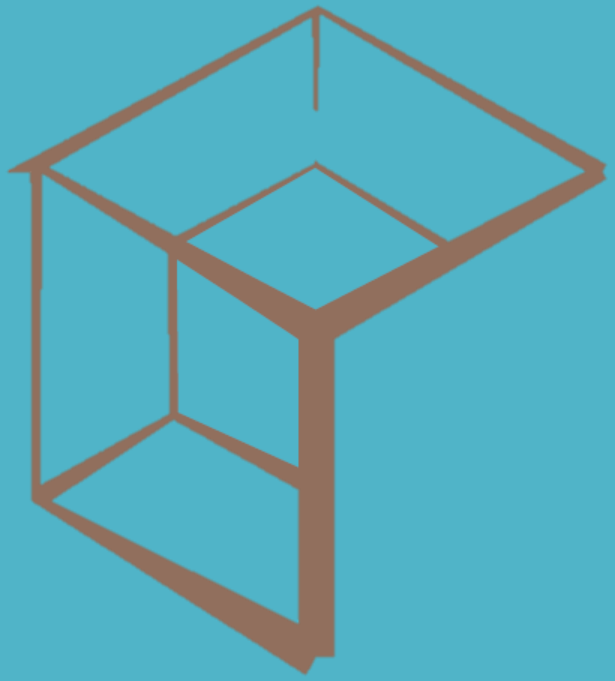
The Importance of Expressing GDPR Codes of Conduct and Certificates in Machine Readable Format



W3C DPV Community

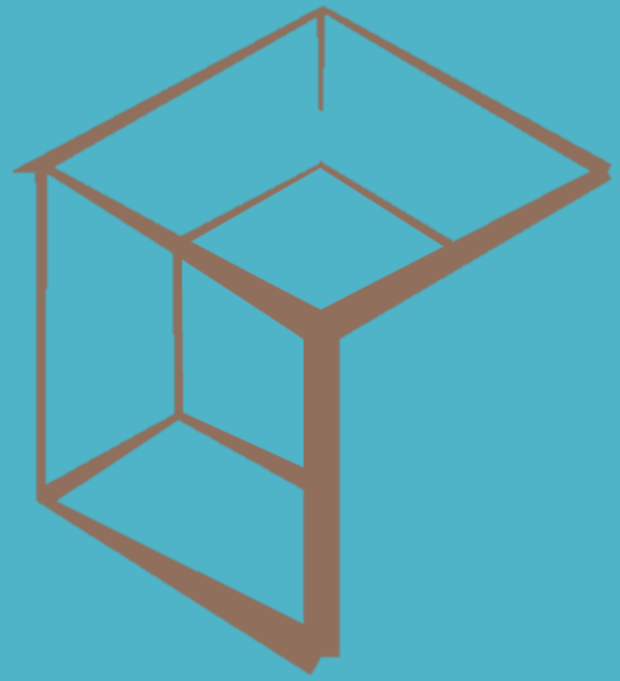
27 March 2025

Online

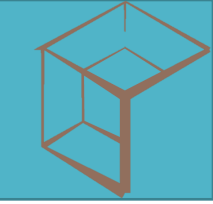
Efstratios (Stratis) Koulierakis (STeP Research Group, University of Groningen)

Email: e.koulierakis@step-rug.nl

The problem



Expressing legal rules (1)



Abstract legal requirements

Data Protection Policies

Expression of Policies in Machine Readable Format

Expressing legal rules (2)

'One of the primary challenges involves bridging the gap between very abstract legal requirements and the very detailed business policies'

De Vos et al., 'ODRL Policy Modelling and Compliance Checking' (2019) 11784 LNCS, 35

The vagueness of the GDPR

- Examples:
  - Article 25(2) GDPR
    - By default the controllers should only process *data which are necessary for each specific purpose*
  - Article 5(1)(e)
    - Personal data shall be kept *for no longer than is necessary*

