Engaging Content
Engaging People

DCU

Support for Enhanced GDPR Accountability with the Common Semantic Model for ROPA (CSM-ROPA)

Paul Ryan, Rob Brennan,
ADAPT Centre, School of Computing, Dublin City University
Uniphar Plc, Ireland

Trust over IP Presentation May 2 2022

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.

Background

- Data Protection Compliance Officer for a Healthcare Organisation
  Uniphar Diversified Healthcare Services | Uniphar Group

- PhD Student Dublin City University / Adapt Research Centre

Motivation of our work

- GDPR Accountability requires appropriate and effective measures to be put in place and to demonstrate compliance on request

- Register of Processing Activities (ROPA) is a necessary and critical element for the demonstration of compliance (CNIL France)

- Almost half of organisations are using such manual approaches to completion of ROPA (45%) (IAPP, Trust Arc 2019)

- Only 23% of ROPA's sufficiently detailed for purpose (Castlebridge,2020)

An Example of a ROPA Template from an EU Data Protection Regulator (Finland)

A Legal Requirement

- Name and contact details
- Data Protection Officer (if designated)
- Representative (if required)
- Purposes of processing
- Name and contact details of the joint controller (if required)
- Description of the categories of data subjects
- Description of the categories of personal data
- Categories of recipients
- Reference to the personal data processing agreement signed with the processor
- Third countries and international organisations to which data is transferred,
- Documentation on suitable safeguards for International transfer
- Data storage times or the criteria for defining such storage times
- A description of the technical and organisational security measures

A Survey of Organisational Approaches to ROPA Compliance

- Manual Mapping
- Stand-alone
- Lack Interoperability
- Lack standards based approaches
- Not sufficient detailed
- Generalised or vague
- Not being kept up to date

