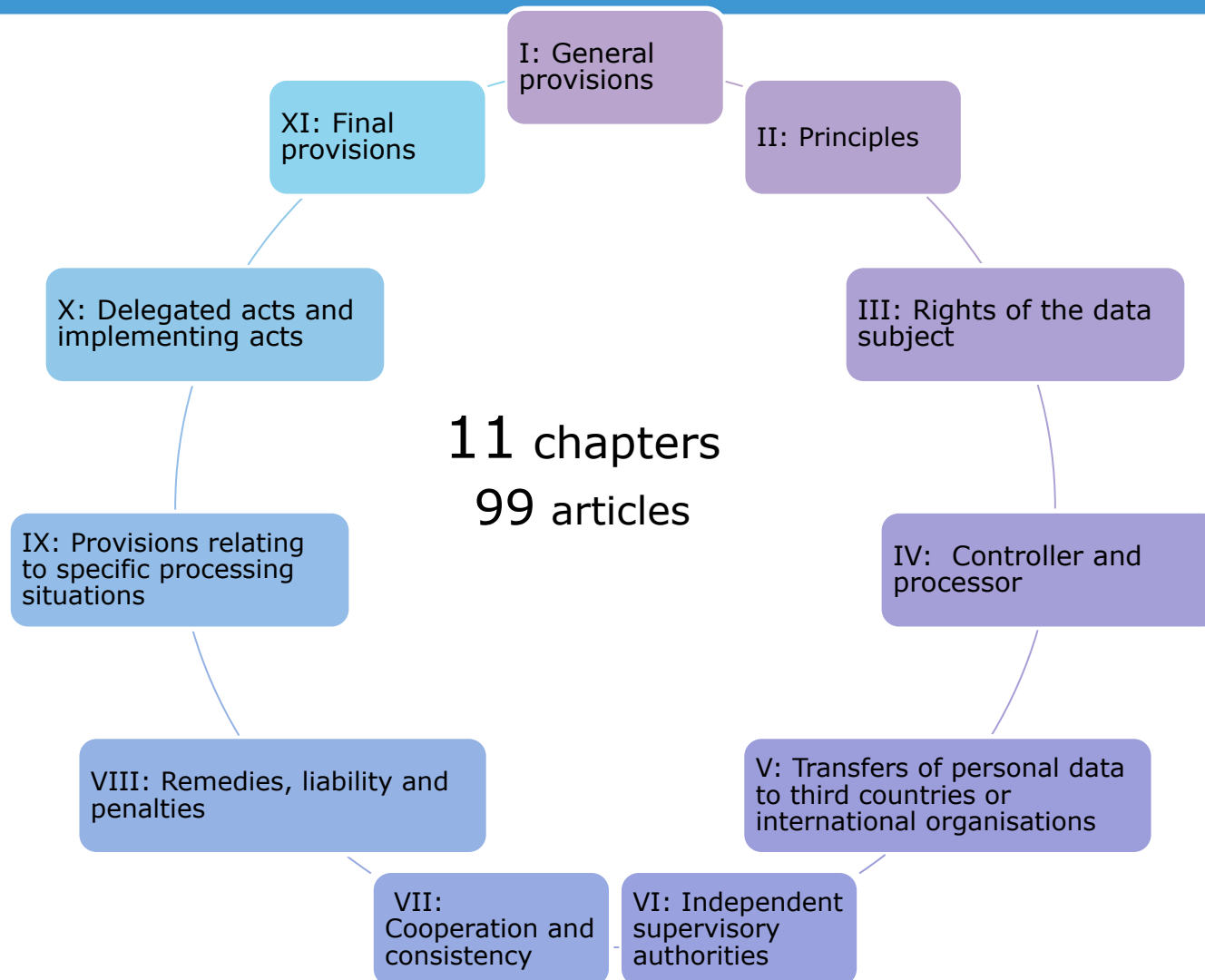
Analysing the GDPR – Articles are not Isolated

Chapter III > Section 1 > *Article 12*

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

Paragraph 1

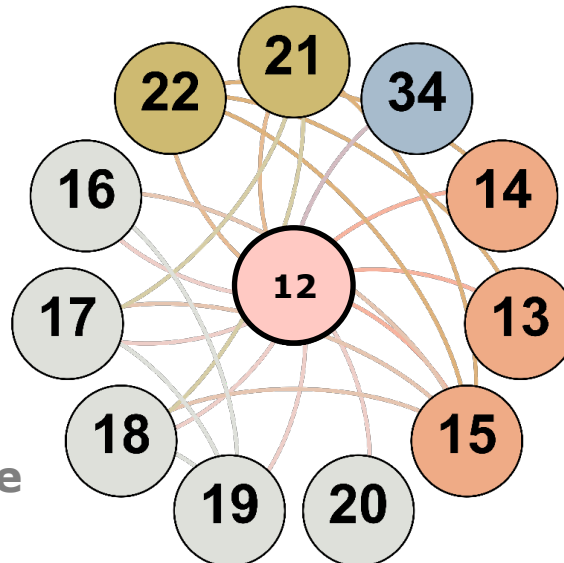The controller shall take appropriate measures to provide any information referred to in **Articles 13 and 14** and any communication under **Articles 15 to 22 and 34** relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language