The market data example

DEUTSCHE BÖRSE GROUP

C.1.2 Standard Data Fees Professional Customers

Deutsche Börse Group Spot Markets

	Access ID €/Month	Physical User ID €/Month
Xetra® Order by Order	107.46	118.20
Xetra® Ultra Level 2	91.23	99.83
Xetra® Ultra Level 1	75.12	82.64
Xetra® Core Level 2	84.36	92.31
Xetra® Core Level 1	69.74	76.83
Xetra® ETFs & ETPs (available as of 1 Jul. 2023)	5.00	5.50
Börse Frankfurt Certificates and Warrants	no charge until further notice	
Tradegate®	no charge until further notice	

Deutsche Börse Group Derivatives Market

	Access ID €/Month	Physical User ID €/Month
Eurex® Order by Order Futures + Options	102.68	112.83
Eurex® Order by Order Futures	82.15	90.27
Eurex® IOC Liquidity Indicator for Options	188.05	206.86
Risk Alerts	2.15	2.36
Eurex® ICAP Swap Spreads	175.18	192.70
Eurex® Ultra	58.67	64.54
Eurex® Core	56.42	62.06
Eurex® Retail Europe	not permitted	
Eurex® Micro Futures + Options	not permitted	

NYSE

EURONEXT

Nasdaq

LONDON STOCK EXCHANGE

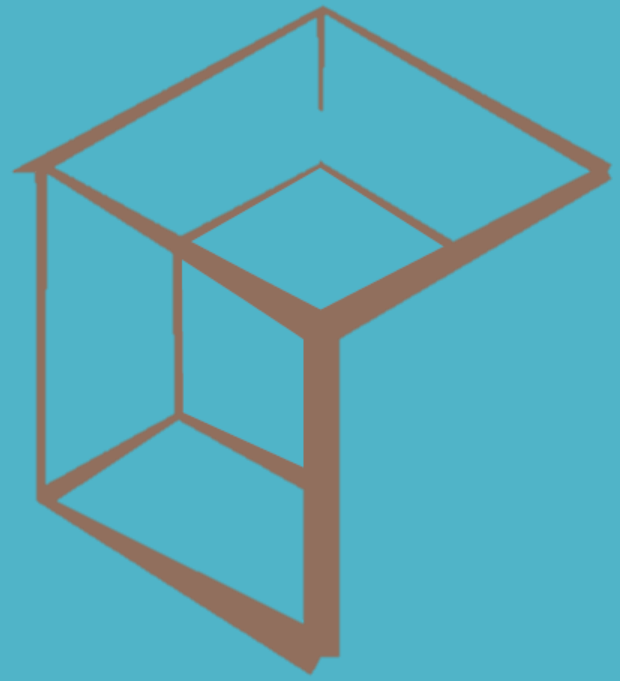
The need for a ‘bridge’

Abstract legal requirements

Data Protection Policies

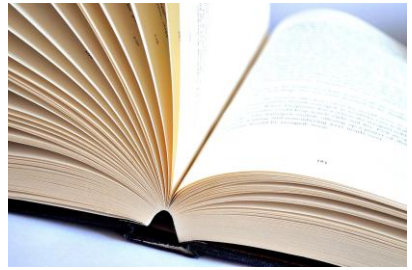
Expression of Policies in Machine Readable Format

A solution



An overview of the official documents

- Codes of conduct (articles 40-41 GDPR)
  - Texts with data protection policies about a domain of activities
  - Voluntary instrument
  - A mechanism that monitors compliance



- Certification schemes (articles 42-43 GDPR)
  - A process that leads to a certificate of compliance with the GDPR
  - Certifying compliance with pre-determined criteria
  - Voluntary instrument
  - A mechanism that monitors compliance