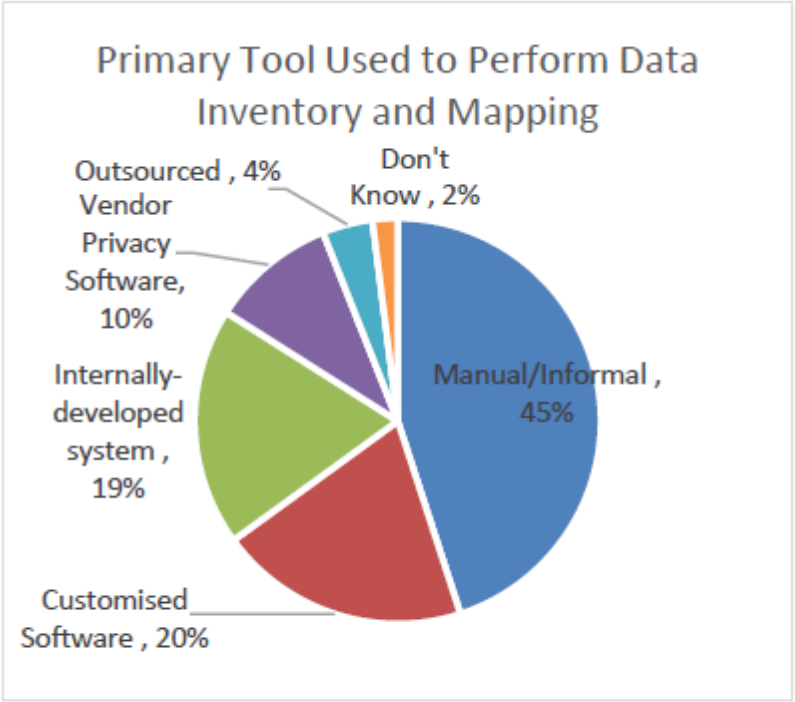
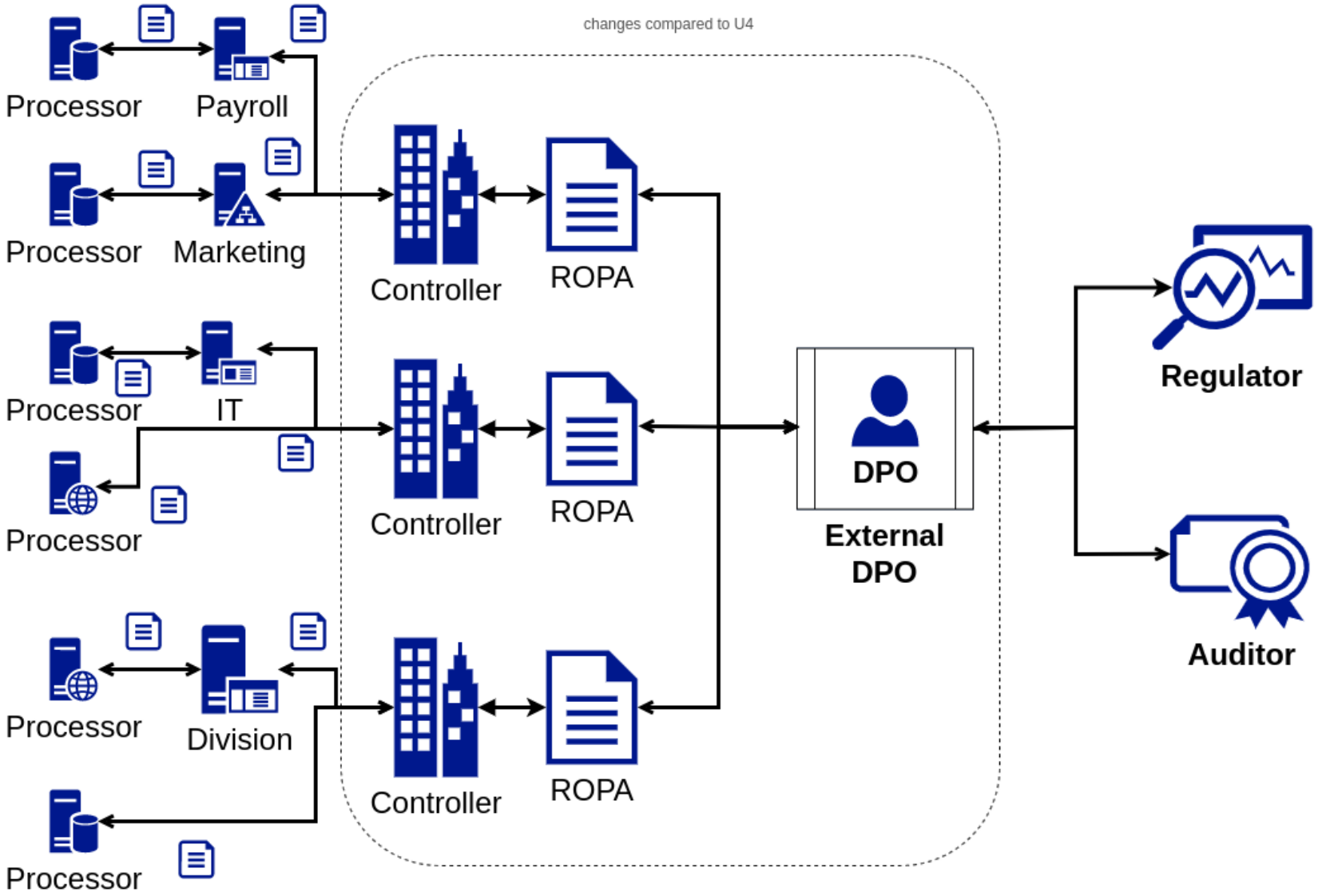


Figure 2: Primary Tool Used by Organisations for Data Inventory and Mapping.

REF: International Association of Privacy Professionals (IAPP). Trust Arc.: measuring privacy operations. (2019). https://iapp.org/resources/article/measuring-privacy-operations/. Accessed 11 Sept 2021

An Example of a Use Case



https://doi.org/10.5281/zenodo.6448788

- Applying ICT Advances to GDPR Accountability
- The digitalisation of data
- Agreement on Common Standards and Agreed Semantics for Personal Data Processing
- Data Protection Supervisory Authorities as an Enabler

Requirements for a machine readable ROPA

- DPO must have access to the most up to date information
- Low level of GDPR compliance
- ROPA a vital element for GDPR compliance
- Processing becoming more complex – higher risk
- Direct view of the front line
- Toolset to continually monitor compliance
- Can assist with new or modified personal data processing analysis
- Automated compliance verification
- Sharing of accountability with regulators / certification bodies

Final Derived Requirements for Automated GDPR Accountability (Part 1)

R1: Records the information necessary for the completion of an ROPA and demonstrate accountability

- Supports the heterogeneity of data sources required
- Spans application-centric data silos
- Spans organisational and functional units
- Interlinking capability—any relevant models or data can be linked

R2: Supports the digital exchange of data between parties (and systems) such as processors and regulators