Chapter III > Section 4

Right to object and automated individual decision-making

CHAPTER IV > Section 2

Security of personal data

Chapter III > Section 2

Information and access to personal data

Chapter III > Section 3

Rectification and erasure

Analysing the GDPR -
All relations defined in the GDPR

Article 83
General conditions for imposing administrative fines

99 articles have
~350 relations defined
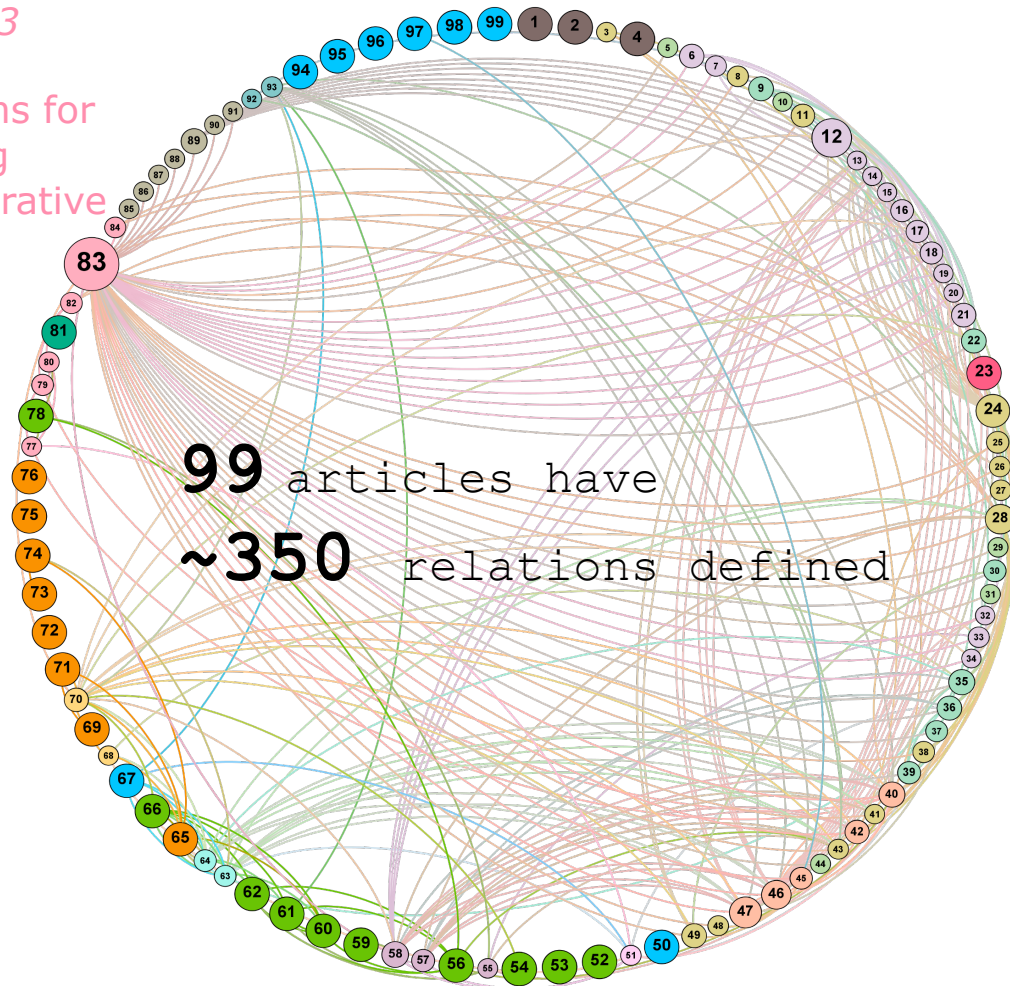
- Other things to be considered
  - Direction of the relationship
  - Article chains
  - Semantics of the relationship
- Model the consequences and fines in the case of non-compliance

Modelling the GPDR

Relations make it complex for the developers

Actionable instructions

Modelling the GDPR – Open Digital Rights Language Model

COMMUNITY & BUSINESS GROUPS

W3C®

ODRL designed to define rules for the publishing, distribution, and consumption of digital media.

Home / ODRL Community Group / ODRL 2 Core Model... / ODRL Version

ODRL Version 2.1 Core Model

Final Specification: 5 March 2015

This Version: http://www.w3.org/community/odrl/model/?

Latest Version: http://www.w3.org/community/odrl/mode

Editors:

Renato Iannella, Semantic Identity, ri@semanticidentity.com
Susanne Guth, Vodafone, susanne.guth@vodafone.com
Daniel Paehler, University of Koblenz, tulkas@uni-koblenz.de
Andreas Kasten, University of Koblenz, andreas.kasten@uni-k

W3C®

Permissions & Obligations Expression Working Group Charter

Scope	
Deliverables	
Dependencies and Liaisons	
Participation	
Communication	
Decision Policy	
Patent Policy	
About this Charter	

The Web has provided the community with standardized mechanisms for numerous content-management services: publishing, distribution, consumption, describing, and sharing. However, the key area of permissions, obligations and licensing has not been addressed in Web standards to date. Content licenses, rights statements, permissions and obligations express the terms of usage for content. With a standard vocabulary, content owners can express terms and processing systems can determine what permissions and other terms are associated with a given resource or collection of resources.

A permissions and obligations expression system should provide a flexible and interoperable information model that supports transparent and innovative (re)use of digital content across all sectors and communities. The underlying model should support the business models of open, educational, government, and commercial communities through profiles that align with their specific requirements whilst retaining a common semantic layer for wider interoperability. The system should not, however, be the basis of legal compliance or enforcement mechanisms.

A permissions and obligations expression language is composed of detailed terms that are both machine-processable and expressible in a form for human-consumption. Allowable actions, constraints, and requirements are expressed at a level enabling complex and business-specific expressions to be created from a vocabulary with specific semantics. This accommodates a broad range of situations and addresses a different business/user need than systems such as Creative Commons that provide generic sharing licenses.