Process of approval

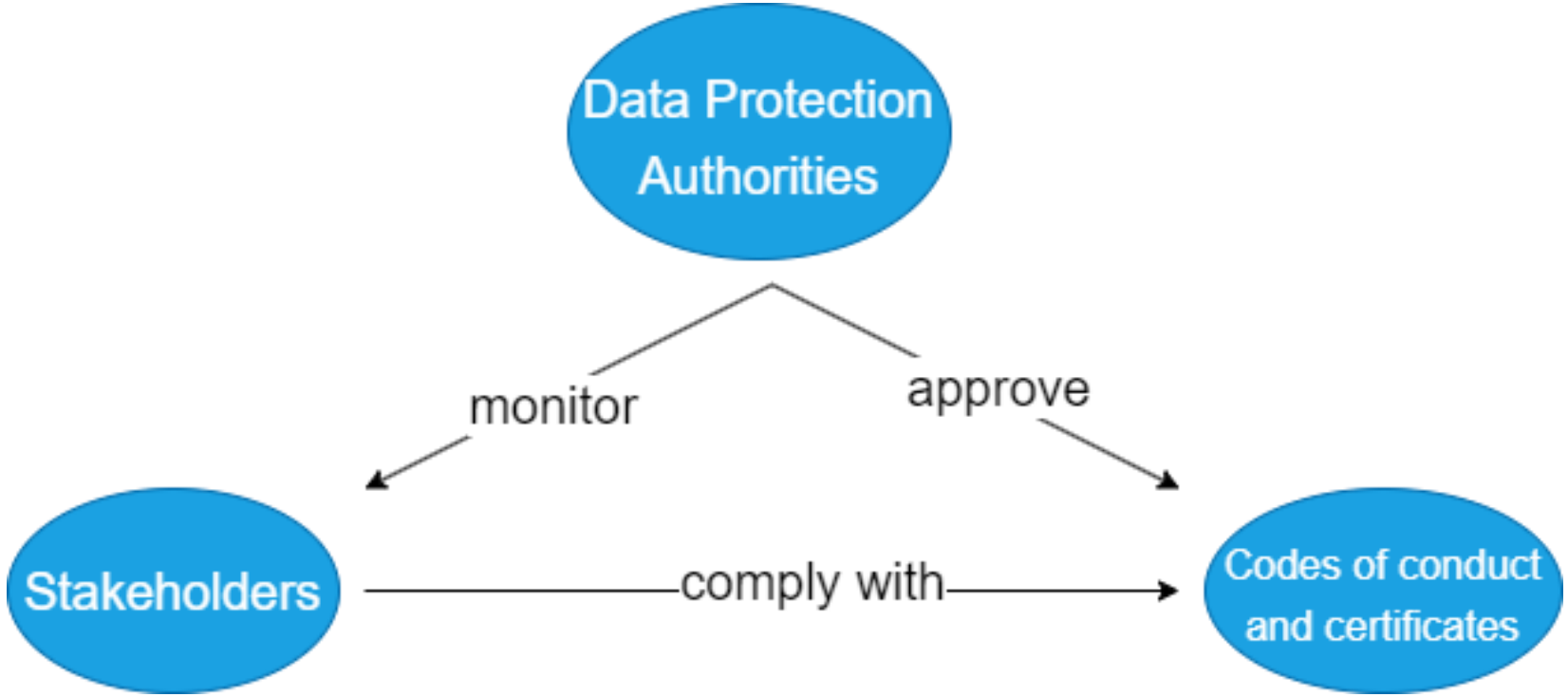
Codes of Conduct

- Draft submitted by stakeholders
- Approval by the National Authority
- Approval at EU level

Certification Schemes

- Draft submitted by scheme owners
- Approval by the National Authority
- Approval at EU level

Legal certainty



Approved documents

Codes of Conduct

CISPE.cloud

EU CLOUD COC

BABE

DW Die Wirtschaftsauskunfteien e.V.