- Standards-based approach, defining:
  - Data formats—data are available in a common agreed semantic standard, e.g., RDF
  - Protocols/interfaces for transfer and access
  - Processes and compliance points
  - Common definitions of terms

Final Derived Requirements for Automated GDPR Accountability (Part 2)

R3: Automated accountability compliance verification

- Semantic models/support for inference
- Standards as per R2

R4: Privacy-Aware Data Governance

- Integration with organisational data governance processes, roles and data management systems, so these and their metadata can be reused for GDPR compliance and governance
- Supports risk-based data governance
- Specifes machine-readable data protection and data processing policies
- DPO-centric tools to monitor, evaluate and report on GDPR compliance
- Reporting/digital exchange with internal and external GDPR stakeholders
- Methods and tools to manage the accountability metadata lifecycle, e.g., data quality assurance of accountability data

What is the Data Privacy Vocabulary ?

- The DPV is a vocabulary (terms) and an ontology (relationships) serialised using semantic-web standards to represent concepts associated with privacy and data protection, primarily derived from GDPR

- A community specification through the W3C Data Privacy Vocabulary and Controls Community Group (DPVCG).

- A machine-readable representation of personal data processing and can be adopted in relevant use-cases such as legal compliance documentation and evaluation, policy specification, consent representation and requests, taxonomy of legal terms, and annotation of text and data.

- Links to DPV and community group
- https://w3.org/ns/dpv
- https://www.w3.org/community/dpvcg/

CSM-ROPA - An Overview

- A semantic model
- A use case of the data privacy vocabulary (DPV).
- Deployed as a mediation layer
- evolved to support machine to machine accountability compliance verification
- CSM-ROPA is a basis for the development of platforms and tools that allow for the smooth interoperation of systems

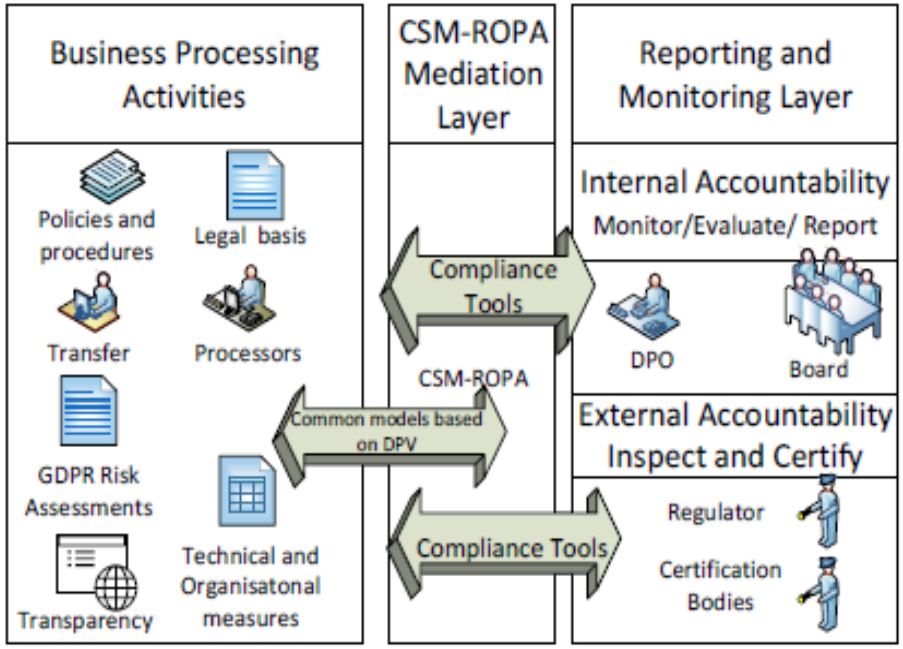


Figure 3: CSM-ROPA as a Mediation Layer.

