Solid Symposium

KG Usage Control Policy Framework

WIRTSCHAFTS
UNIVERSITÄT
WIEN VIENNA
UNIVERSITY OF
ECONOMICS
AND BUSINESS

KNOW GRAPHS

Ines Akaichi, Giorgos Flouris, Irini Fundulaki, and Sabrina Kirrane

EQUIS ACCREDITED AACSB ACCREDITED ASSOCIATION OF MBAS AMBA ACCREDITED

Nuremberg, Germany, March 31st 2023

Usage Control
Context

- An extension of access control
- Regulates usage of the data: permissions (prohibitions) and obligations (dispensations)
- Ensures data sovereignty
- It involves data consumers and data providers/owners
- Related to data storage, distribution, aggregation and processing
- Context of **intellectual property protection**, **privacy protection**, **compliance with regulations** and **digital rights management**

We focus on **policy-based usage control**, where we use **machine-readable policies** to express requirements for future data usage and mechanisms to enforce the respective usage policies

Usage Control
Context

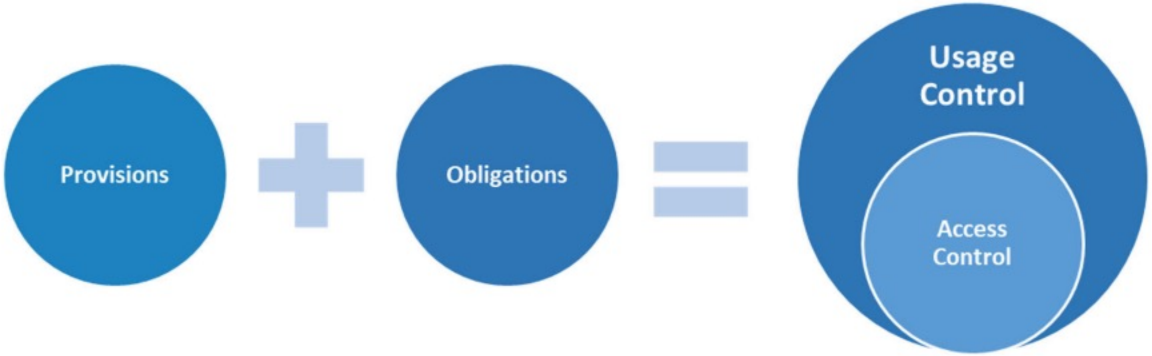


Figure taken from Usage Control in the International Data Spaces V3.0 (2021). Steinbuss et al.

Usage Control Policy Languages
Related Work

- Usage control policy frameworks/ languages
  - UCON (Park et al., 2004) and derivatives cf. (Colombo et al.,2010), (Quintero et al., 2021)
  - The Obligation Specifcation Language (Hilty et al., 2007)
  - ...
- General policy languages
  - Kaos (Uszok et al, 2003)
  - Rei (Kagal et al., 2003)
  - ...
- Tailored policy languages
  - ODRL (Iannella et al., 2018)
  - The Special Policy Language (Bonatti et al., 2020)
  - …

Use Case
Legal Requirements

The legal requirements regarding the registration process in Austria:

Rule 1. A person is obliged to register their address with one of the local authorities within three days of changing residence or having moved from abroad to Austria.

Rule 2. A person is obliged to deregister their old address within three days of changing their place of residence, or of leaving the country.

Rule 3. Tourists in Austria are exempt from registering their address.