The **mission** of the Permissions & Obligations Expression Working Group is to define a semantic data model for expressing permissions and obligations statements for digital content, and to define the technical elements to make it deployable across browsers and content systems.
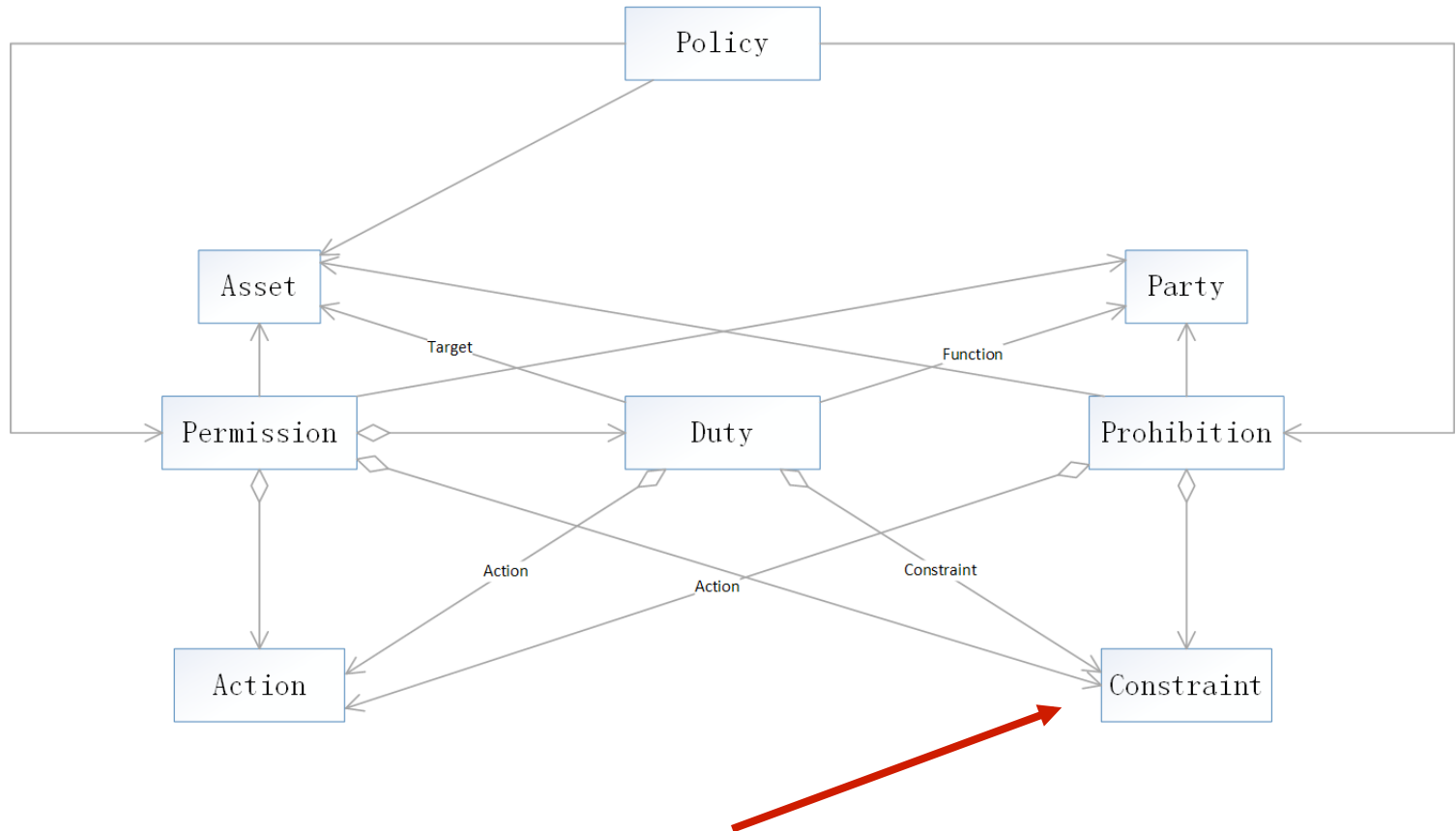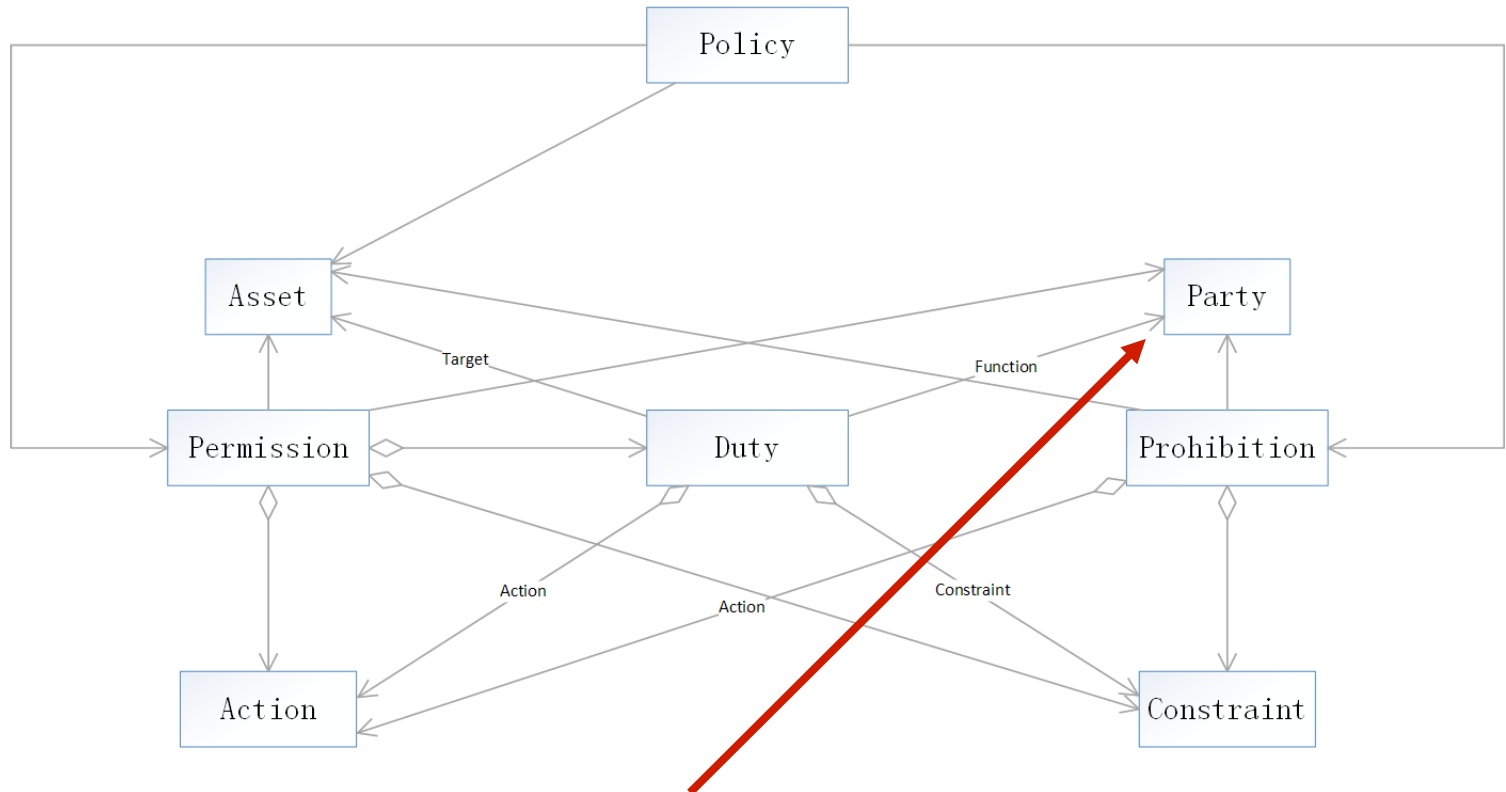
Modelling the GDPR –
Open Digital Rights Language Model
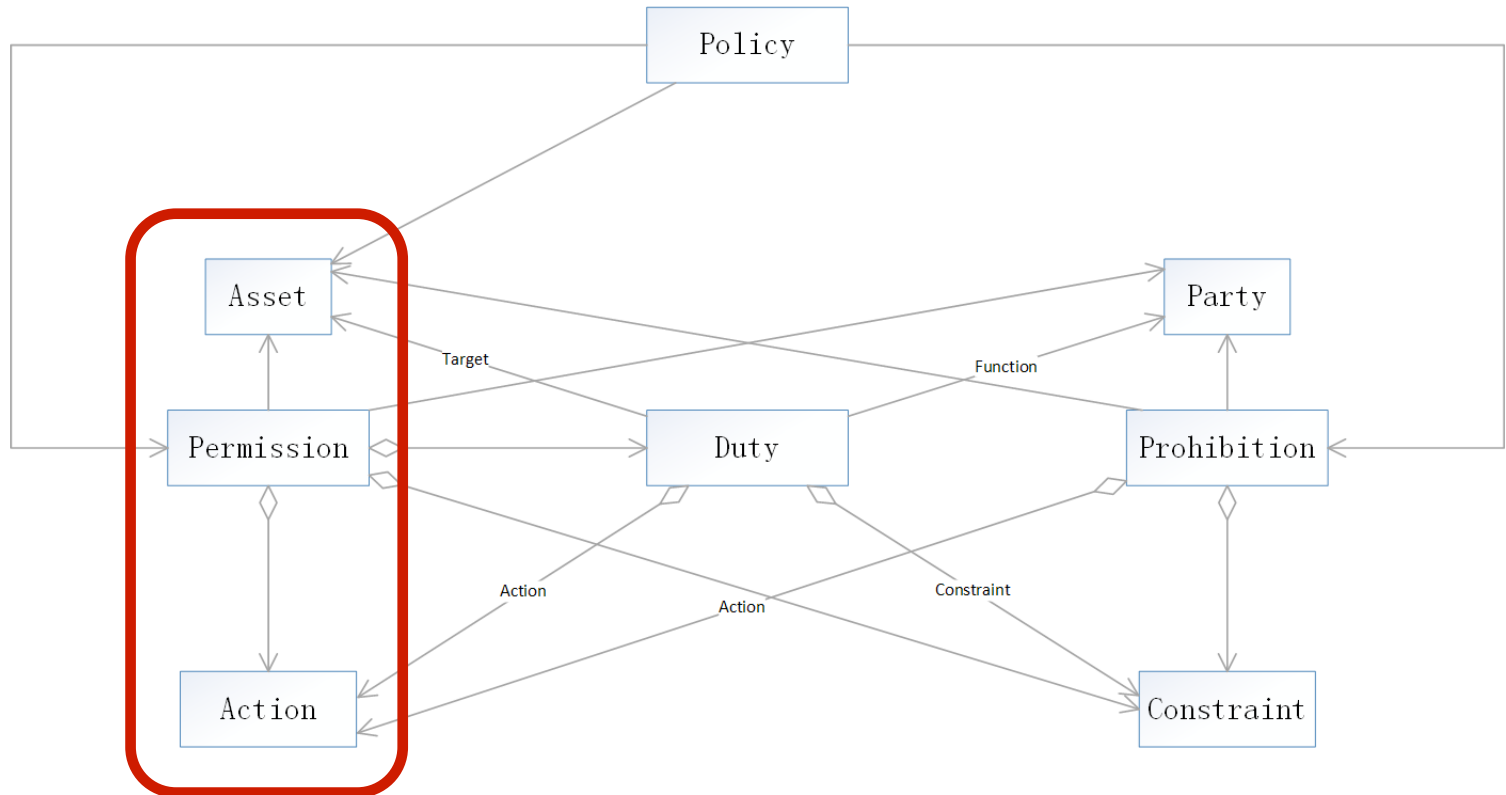
A Permission *allows* a particular Action to be executed on a related Asset, e.g. "Play the audio file abc.mp3".