Case Study

- A potential deployment of the CSM–ROPA data model
- We evaluate the extent to which an organisation can utilise the CSM–ROPA as a mediation layer to demonstrate ROPA compliance and as a basis for developing compliance tools

The ICO Accountability Framework

Category	No. of Expectations	No of Questions
Leadership and Oversight	6	33
Policies and procedures	4	17
Training and awareness	5	17
Individuals' rights	11	42
Transparency	7	31
Records of processing and the lawful basis	10	33
Contracts and data sharing	9	31
Risks and Data Protection Impact Assessments.	5	29
Records management and security	12	63
Breach response and monitoring	8	38
	77	334

https://ico.org.uk/for-organisations/accountability-framework/

Summary of Analysis

Table 3 Summary of mapping results

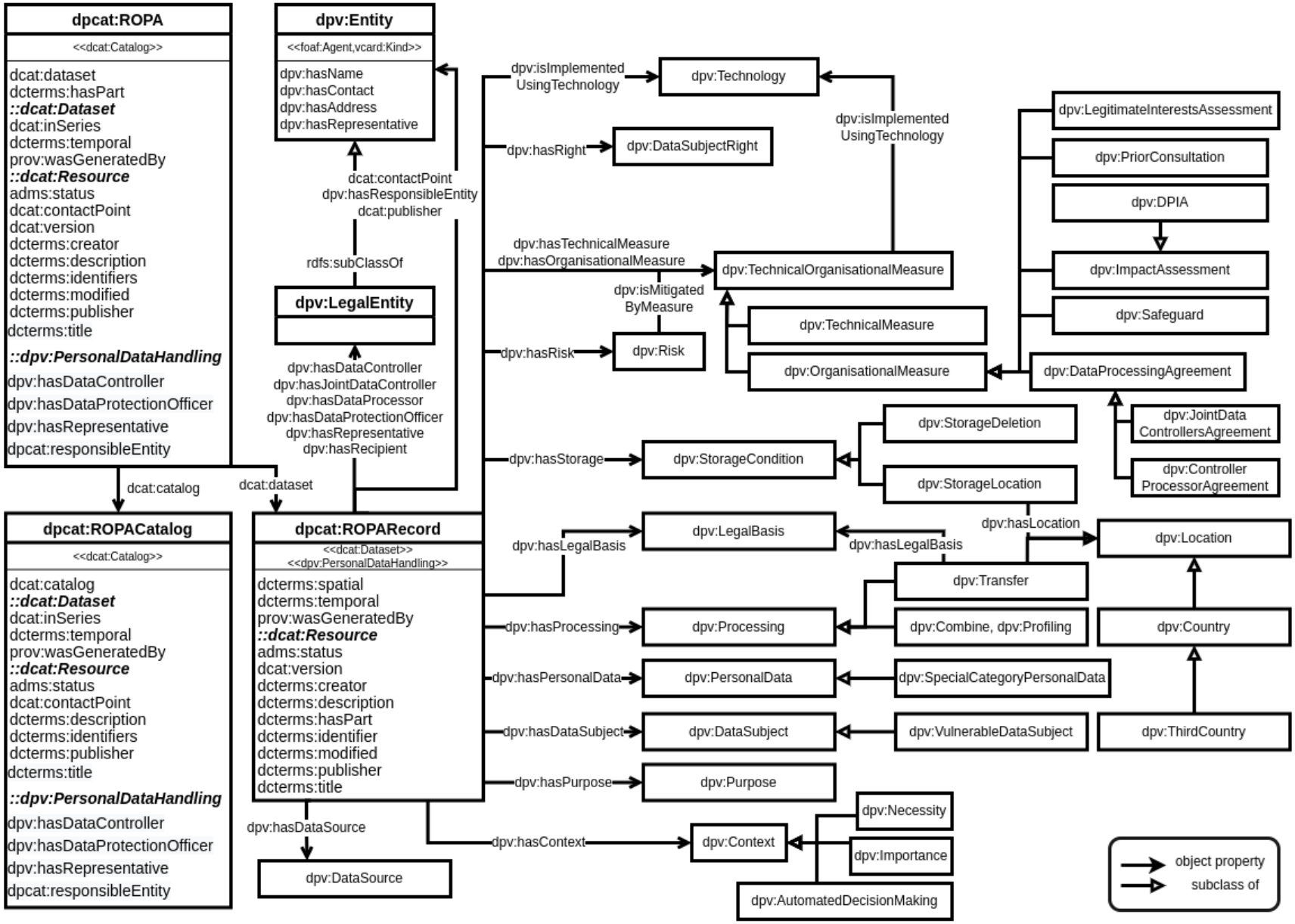
Outcome of mapping	No. of terms	% of terms (%)
Exact mapping one to one	77	55
Mapped using other vocabularies	12	9
Complex mapping	15	11
Partial mapping	32	23
No mapping, under consideration with DPVCG	3	2

Terms communicated to the DPVCG for inclusion "Data Protection Authority" "Data Flow Map "and "Legislation"

