Policy Modeling with ODRL: Framework, Lifecycle and Inference for Machine Processing of Legal Regulations

Muhammad Ahtisham ASLAM[1][0000−0001−7080−0327], Peter Brosten[2], Adrian Asensio[3], Andrea Villa[4], and Maria Cristina Timon[5]

[1] Fraunhofer FOKUS, Berlin, Germany
muhammad.ahtisham.aslam@fokus.fraunhofer.de
[2] Eurecat, 72, Bilbao Street, 08005 Barcelona, Spain peter.brosten@eurecat.org
[3] Universitat Politecnica DE, Catalunya, Spain adrian.asensio@upc.edu
[4] Cefriel, Politecnico Di Milano, Milan, Italy andrea.villa@cefriel.com
[5] Arthur's Legal B.V., 1070 AK AMSTERDAM, Netherlands
timon@arthurslegal.com

Abstract. Background: In the current age, AI based systems are being developed and used more than ever before to perform our daily tasks, technical work as well as scientific activities. On the one hand, it is considered a positive sign and contribution to strengthen the industry and technology sectors but at the same time it could also compromise the fundamental rights of a society, freedom, and human values if not developed and adopted in a controlled manner.
Problem: To protect European states from such threats, secure basic rights, and enforce the controlled development and usage of AI based systems, the EU has defined and implemented several laws such as GDPR, Data Acts, AI Acts, and Data Governance Acts. With all these developments and emergence of legal acts and regulations, the European industry and business sector is missing appropriate technologies and solutions that can automate the transition and compliance assessment of Data and AI Operations of business and industrial systems.
Solution: To address these challenges, ACCOMPLISH project is targeting to develop a framework (i.e., ACCOMPLISH framework) that can be used for compliance assessment and certification of Data and AI Operations (Data/AI Ops) of advanced systems in an automated way. At the core of this framework are requirements for compliance assessment that are extracted from these legal documents. Then a Compliance Policy Models Repository consisting of ready-to-use extendable compliance policy models that effectively consolidate the policy rules, guidelines, restrictions and obligations to automatically check the compliance by using the Human-in-the-Loop (HITL) approach, is developed and maintained. To maximize the interoperability and minimize the policy modeling overhead, existing profiles/vocabularies are re-used at maximum and only missing vocabulary is introduced as part of ACCOMPLISH Profile for ODRL. These contributions can smoothen the affordable technologies development and adoption to automate compliance assessment and certification, thus enabling already established infrastructures (such as data spaces) to easily connect and consume the automated compliance.

Keywords: Government Data · Data Analysis · Data Digitization.

1 Introduction

In the third decade of twenty first century, the world is going through unprecedented technological evolution backed up by several key enablers such as blockchain [24], dataspaces [4], cloud computing [2], and artificial intelligence (AI) [23]. Among these, development and usage of AI based systems has triggered several challenges to privacy of individuals, fundamental rights, social values as well as increased technological risks [21].

Legal bodies and regulatory authorities are keenly looking at possible impacts and potential harms of developing AI based systems and using them in an uncontrolled manner [15]. This is resulting in various regulatory frameworks, acts and laws such as EU Data Act, AI Acts, GDPR and Data Governance rules [11], [18], implied to development and usage of AI based systems in general and Data and AI operations (Data&AI Ops) in particular [1]. The ultimate goal is to regularize the controlled usage of AI such that basic rights of the European citizens as well as IT industry and it's technological growth is not compromised [5]. Major issues in adopting these legal acts and laws to regularize the AI based system are compliance requirements extraction from these legal documents, developing policy models based on these requirements and then implementing them such that they can easily be used in the already established infrastructure (such as data spaces) for automated compliance assessment.

To address these issues, we present our approach to keep an eye on existing, upcoming and updates in existing laws and acts **(Andrea or Lina)**. Since, legal experts are not much familiar with technical aspects of policy modeling and technical experts are not use to of dealing with legal matters, therefore, we adopted a joint methodology i.e., *Methodology for Synchronization Between Requirements and Policy Models (MSRP)*, that can be used to generate compliance requirements from legal documents and to keep them updated with any changes in legal acts and laws. As technical experts have been part of the process of generating compliance requirements from legal documents therefore, they can adopt, revise (by using back and forth channel) and use them to produce extendable compliance policy models. We also present the a *Extendable Compliance Policy Models Repository* consisting of ready-to-use extendable compliance policy models that can be used for compliance assessment and certifications of Data&AI Ops by using Human-in-the-Loop (HITL) approach [16]. We focused on developing ready-to-use policy models in ODRL by maximizing the use of existing vocabularies instead of focusing on developing a new profile for policy modeling language. It also helped in minimizing the policy modeling effort and to maximize the policy adoption in AI based systems. For sure, during the modeling process missing vocabularies are documented as ACCOMPLISH profile for ODRL. Finally, we present a use case scenario for compliance assessment for Data&AI operations. The paper has the following seven contributions:

– Regulatory radar for continuous regulations monitoring

- Methodology for Synchronization Between Requirements and Policy Models (MSRP)
- Policy modeling approach and *Extendable Compliance Policy Models Repository*
- ACCOMPLISH ODRL Profile
- Compliance Assessment Use Case

The rest of the paper is organized as follows: the related work is discussed in Section 3. Our approach for keeping the ACCOMPLISH framework up to date with any changes or emergence of new laws is discussed in the Section . *Methodology for Synchronization Between Requirements and Policy Models (MSRP)* is presented in Section 4. The policy modeling approach and *Extendable Compliance Policy Models Repository* is presented in Section 5. The Section 6 describes the initial version of the ACCOMPLISH ODRL profile (use slides pictures for this section). A compliance assessment use case is discussed in the Section7. Finally, we conclude our work and suggest future directions in Section 8.

2 Related Work

As part of ACCOMPLISH project, policy modeling for automated compliance assessment and certification needs to investigate the state of the art from several perspectives such as legal, theoretical and technical. Here, we discuss the related work from all these perspectives.

In [3], authors presented the Agent Based Model (ABM) for policy making when many statistical models are becoming unstable with changing environmental interactions. Authors prove the stability of ABMs in policy making by conducting a systematic review of 34 articles describing the use of ABM including the formal communication and model tractability. Similarly, a conceptual framework for problem specific policy modeling is presented in [19]. Theoretical and reuse able ABMs are developed and deployed for generic modeling purposes. One main issue with this approach is that developing a generic model before the development of actual model is quite resources and time consuming limiting the adoption of this approach.

From technical perspectives we have several candidate approaches that can be used for policy modeling such as Open Digital Rights Language (ODRL), Web Ontology Language (OWL), Shapes Constraints Language (SHACL), and Semantic Web Rule Language (SWRL). Among all, a technical and feasibility study in the ACCOMPLISH project resulted in the ODRL to be the best suitable choice for policy modeling in the project perspective [13][22] [14]. ODRL provides a very comprehensive information model that can be used to model the policy flow in a very comprehensive way. In addition to this several profiles of ODRL such as Data Privacy Vocabulary (DPV) [12][20], Vocabulary for High Risk AI Systems [9], and vocabulary do define Access Controls [6]. Additionally, AI Risk based Ontology [8], [17] provides vocabulary that specifically focuses on modeling entities of GDPR articles [7][18] , EU AI Acts [10][25] etc.

ODRL, together with all these profiles provides a very comprehensive set of vocabularies required to do policy modeling for GDPR Articles, Data Acts, AI Acts and Data Governance Acts.

3 Regulatory Radar for Continuous Regulations Monitoring

The scientific and technology radar activity is a continuous, structured monitoring process that captures the evolution of the regulatory, scientific, and technological landscape relevant to compliance in Data and AI Operations within the scope of the ACCOMPLISH project. The methodology combines regulatory intelligence, technology scouting, and iterative validation with project partners to ensure that the project's compliance models and technical developments remain aligned with both current requirements and emerging trends.

The regulatory monitoring primarily covers European regulations affecting data governance, artificial intelligence, cybersecurity, and digital compliance, i.e. the GDPR, the AI Act, the Data Governance Act, the Data Act, the NIS2 Directive, and the Cyber Resilience Act. These topics were monitored through institutional portals, regulatory updates, guidelines, liaison activities, and the expertise already available within the consortium.

In parallel with the regulatory analysis, the radar includes a systematic technology watch over scientific literature, industry reports, online sources, existing compliance tools, and related European initiatives. The objective is to identify relevant technologies and trends, and assess their positioning with respect to ACCOMPLISH's objectives and intended solution space. The radar results highlighted a rapidly increasing complexity in the compliance landscape for organisations operating data- and AI-driven operations. The analysis confirmed that compliance requirements are becoming more interdependent across regulatory domains, combining privacy, security, data governance, AI risk management, transparency, and sector-specific obligations. This finding reinforced the need for multidimensional compliance frameworks that integrate heterogeneous regulatory requirements into operational models that can be updated over time.

4 Methodology for Synchronization Between Requirements and Policy Models (MSRP)

As the name (i.e., *Methodology for Synchronization Between Requirements and Policy Models (MSRP)*) suggests that *MSRP* starts with the selection of legal articles, laws, regulations and acts that are related to data&AI Ops of AI based systems. These selected legal articles and regulations are then used to identify and extract compliance requirements creating the base for developing policy models which ultimately are used for compliance assessment of data&AI Ops in an automated way (as shown in the Figure 1). Here, we explain these phases.