DATA PRO CREATED BY NEDERLAND ICT

AUTO CONTROL Asociación para la Autorregulación de la Comunicación Comercial

Netbeheer Nederland

unespa

Certification Schemes

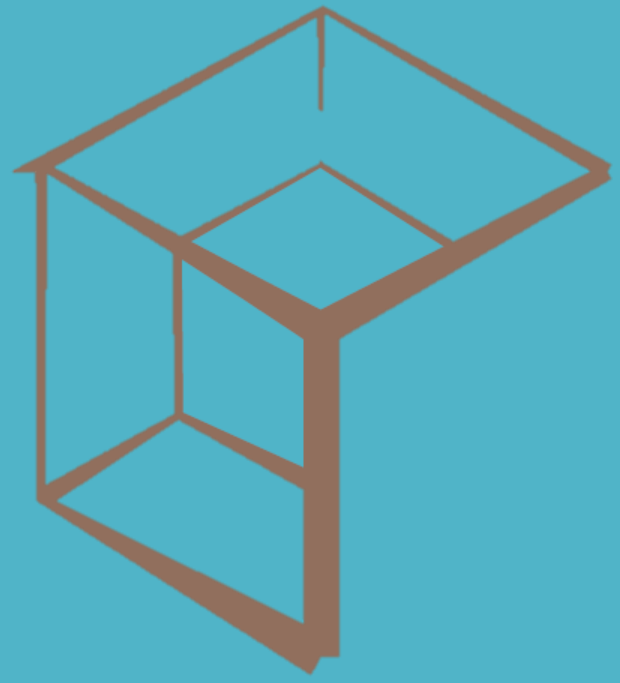
Age Check Certification Scheme

Euro PriSe European Privacy Seal

CNPD COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

ADISA®

Approved policies



Specifications

1. Internal policies for training employees and handling data subject requests 
2. Notifications, alerts and information for the data subjects 
3. Detailed Security measures 
4. Grounds for processing 
5. Processing agreement details 
6. Detailed data protection policies 
7. Quantification of risks 
8. Records of processing 

Detailed data protection policies

unespa

DEFINITION	DATA TO BE PROVIDED BY THE SENDING ENTITY	DATA PROVIDED FROM OTHER ENTITIES (Per claim)
Data of the owner of the vehicle declared in the claim (identification, name and surname, address, telephone or current account) with claims previously declared in the information System as policyholder or owner	- Claim number - Identification - Address - Phone - Banking Data	▪ Entity ▪ Claim Number ▪ Figure received by the person consulted ▪ Date of occurrence ▪ Type of claim ▪ Sinister situation ▪ Refused lack of coverage ▪ (Y/N) ▪ Refused Vehicle location ▪ (Y/N) ▪ Refused by judgement ▪ Remains secured (Y/N)

Netbeheer Nederland

Monitor Power Quality (deliver according to quality standards of the law)

- **Description Purpose:** Reading Meters in order to monitor Power Quality Voltage so that potential bottlenecks in the Grid can be identified. The Grid Operator can read Power Quality Voltage from all Meters at any time for management of the Grid.
- **Reason:** There need not be a specific reason other than the purpose.
- **Number:** all Meters.
- **Data Type:** Power Quality Voltage and events can be read.
- **Readout frequency:** To be determined by the Grid Operator in the DPIA
- **Data frequency:** Day mode or interval.
- **Readout period:** To be determined by the Grid Operator in the DPIA

Conclusion

- Officially approved means of compliance

- Opportunities for building profiles and enriching vocabularies

- Development of useful tools for compliance and compliance checking

Suggestions for discussion

DPV classes	Recommended subclasses
Organisation	• Credit reporting agency • Private education institution
Purposes	• Grid management (with further subclasses specified in the Grid Management CoC) • Meter management (with further subclasses specified in the Grid Management CoC)
Technical measures	• Age check practices • Zoning • Email deletion
Organisational measures	• Flagging AI outputs • Video monitoring • Personnel screening

Thank you for your attention