Modelling the GDPR –
# Open Digital Rights Language Model

A Constraint like "at most 10 times" might be added to specify the Permission more precisely.

Modelling the GDPR –
Open Digital Rights Language Model
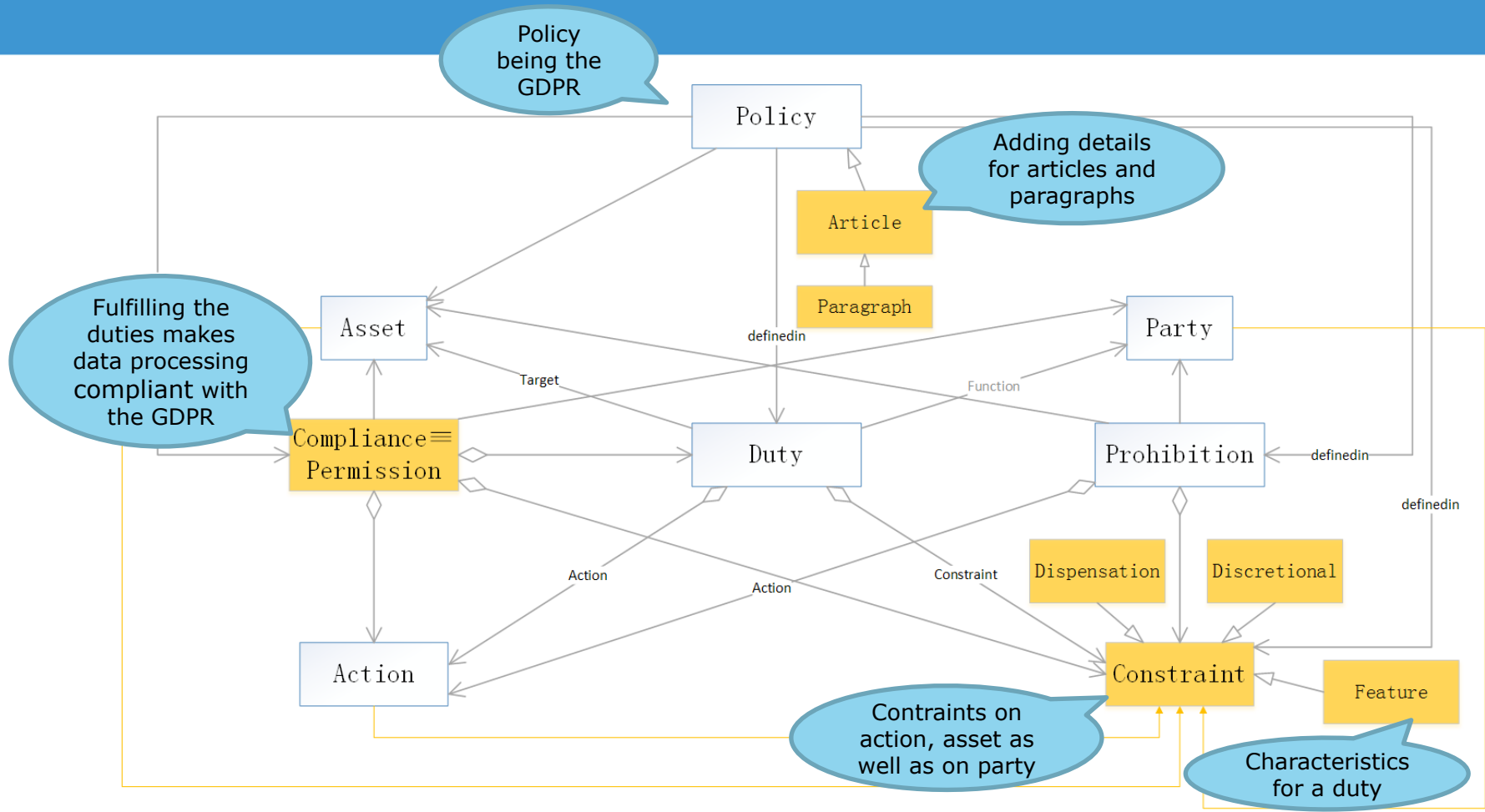