Phase I: Legal Article Selection Since, ACCOMPLISH framework is targeted to be used for compliance assessment of data&AI Ops of advanced

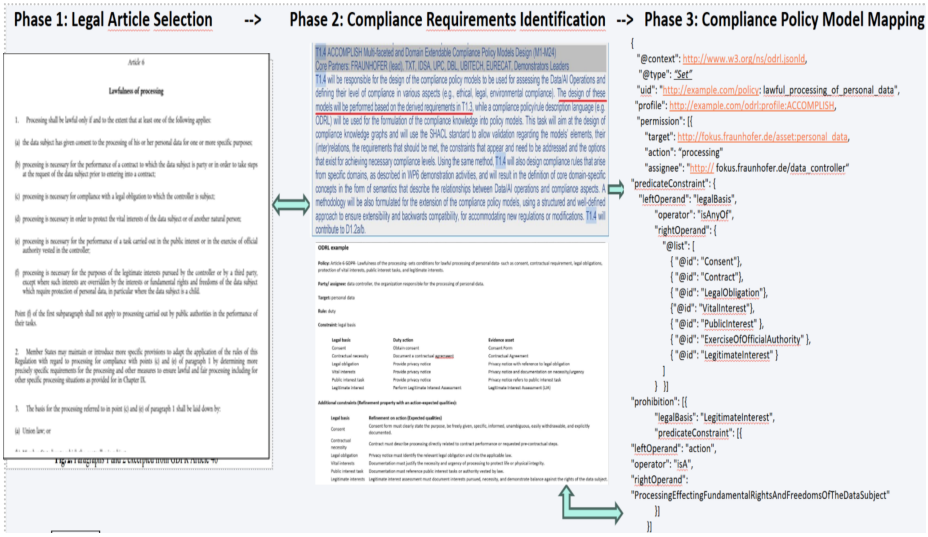
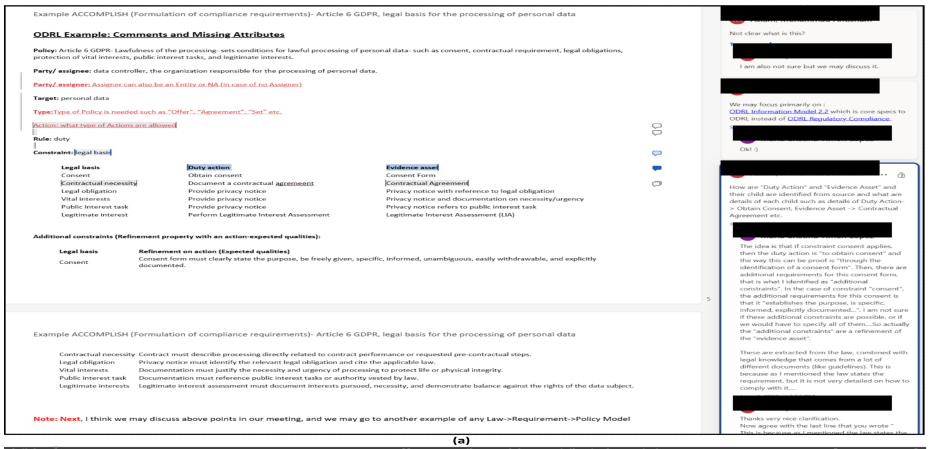


Fig. 1. Different phases of *Methodology for Synchronization Between Requirements and Policy Models (MSRP).*

systems, therefore, this phase focuses on selection of articles that have regulatory contents for data&AI Ops. As mentioned earlier that Human-in-the-Loop (HITL) approach is used in requirements gathering and policy modeling, therefore in this phase legal documents are selected on manual basis with common understanding of technical and legal experts based on mutual discussion, importance and relevance of legal articles to the data&AI Ops. Major regulatory contents that are selected and used in this phase are GDPR articles, Data Acts, AI Acts and Data Governance Acts.

Phase II: Compliance Requirements Identifications In this phase compliance requirements from selected legal articles are identified, extracted and documented such that they can easily be used by technical team for policy modeling purposes. One major issue faced during this phase was how to document the identified compliance requirements such that they become clear, easy to understand and properly structured in a way that they can easily be used by technical experts for compliance policy modeling purposes. For this purpose legal and technical experts jointly designed a *Compliance Requirements Documentation Template (CRDT)* (as shown in the Figure 2). The Figure 2(a) shows the first version of the CRDT that we used for cross discussion and analysis of compliance requirements between legal experts and technical team. This resulted in two key improvements in CRDT: i) identification of new entities, factors, parameters, and attributes, ii) an improved, clear and easy to understand structure (as shown in the Figure 2(b)) of compliance requirements that was very helpful in policy modeling. Finally, this structure is used to document the compliance requirements of GDPR Articles, Data Acts, AI Acts, and Data Governance Acts

that are selected in phase I. It is important to highlight here that Phase II & III are recursively iterated, feeding each other in policy modeling and requirements identification. Extracted and documented requirements are forwarded as input to Phase III for policy modeling where as issues, missing information and structural limitations of these requirements are communicated back as an input to Phase II. This recursive back-and-forth channel helped in identification of quite extensive and micro-level requirements that ultimately was helpful in developing and implementing extendable compliance policy models (as discussed in in Phase III).



