Towards Usage Policy Enforcement in Dataspaces

Andreas Krimbacher[1], Tobias Dam[2][0000−0002−2463−5831], and Sebastian Neumaier[2][0000−0002−9804−4882]

[1] nexyo GmbH, Vienna, Austria
andreas.krimbacher@nexyo.io
[2] St. Pölten University of Applied Sciences, Austria
tobias.dam@fhstp.ac.at
sebastian.neumaier@fhstp.ac.at

1 Introduction

Dataspaces have emerged as a decentralized infrastructure, facilitating data exchange between providers and consumers through specific toolsets, so-called Dataspace connectors. In this context, the Eclipse Dataspace Components (EDC)[3] plays a crucial role by providing such implementations. Developed within the Eclipse Foundation, the EDC promises compatibility with the International Data Spaces (IDS) standard and the GAIA-X project. Eventually, its goal is that through defined data contracts, the EDC enables automated negotiation to regulate controlled access to data assets.

At the time of writing, the EDC, being in an early phase of development, lacks an agreed-upon set of policy patterns that support enforceability by the connector. Additionally, the EDC does currently not offer functionality to administer and manage policies. To address these gaps, we present the following topics of discussion in this position paper:

- **Collection of Policy Patterns:** By conducting a review of existing usage control frameworks, we identify a set of relevant policy patterns for usage control in Dataspaces. These patterns encapsulate common policy requirements and scenarios encountered in data sharing and governance. We have published the complete list of policies online at our Github repository.[4]
- **Representation using ODRL:** To foster interoperability and standardization, we propose the use of the Open Digital Rights Language (ODRL)[5] to represent the collected policies. ODRL is widely adopted

[3] https://github.com/eclipse-edc/Connector, last accessed 27-07-2023
[4] https://github.com/fhstp/dataspaces-policies
[5] https://www.w3.org/TR/2018/REC-odrl-model-20180215/

for expressing permissions, obligations, and conditions related to digital rights, enabling machine-readable policy definitions within Dataspaces. In cases where the ODRL vocabulary is insufficient to articulate a policy, we propose an ODRL Profile extension with Dataspace-specific properties.[6]
- **Policy Administration:** To outline possible approaches to implement Policy Administration Points, we explain how policies are handled in the Nexyo DataHub and how the collected patterns will be integrated in the Nexyo software.

The successful development of Dataspaces necessitates a concrete set of policy patterns for usage control, effectively ready to get implemented by connectors. We advocate for the adoption of ODRL to represent and implement these policies, however, specific vocabulary extensions are needed that require a community effort.

2 Policy Enforcement in Dataspaces

A comprehensive enforcement framework encompasses preventive mechanisms and continuous detective mechanisms to address various aspects of policy enforcement:[7]

- *Preventive Mechanisms:* These dynamic and proactive enforcement mechanisms allow or prohibit data usage requests, revoke access in case of policy violations, delay usage requests until obligations are fulfilled, update user or object attributes based on usage decisions, and execute actions like sending notifications to data owners.
- *Detective Mechanisms:* These mechanisms come into play when the usage control framework cannot enforce policy restrictions or prevent policy violations. Detective mechanisms, such as auditing or logging, provide evidence or indications of executed commands.

To effectively implement usage control enforcement in a distributed and modularized manner, an enforcement framework can be divided into distinct components, with each component handling specific aspects of the process:

- *Policy Decision Point (PDP):* Responsible for making access control decisions, evaluating the request sent by the policy enforcer, and considering applicable policies. Depending on the policy pattern, the data

[6] https://w3id.org/dataspaces-policies/
[7] eXtensible Access Control Markup Language (XACML), OASIS, Version 3.0, 2013. URL: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.

consumer or provider can be responsible for determining the fulfillment.
- *Policy Information Point (PIP):* Provides contextual information during policy evaluation, enhancing the granularity of access control decisions. Such information can be provided by the connector of the provider or consumer, or by a trusted third party.
- *Policy Administration Point (PAP):* Not directly involved in enforcement but crucial for policy specification and management. It handles the creation, activation, and deletion of policies and is typically located at the stakeholder responsible for deploying the policy.

3 Collection of Policy Patterns

In our corresponding Github repository,[8] we provide a collection of policy patterns for usage control. To collect the patterns, the survey of usage control approaches by Akaichi and Kirrane[9] serves as a basis: the list consists of policy examples from the literature, aggregated and classified based on the enforcement types; for each policy pattern the stakeholder responsible for deploying (PAP) and the stakeholder responsible for providing information about its fulfilment (PIP) and evaluating (PDP) the policy is identified.