The Party that grants this Permission is the *assigner*, the Party that is granted the Permission is the *assignee*, e.g.
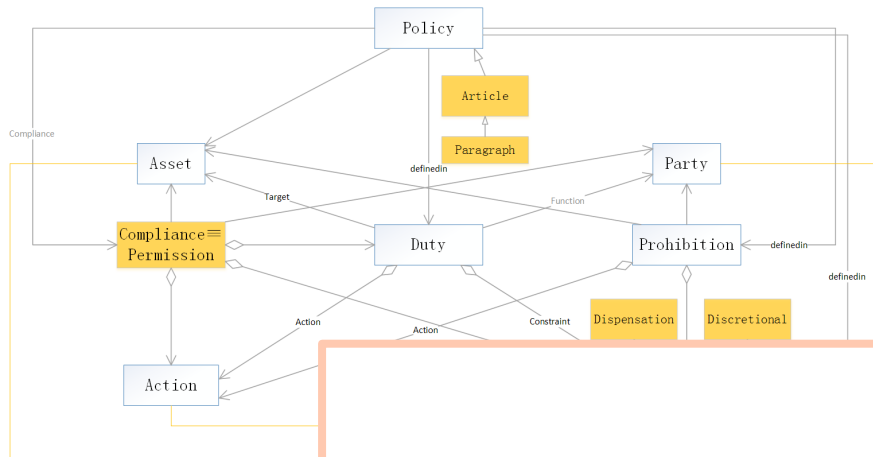"assigner VirtualMusicShop grants the Permission to assignee Alice".
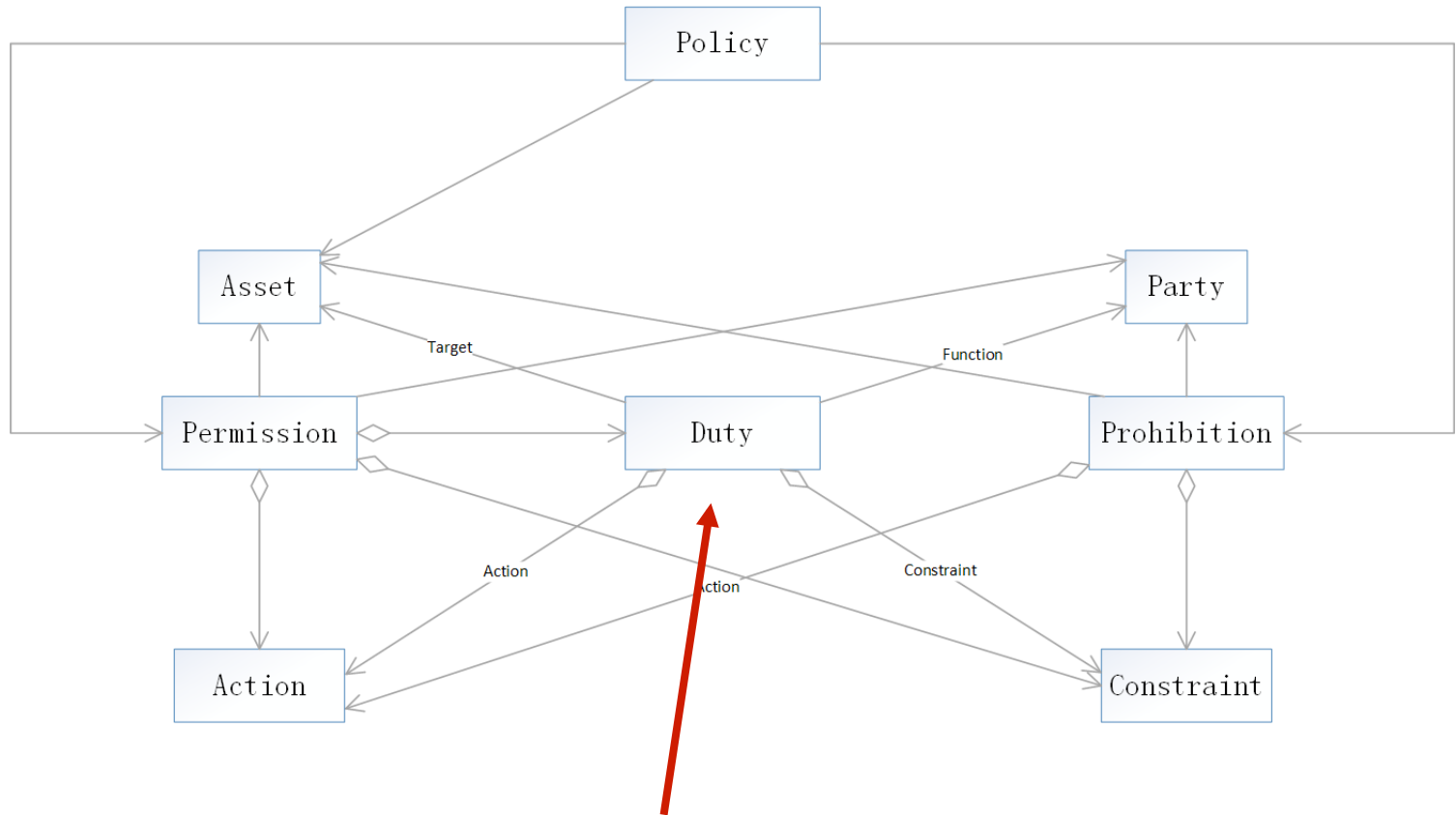
Additionally, a Permission MAY be linked to Duty entities e.g. "Alice must pay 5 EUR in order to get the Permission to play abc.mp3".

Modelling the GDPR – Proposed profile for the GDPR

Compliance for performing an Action (e.g. data processing) on some Asset (e.g. personal data), the responsible Party should fulfill the applicable Duty.

Modelling the GDPR – Proposed profile for the GDPR

Modelling the GDPR – Proposed profile for the GDPR

concise, transparent, intelligible and easily accessible form, using clear and plain language

Duty

Article 12

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

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 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. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Feature

Modelling the GDPR – Proposed profile for the GDPR

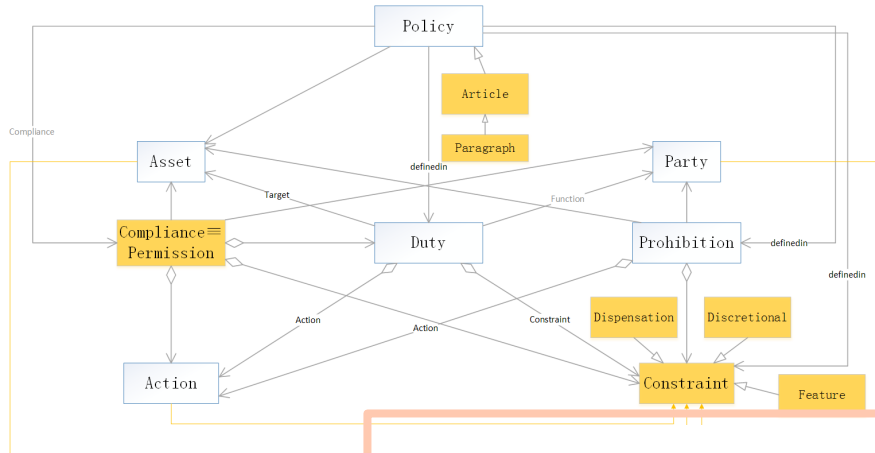Standardised icons **may** be used

Article 12

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

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 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. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

7. 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.