(a)

Article No.	Legal Provision	Scope	Requirement type	Measures, actions and documentation to demonstrate compliance	Monitoring requirement	Consequences of non-compliance
6	**Legal bases for processing general personal data:** define the conditions under which an entity is enabled or authorized to process such data.	Applies to the entities determining the purposes and means of the processing: **data controllers.**	**Duty:** when processing personal data, the entity must establish a valid legal basis. Or **Permission:** when an entity has a legal basis, it is 'authorised' to process that personal data.	*A. Binary (yes/no):* if these elements are present, there is *evidence towards* demonstrating compliance. a. **Consent:** a signed consent form is stored, or consent is clearly recorded (e.g., by clicking *Accept Terms and Conditions*) b. **Contractual necessity:** record or copy of the contract or service agreement under which the data processing is required. c. **Legal obligation:** available privacy notice or policy that references the specific law or regulation enabling the data processing. d. **Vital interest:** documentation or other evidence of the urgent situation (e.g. emergency, danger to life) e. **Public task or authority:** available privacy notice or policy that references the specific law granting the entity or organization authority to process personal data. f. **Legitimate interest:** record of a Legitimate Interest Assessment (LIA). *B. Non-binary (require a contextual assessment):* building on the binary actions, a contextual assessment of these points is required to further verify compliance with each specific legal basis. a. **Consent:** verification that consent is freely given, specific, informed, unambiguous and easy to withdraw. b. **Contractual necessity:** verification that the data requested is directly tied to the effectiveness and performance of the contract. c. **Legal obligation:** verification that the law enabling the data processing is specific and applies to your organization. In addition, the data must be necessary, rather than merely useful, for fulfilling the legal duty. d. **Vital interests:** documentation must demonstrate why the situation was urgent and why it was not possible to obtain consent in time (or why another legal basis did not apply).	Verification of stored documentation confirming the applicability and validity of the legal basis. Among others: a. Verification that consent has not been withdrawn or that the contract remains in force. b. Enabling laws remain in force and are applicable. c. Reassess legitimate interest balance to ensure they still outweigh any impact on individuals or the existence of vital interest.	- Fines up to €20 million or 4% of global turnover. - Legal claims for damages by individuals. - Suspension or deletion of data processing. - Reputational damage and loss of public trust. - Supervisory authorities can conduct investigative, corrective and advisory powers.

(b)

Fig. 2. Compliance requirements documentation template used for documenting compliance requirements for policy modeling.

Phase III: Compliance Policy Modeling Mapping Once compliance policy requirements are identified, extracted and documented in the CPRT, they are taken as input for phase III for policy modeling purposes. Each requirement from the CPRT is translated to the corresponding policy instruction encoded in

ODRL as core information model and its various profiles as suitable vocabulary containers.

5 Extendable Compliance Policy Models Repository (ECPMR)

Extendable Compliance Policy Models Repository (ECPMR) is basically a central compliance policies bank that is used to fuel the compliance assessment process of the ACCOMPLISH framework. Main part of the ECPMR are policy models that are developed and injected into the repository for selected articles and acts from GDPR, AI Acts, Data Acts and Data Governance Acts, based on their relevance to data&AI Ops. Here, we use the term *"extendable"* with policy models because in ACCOMPLISH project we performed an extensive review of EU regulations from different sectors to create policy models that can be expanded with future needs as well as forth coming legal acts and regulations, as the modeling process to be employed remains the same.

Additionally, as part of implementing the policy model in ODRL, compliance requirements for every article and act (as discussed in the Section 4) are taken as input and basic flow of the policy is encoded in ODRL information model. Each requirement (binary and non-binary) are taken one by one, corresponding best suitable vocabulary is searched and investigated among existing profiles of ODRL, and every requirement is mapped to suitable ODRL policy code (as shown in Figure 3). For the purpose of interoperability we tried to re-use the existing vocabularies to our best. In extreme case where no suitable vocabulary is found in any of the existing profiles, a new term / entity (with its corresponding details) is defined and documented as part of ACCOMPLISH ODRL Profile (further discussed in Section 6).

Once requirements are mapped to corresponding ODRL instructions and the basic policy flow is designed by using core ODRL information model, requirements are categorized and encoded as *Prohibitions*, *Obligations*, *Permissions*, *Duties* and possible *Consequences*. Since, in most of the cases (i.e, legal acts and articles that are related to data&AI Ops), consequences are almost similar (i.e., "Administrative fines up to €15,000,000 or 3% of total worldwide annual turnover") therefore, we modeled such consequences in ODRL (as shown in the Figure 4) and synchronized the code across the policy models until and unless consequences are changed in legal articles. Appendix **??** shows the sample ready-to-use policy model for AI Act 10.