Contributions of the paper

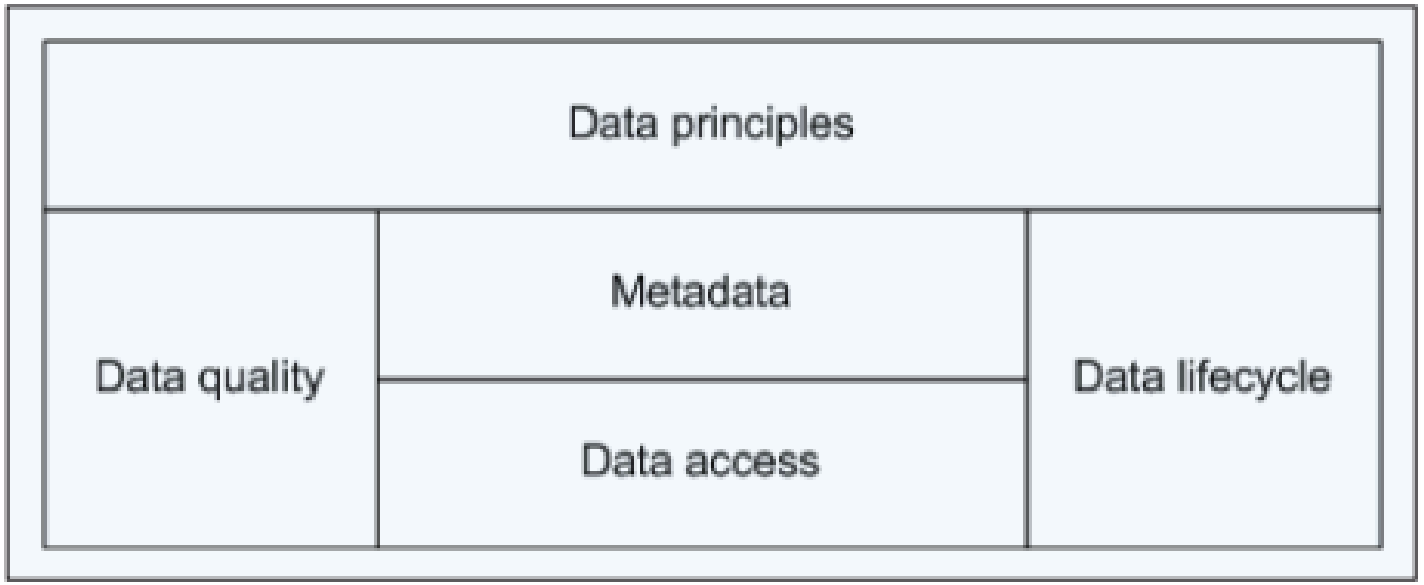
- The application of RegTech best practices to resolve a significant GDPR challenge
- the demonstration of the expressiveness and effectiveness of CSM–ROPA to facilitate GDPR supported accountability
- to identify the key features that systems must possess to assist organisations and show that CSM–ROPA contains the key features to support the digital exchange of accountability data between stakeholders
- compares CSM–ROPA-based accountability with both manual approaches and a leading proprietary privacy software systems

Our recent work - DP-Cat



Data Governance Framework

Figure 2: Decision domains for data governance.



- Metadata: underlying metadata of GDPR Accountability data
- Data Quality: Shacl / DCAT-AP / Survey of templates
- Data Principles : Uses of data for the business

Ref: doi: 10.1145/1629175.1629210

Maintenance of record of processing activities as a core data management capability of organisations

System Capabilities				
Define protected data scope	Identify data objects	Classify data attributes	Locate data records	
Manage Consent	Implement consent items	Record consent instances	Distribute consent	Enforce consent-based processing
Enable Data Processing Rights	Delete data	Pseudonymize data	Transmit data in standardized form	
Maintain ROPA	Aggregate accountability data	Exchange standardised data with stakeholders	Generate DPA-specific records	Assure data quality
Organisational Capabilities				
Orchestrate Data Protection Activities	Assume data protection responsibilities	Oversee data protection activities	Control compliance of external processors	
Demonstrate Compliant Data Processing	Maintain records of processing activities	Maintain documentation of system landscape	Supervise sensitive processing activities	
Disclose Information	Disclose information to individuals	Disclose information to authorities		

Acknowledgements

- Dublin City University School of Computing
- ADAPT Centre for Digital Content Technology
- Uniphar PLC