Modelling the GDPR – Proposed profile for the GDPR
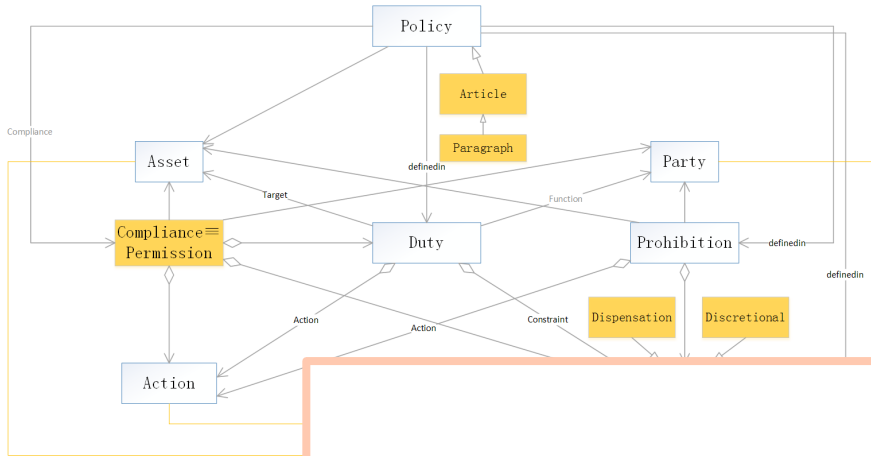
Exception based on Union or Member State law

Dispensation

Article 9

Processing of special categories of personal data

1.   Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2.   Paragraph 1 shall not apply if one of the following applies:

(a)   the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
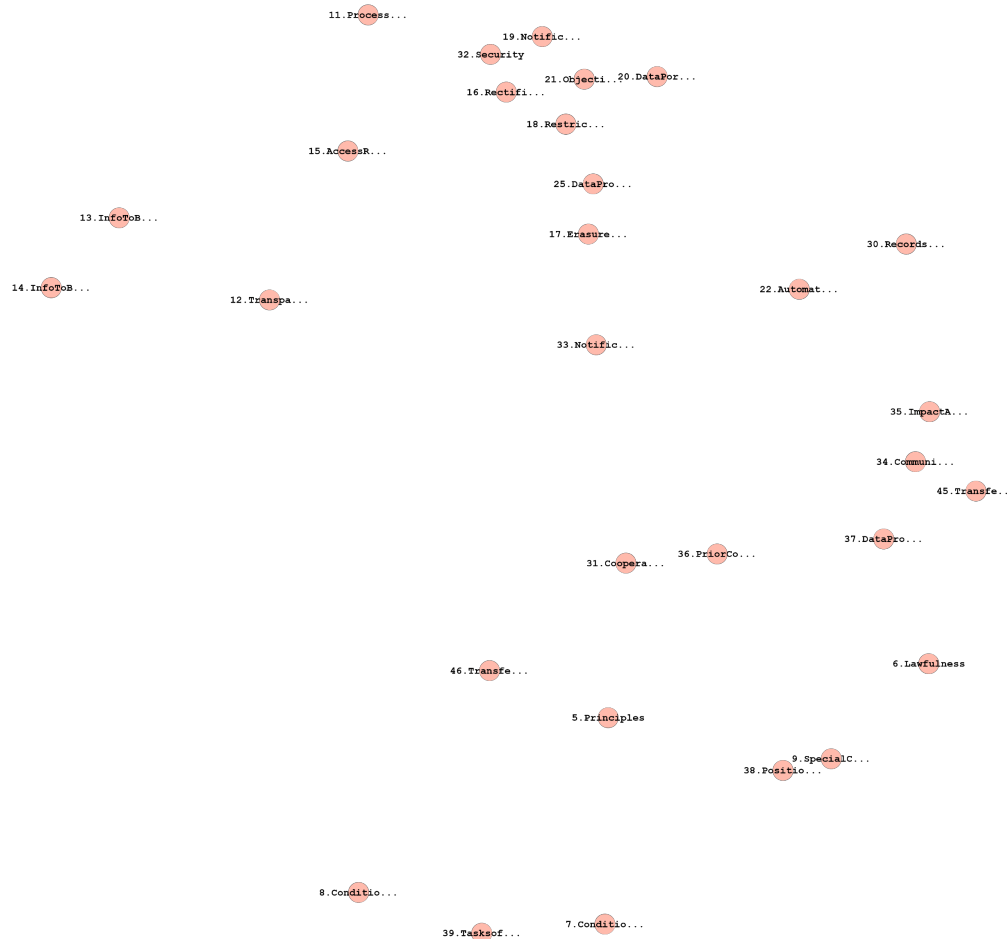
Modelling the GDPR –
Proposed profile for the GDPR

- Not all of the 99 articles define obligations (e.g. objectives, definitions, GDPR's entry into force etc.)