- *Provider-Administered Policy Patterns:* In this scenarios, the data provider grants permissions to data consumers and enforces policies on data access and usage. For instance, a provider-administered policy where the data provider demands the consumer to delete the data after a specific date and to anonymize the acquired data.

```
<http://example.com/policies#consumer-administered> odrl:permission [
    odrl:assigner <https://www.example.com/provider> ;
    odrl:assignee <https://www.example.com/consumer> ;
    odrl:action odrl:read ;
    odrl:obligation [
      odrl:action odrl:delete ;
      odrl:constraint [
        odrl:leftOperand odrl:dateTime ;
        odrl:operator odrl:lt ;
        odrl:rightOperand "2023-07-10T00:00:00Z"^^xsd:dateTime
      ]
    ], [
      odrl:action odrl:anonymize
    ]
  ] .
```

[8] https://github.com/fhstp/dataspaces-policies

[9] I. Akaichi, S. Kirrane, Usage control specification, enforcement, and robustness: A survey, 2022. URL: https://doi.org/10.48550/arXiv.2203.04800.

– *Consumer-Administered Policy Patterns:* In this type of policy, the data consumer plays an active role in specifying usage control requirements to the data provider. For instance, a consumer-administered policy where the consumer demands the provider to continuously update the data and conform to a specific schema.[10]

```
<http://example.com/policies#consumer-administered>
  odrl:profile <http://www.w3id.org/dataspaces-policies/> ;
  odrl:obligation [
    odrl:assigner <https://www.example.com/consumer> ;
    odrl:assignee <https://www.example.com/provider> ;
    odrl:action <http://www.w3id.org/dataspaces-policies/update> ;
    odrl:constraint [
      odrl:leftOperand odrl:timeInterval ;
      odrl:operator odrl:eq ;
      odrl:rightOperand "P30S"^^xsd:duration
    ]
  ], [
    odrl:action [
      rdf:value <http://www.w3id.org/dataspaces-policies/qualityControl> ;
      odrl:refinement [
       odrl:leftOperand <http://www.w3id.org/dataspaces-policies/conformsTo>;
       odrl:operator odrl:eq ;
       odrl:rightOperand <http://example.com/shacl-shape>
      ]
    ] ;
    odrl:constraint [
      odrl:leftOperand odrl:event ;
      odrl:operator odrl:lt ;
      odrl:rightOperand odrl:policyUsage
    ]
  ] .
```

4 Policy Administration in the Nexyo DataHub

The Nexyo DataHub is a data management platform that allows the administration of data assets in Dataspaces. To this end, it integrates various data connectors, including the EDC connector. Figure 1 displays a screenshot of the Nexyo datahub which showcases the creation of a specific usage policy for a data asset. Currently, it allows to specify the permissions, obligations and prohibitions of a usage policy as textual information, attached to the asset. In a next step of development, our research results on policy patterns will be incorporated into the Nexyo user interface. However, before that, an implementation for the enforcement of concrete policies must also progress in the connector implementations.

[10] This example showcases the use of ODRL with self-defined extensions to formalize the policy requirements.

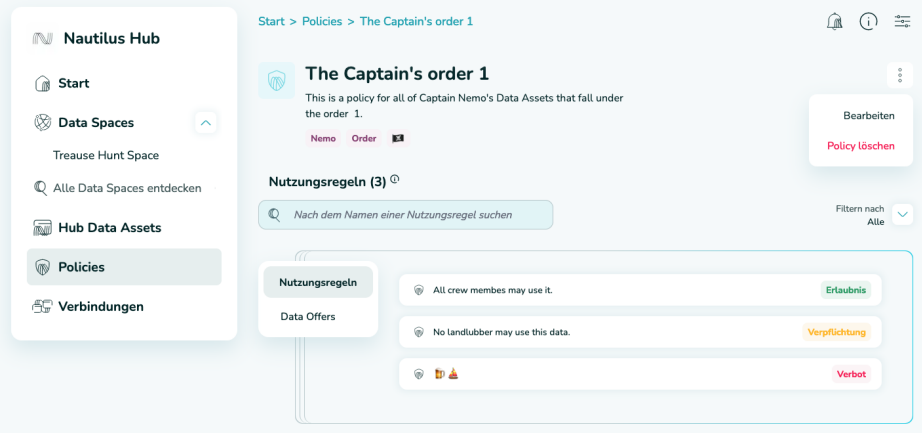

Fig. 1. Screenshot of the policy administration functionality in the Nexyo DataHub.

5 Conclusions

In this position paper, we have proposed a collection of usage control policies for Dataspaces. The goal is to foster the implementation of corresponding enforcement mechanisms in Dataspace connectors such as the EDC. A user-friendly support of the creation and management of policies is essential; in this respect, the nexyo DataHub serves as a policy administration point for the connectors.

We acknowledge that our collection of policy patterns is potentially incomplete and needs further refinement. To provide a more comprehensive collection, and corresponding ODRL models, that align with the needs of data sharing companies, future research will focus on gathering real-world use cases and obtaining feedback from these companies.

In some of the proposed policy patterns, we have found that the existing ODRL core and common vocabulary are not sufficient to create ODRL instantiations. To this end, we have developed an initial set of complementing terms as an ODRL Profile;[11] this extension needs further definition, extension and evaluation in future work.

Acknowledgements

This research was funded by the Austrian Research Promotion Agency (FFG) through BRIDGE project 891103 “DiDaMe”. The financial support by the Austrian Research Promotion Agency is gratefully acknowledged.

[11] https://w3id.org/dataspaces-policies