5.1 Policy Models Validation

Validation and verification is an important part of quality assurance, before any software, tool or a component is deployed. We also validated compliance policy models before deploying them to the ECPMR to be used as part of ACCOMPLISH framework as well as to be used publicly. We validated our compliance

Article No.	Legal Provision	Scope	Requirement type	Measures, actions and documentation to demonstrate compliance	Monitoring requirement	Consequences of non-compliance
10	**Data and data governance:** requires that data complies with a set of standards during development, updates or retraining.	Applies to **providers** of the high-risk AI system.	**Duty:** before placing a high-risk AI system on the market or put into service, applies also to updated involving retraining or real-world data input.	*A. Binary (yes/no):* if these elements are present, there is *evidence towards* demonstrating compliance. a. Documented data governance and dataset-quality procedures containing the following elements: - Documented data governance framework. dpv:hasOrganisationalMeasure dpv:DataGovernance - Documented dataset specification. tech:hasDocumentation aiact#CommonSpecification tech#Documentation - Documented procedures to detect and correct data errors. - Bias/ representativeness assessment. dpv:hasAssessment **dpv:DataQualityAssessment** ai#BiasDetection - Error management procedures. *B. Non-binary (require a contextual assessment):* building on the binary actions, a contextual assessment of these points is required to further verify compliance with each specific legal basis. - Statistical analysis of dataset representativeness. - Bias-detection reports (quantitative fairness metrics). risk:detects ai#ValidationDataBias - Documentation showing how identified biases were corrected. - Data validation reports. - Documentation of reviewer checks.	Verification that data used (training, validation, testing, and real-world inputs) remains appropriate, representative, complete, and free of errors for the intended purpose of the high-risk AI system, and whether data issues lead to new risks or performance degradation. ai:TrainingData ai#TestingData **ai:ValidationData** Among others: a. Existence of a documented data monitoring policy. dpv:hasPolicy dpv#MonitoringPolicy b. Documented roles and monitoring responsibilities. dpv#hasTechnicalOrganisationalMeasure **dpv:ActivityMonitoring** c. Documented monitoring schedule. dpv:hasPolicy dpv#MonitoringPolicy **dpv:PhysicalSurveillance (option)**	-Administrative fines up to €15 000 000 or 3% of total worldwide annual turnover. "leftOperand": "payAmount", "operator": "lteq", "rightOperand": { "rdf:value": "15000000.00", "xsd:decimal": true }, "unit": "http://dbpedia.org/resource/Euro" -Penalties and enforcement measures adopted at the Member State level.

Fig. 3. Requirement to ODRL vocabulary mapping.

```
"consequence": [
  {
    "rdf:value": {
      "@id": "compensate"
    },
    "refinement": [
      {
        "odrl:or": [
          {
            "leftOperand": "payAmount",
            "operator": "lteq",
            "rightOperand": {
              "rdf:value": "15000000.00",
              "xsd:decimal": true
            },
            "unit": "http://dbpedia.org/resource/Euro"
          },
          {
            "leftOperand": "payAmount",
            "operator": "lteq",
            "rightOperand": {
              "rdf:value": "0.03",
              "xsd:decimal": true
            },
            "unit": "http://dbpedia.org/resource/Turnover"
          }
        ]
      }
    ]
  }
]
```

Fig. 4. Consequences modeled in ODRL.

policy models in three different ways (as discussed below): **Internal Reviews-Semantic Validations:** Once technical team finishes the implementation of policy models based on the requirements that are extracted and documented by the legal experts, policy models go through internal review process. In the internal review process each policy model is analyzed from requirements perspectives, semantically and syntax wise, jointly by legal and technical experts. This process also results into requirements corrections/updates, syntax validation and policy updates. Any existing issues are reported as comment/feedback and are addressed as part of review process. Once verified, policy models go through syntax validation at two levels (i.e., JSONLD validation and ODRL validation).

Syntactical Validation: Since, policy models are encoded in ODRL by using jsonld serialization therefore, policy models are validated by using JSONLD playground [6] to address any kind of syntactical discrepancies. Additionally, ODRL code of policy models is validated by using ODRL validator [7]. Figure 5 shows the jsonld and ODRL validation of the policy model for AI Act 10 before deploying it to the ECPMR.