- We also omit articles defining obligations for other parties like the Supervisory Authorities and European Data Protection Board can be neglected.
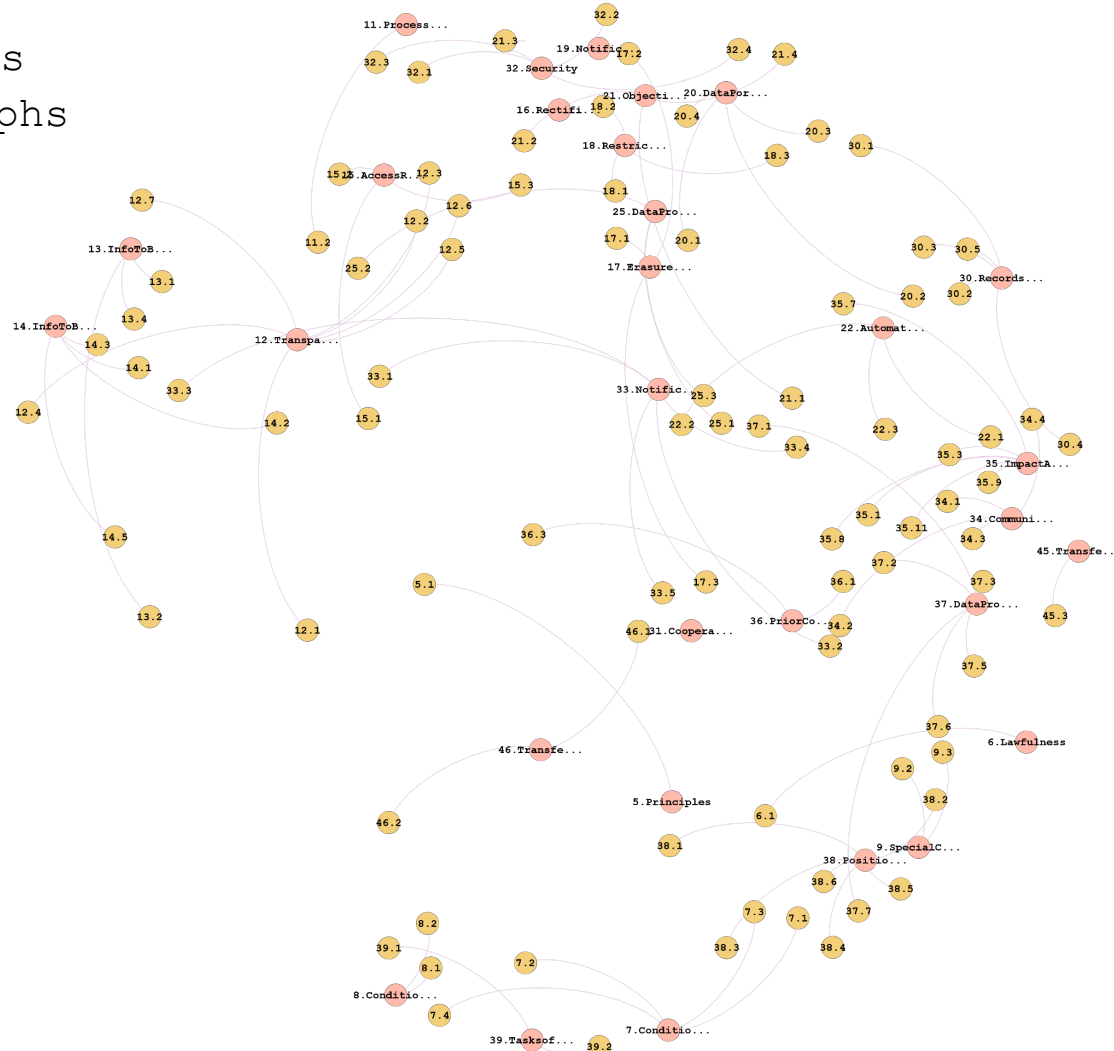
Modelling the GDPR –
Proposed profile for the GDPR

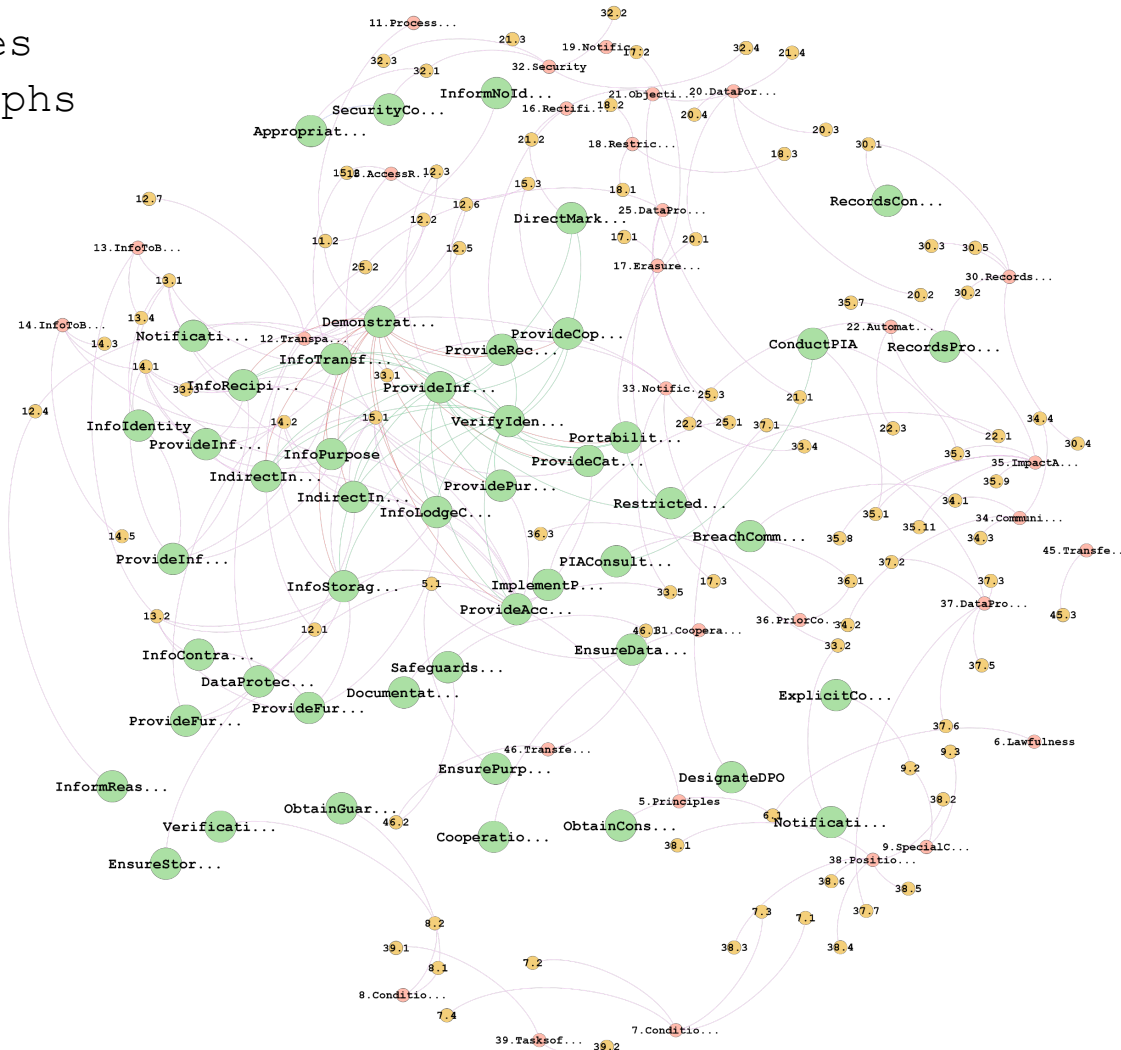- **31** Articles

- **31** Articles
- **91** Paragraphs

- **31** Articles
- **91** Paragraphs
- **48** Duties
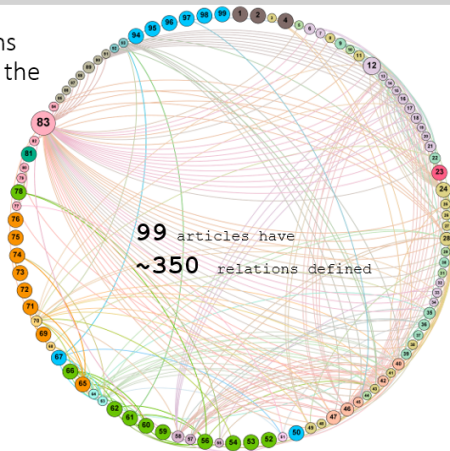
Modelling the GDPR –
Proposed profile for the GDPR