6 ACCOMPLISH ODRL Profile

Creating a profile for a policy modeling language such as ODRL that can support the vocabulary required to model policies for specific legal articles or acts has always been a supporting and useful mechanism. Some times creating new profiles containing vocabularies that have matching semantics with some existing vocabularies creates interoperability issues as well as modeling overhead. In ACCOMPLISH project we minimized this overhead at two levels: i) interoperability is maximized by adding a module i.e., searching and identifying existing vocabularies to be reused, as pre-requisite to profile modeling, ii) only introducing new entities and terms as part of ACCOMPLISH ODLR Profile that either absolutely not exists or have no semantic matching in existing vocabularies. That's why one of the main contributions of the ACCOMPLISH project is *Compliance Policy Models Repository (CPMR)* consisting of ready-to-use policy models with human-in-the-loop (HITL) approach instead of ACCOMPLISH ODRL profile. This is also the reason that ACCOMPLISH ODRL profile consists of only those terms that are not found in any existing profiles. All such terms/entities are documented as part of ODRL profile with necessary details. The Figure 6 shows a sample entity description from ACCOMPLISH ODRL profile. As a review mechanism, ACCOMPLISH ODRL profile is continuously reviewed for any kind of updates such as an entity is found in an existing vocabulary at later stage during modeling process. Such entities are deprecated from profile and updated in policy models.

[6] https://jsonformatter.org/
[7] https://odrlapi.appspot.com/

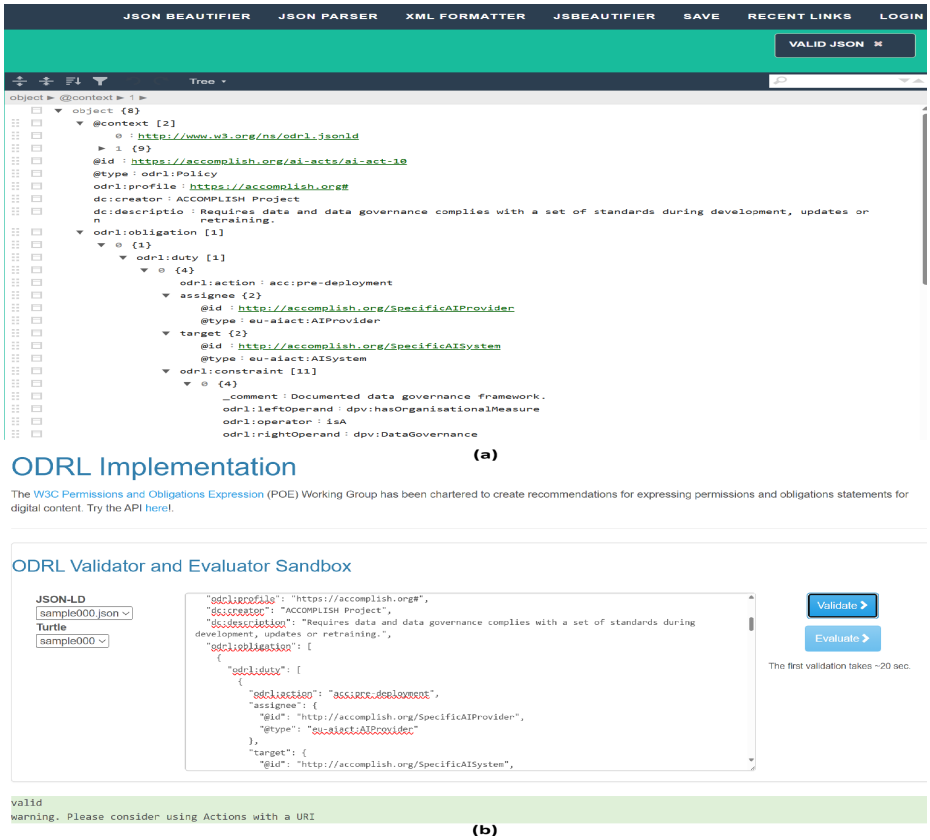


Fig. 5. Policy models validation at syntactical level.

Items	Contents
Term	*Accuracy*
Label	*Data Accuracy*
IRI	*https://accomplish.org/DataAndAI#Accuracy = acc:Accuracy (ACCOMPLISH namespace and URI to use)*
Type	*rdfs:Class, skos:Concept*
Parent Classes	--
Child Classes	--
Domain of Properties	*hasDataAccuracyStatus*
Range of Properties	--
Definition	*Concept indicates the data accuracy that can be presented by using the "hasDataAccuracyStatus" which may have different values (e.g., Accurate, NotAccurate etc.)*
Additional Notes	--
Usage Example	*"constraint": [{ "leftOperand": "acc:accuracy", "operator": "eq", "rightOperand": "acc:inaccurate" }*
Source Legal Document/Article/Act	*GDPR 2016, Article 16 & 19*
Creation Date	*25-11-2025*
Updating Date	--
Contributor	*Ahtiham and Peter*
Cross Discussion / Comments	• *Any reviewer may comment/ suggest correction/updates here.* • *Cross discussion between community members.*

Fig. 6. Entity description in ACCOMPLISH ODRL profile.