- **31** Articles
- **91** Paragraphs
- **48** Duties
- **144** Constraints
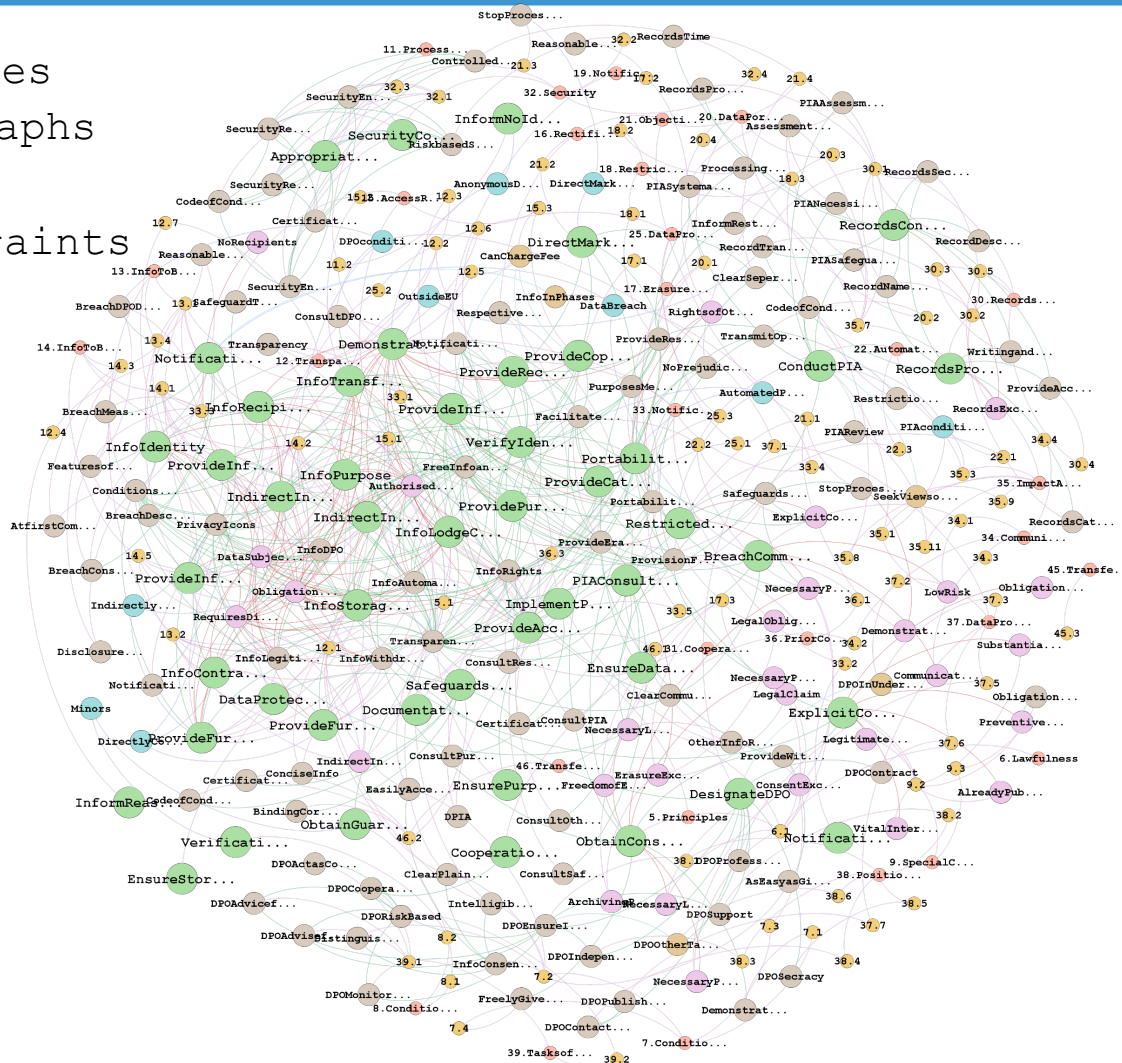
Future Work

All relations defined in the GDPR

99 articles have **~350** relations defined

Proposed profile for the GDPR

To attain **Compliance** for performing an **Action** (data processing) on some **Asset** (personal data), the responsible **Party** should fulfill the applicable **Duty**
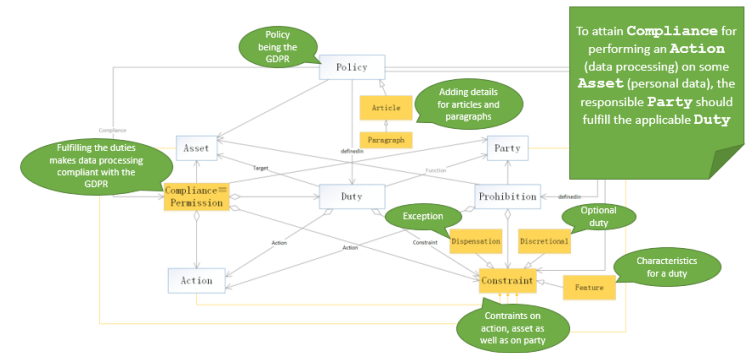
- **31** Articles
- **91** Paragraphs
- **48** Duties
- **144** Constraints
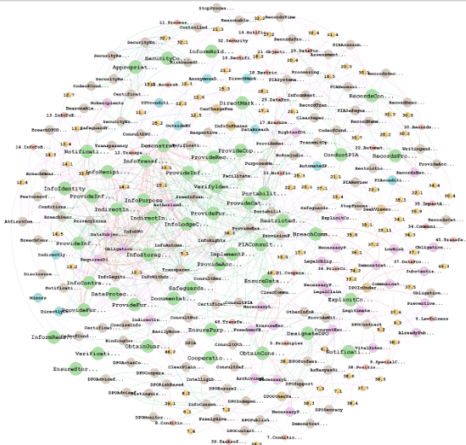
Planned use cases for the model

Checking compliance

Assessing Privacy Impact