7 Compliance Assessment Inference Engine

8 Conclusion and Future Work

To strengthen and secure the Europe's industrial competitiveness, the European Parliament has prepared and enforced a set of legislative laws and acts such as GDPR, Data Act, AI Acts, and Data Governance Act. To act in compliance with these legal legislations, the business world and industry needs to be equipped with appropriate technology and ever-evolving multifaceted compliance solutions to regularize their daily business together with their data&AI Ops. To address these challenges (as part of ACCOMPLISH framework), in this paper we presented our regulatory radar for continuous regulations monitoring. We also presented the *Methodology for Synchronization Between Requirements and Policy Models (MSRP)* that can be used to extract compliance requirements from legal documents. These requirements create the base for compliance policy modeling. Against the tradition of introducing new profiles, we developed an *Extendable Compliance Policy Models Repository (ECPMR)* that consist of read-to-use policy models with Human-in-the-Loop (HITL) approach. Additional community support is provided by developing and documenting ACCOMPLISH ODRL profile that consisting of entities and their semantic descriptions for only those vocabularies that were found missing in existing profiles during policy modeling tasks. Finally, a compliance assessment use case is presented to prove the practical demonstration of ACCOMPLISH framework in compliance assessment and certifications.

As part of future activities, we are working on several aspects: i) expanding and updating the *Extendable Compliance Policy Models Repository (ECPMR)* with new ready-to-use policy models as well as by updating existing policy models with new requirements, ii) standardizing, completing and publishing the ACCOMPLISH ODRL profile documentation, iii) implementing the profile as OWL ontology.

Acknowledgments. Not declared for double blind review.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Agarwal, S., Kirrane, S., Scharf, J.: Modelling the general data protection regulation (02 2017). https://doi.org/10.38023/4b143376-9ae3-4679-a044-380ae9ef9a79
2. Babalola, O., Adebisi, A., Ogundipe, F., Folorunso, A., Nwatu, C.: Policy framework for cloud computing: Ai, governance, compliance and management. Global Journal of Engineering and Technology Advances **21**, 114–126 (11 2024). https://doi.org/10.30574/gjeta.2024.21.2.0212

3. Belfrage, M., Lorig, F., Davidsson, P.: Simulating change: A systematic literature review of agent-based models for policy-making. In: Proceedings of the 2024 Annual Modeling and Simulation Conference. ANNSIM '24, Society for Computer Simulation International, San Diego, CA, USA (2026). https://doi.org/10.22360/ANNSIM.2024.HSAA.129, https://doi.org/10.22360/ANNSIM.2024.HSAA.129
4. Dam, T., Krimbacher, A., Neumaier, S.: Policy patterns for usage control in data spaces. In: Fifth International Workshop On A Semantic Data Space For Transport @ SEMANTiCS 2023. Leipzig, Germany (September 2023)
5. Ditfurth, L., Lienemann, G.: The data governance act: – promoting or restricting data intermediaries? Competition and Regulation in Network Industries **23**, 178359172211413 (11 2022). https://doi.org/10.1177/17835917221141324
6. Esteves, B., Rodríguez-Doncel, V., Pandit, H.J., Mondada, N., McBennett, P.: Using thenbsp;odrl profile fornbsp;access control fornbsp;solid pod resource governance. In: The Semantic Web: ESWC 2022 Satellite Events: Hersonissos, Crete, Greece, May 29 – June 2, 2022, Proceedings. p. 16–20. Springer-Verlag, Berlin, Heidelberg (2022). https://doi.org/10.1007/978-3-031-11609-4_3, https://doi.org/10.1007/978-3-031-11609-4_3
7. Esteves, B., Rodríguez-Doncel, V.: Analysis of ontologies and policy languages to represent information flows in gdpr. Semantic Web **15**, 1–35 (06 2022). https://doi.org/10.3233/SW-223009
8. Golpayegani, D., Pandit, H., Lewis, D.: AIRO: An Ontology for Representing AI Risks Based on the Proposed EU AI Act and ISO Risk Management Standards (09 2022). https://doi.org/10.3233/SSW220008
9. Golpayegani, D., Pandit, H.J., Lewis, D.: To be high-risk, or not to be—semantic specifications and implications of the ai act's high-risk ai applications and harmonised standards. In: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency. p. 905–915. FAccT '23, Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3593013.3594050, https://doi.org/10.1145/3593013.3594050
10. Golpayegani, D., Pandit, H.J., O'Sullivan, D., Lewis, D.: Semantic frameworks to support implementation of the eu ai act. Computer Law Security Review **61**, 106315 (2026). https://doi.org/https://doi.org/10.1016/j.clsr.2026.106315, https://www.sciencedirect.com/science/article/pii/S2212473X26000568
11. Hulok, M.: The eu model of ai governance: regulating artificial intelligence through law and policy. ERA Forum **26** (12 2025). https://doi.org/10.1007/s12027-025-00869-1
12. J. Pandit, H., Esteves, B., P. Krog, G., Ryan, P., Golpayegani, D., Flake, J.: Data privacy vocabulary (dpv) – version 2.0. In: Demartini, G., Hose, K., Acosta, M., Palmonari, M., Cheng, G., Skaf-Molli, H., Ferranti, N., Hernández, D., Hogan, A. (eds.) The Semantic Web – ISWC 2024. pp. 171–193. Springer Nature Switzerland, Cham (2025)
13. Kebede, M.G., Sileno, G., Van Engers, T.: A critical reflection on odrl. In: Rodríguez-Doncel, V., Palmirani, M., Araszkiewicz, M., Casanovas, P., Pagallo, U., Sartor, G. (eds.) AI Approaches to the Complexity of Legal Systems XI-XII. pp. 48–61. Springer International Publishing, Cham (2021)
14. Kebede, M.G., Sileno, G., Van Engers, T.: A critical reflection on odrl. In: Rodríguez-Doncel, V., Palmirani, M., Araszkiewicz, M., Casanovas, P., Pagallo, U., Sartor, G. (eds.) AI Approaches to the Complexity of Legal Systems XI-XII. pp. 48–61. Springer International Publishing, Cham (2021)

15. Kokina, J., Blanchette, S., Davenport, T.H., Pachamanova, D.: Challenges and opportunities for artificial intelligence in auditing: Evidence from the field. International Journal of Accounting Information Systems **56**, 100734 (2025). https://doi.org/https://doi.org/10.1016/j.accinf.2025.100734, https://www.sciencedirect.com/science/article/pii/S1467089525000107
16. Lazaros, K.P., Vrahatis, A., Kotsiantis, S.: Human-in-the-loop artificial intelligence: A systematic review of concepts, methods, and applications. Entropy **28**, 377 (03 2026). https://doi.org/10.3390/e28040377
17. Leyva-Sánchez, S., Linde, F., Manab, M.A., Poveda-Villalón, M., Rodríguez-Doncel, V.: Daont: A formal ontology for eu data act compliance (2026), https://arxiv.org/abs/2604.16386
18. Lopez Solano, J., de Souza, S., Martin, A., Taylor, L.: Governing Data and Artificial Intelligence for All: Models for Sustainable and Just Data Governance. European Parliament (Jul 2022). https://doi.org/10.2861/915401
19. Nespeca, V., Comes, T., Brazier, F.: A methodology to develop agent-based models for policy support via qualitative inquiry. Journal of Artificial Societies and Social Simulation **26** (01 2023). https://doi.org/10.18564/jasss.5014
20. Pandit, H.J., Polleres, A., Bos, B., Brennan, R., Bruegger, B., Ekaputra, F.J., Fernández, J.D., Hamed, R.G., Kiesling, E., Lizar, M., Schlehahn, E., Steyskal, S., Wenning, R.: Creating a vocabulary for data privacy. In: Panetto, H., Debruyne, C., Hepp, M., Lewis, D., Ardagna, C.A., Meersman, R. (eds.) On the Move to Meaningful Internet Systems: OTM 2019 Conferences. pp. 714–730. Springer International Publishing, Cham (2019)
21. Rane, N., Desai, P., Choudhary, S.: Challenges of implementing artificial intelligence for smart and sustainable industry: Technological, economic, and regulatory barriers, pp. 82–94 (10 2024). https://doi.org/10.70593/978-81-981271-1-2_5
22. Salas, J., Pareti, P., Yumusak, S., Gheisari, S., Ibáñez, L.D., Konstantinidis, G.: Evaluation and comparison semantics for odrl (09 2025). https://doi.org/10.48550/arXiv.2509.05139
23. United Nations System Chief Executives Board for Coordination (CEB): Framework for a model policy on the responsible use of artificial intelligence in un system organizations. Technical Report CEB/2024/HLCM/28/Add.1/Rev.1, High-Level Committee on Management (HLCM) Task Force on the use of Artificial Intelligence in the UN system (October 10 2024), https://unsceb.org/sites/default/files/2024-11/Framework%20for%20a%20Model%20Policy%20on%20the%20%20Responsible%20Use%20of%20AI%20in%20UN%20System.pdf, accessed from United Nations System official repository
24. Von Hafe, F., Wagle, Y., Guede-Fernández, F., Giordano, A.P., Silva, L., Azevedo, S.: Legal frameworks for blockchain applications: a comparative study with implications for innovation in europe. Frontiers in Blockchain **Volume 8 - 2025** (2025). https://doi.org/10.3389/fbloc.2025.1655230, https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2025.1655230
25. Walters, J., Dey, D., Bhaumik, D., Horsman, S.: Complying with the eu ai act. ArXiv **abs/2307.10458** (2023), https://api.semanticscholar.org/CorpusID:259991089