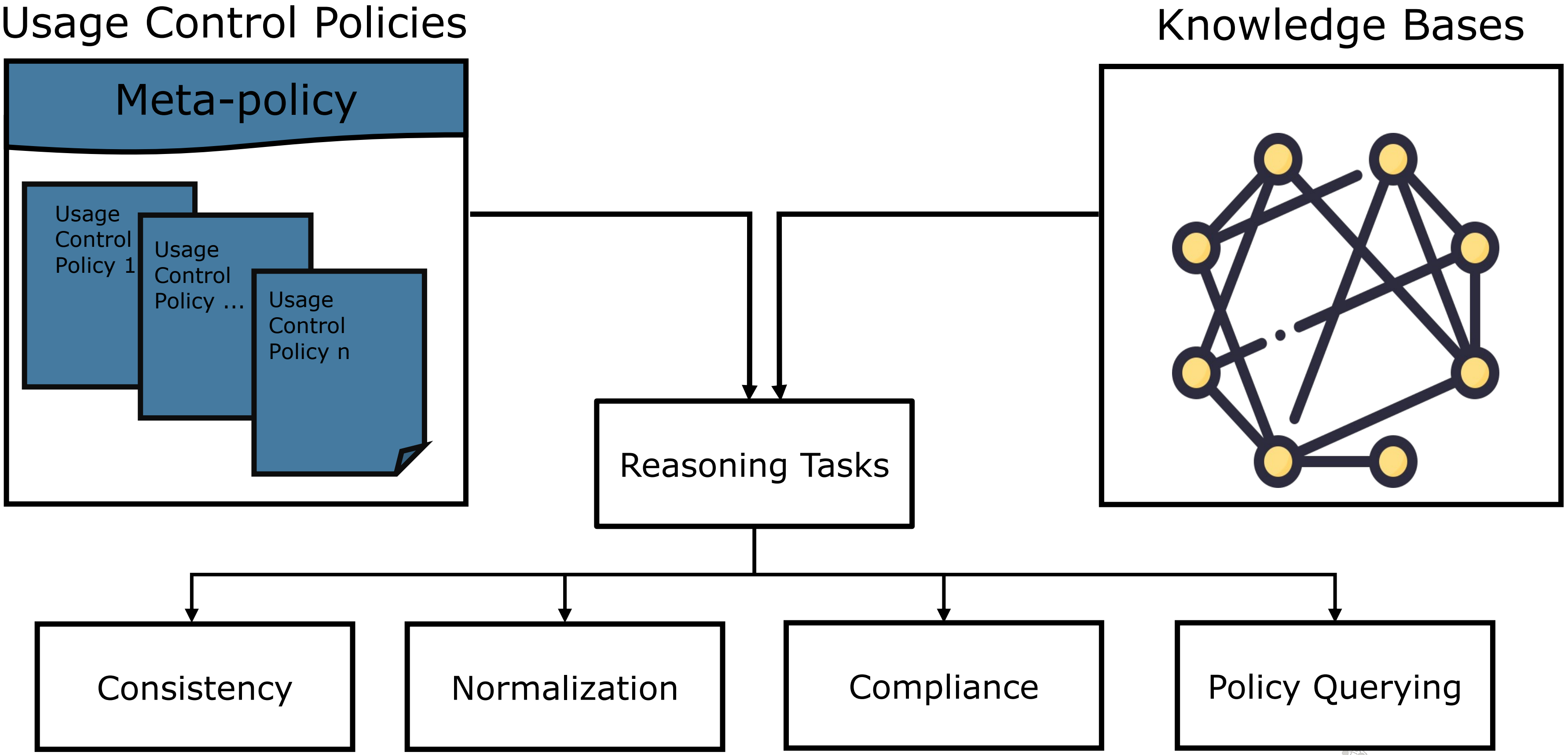
Rule 4. If the person stays in a hotel, they are allowed to request a signature from the hotel.

Rule 5. If the person stays in with friends or family members, they are allowed to request a signature from the property owner.

Rule 6. A person is not allowed to open a bank account if they do not have a certificate of registration.

KG Usage Control Policy Framework

Reasoning Tasks



Usage Control Policies

Knowledge Bases

Meta-policy

Usage Control Policy 1

Usage Control Policy ...

Usage Control Policy n

Reasoning Tasks

Consistency

Normalization

Compliance

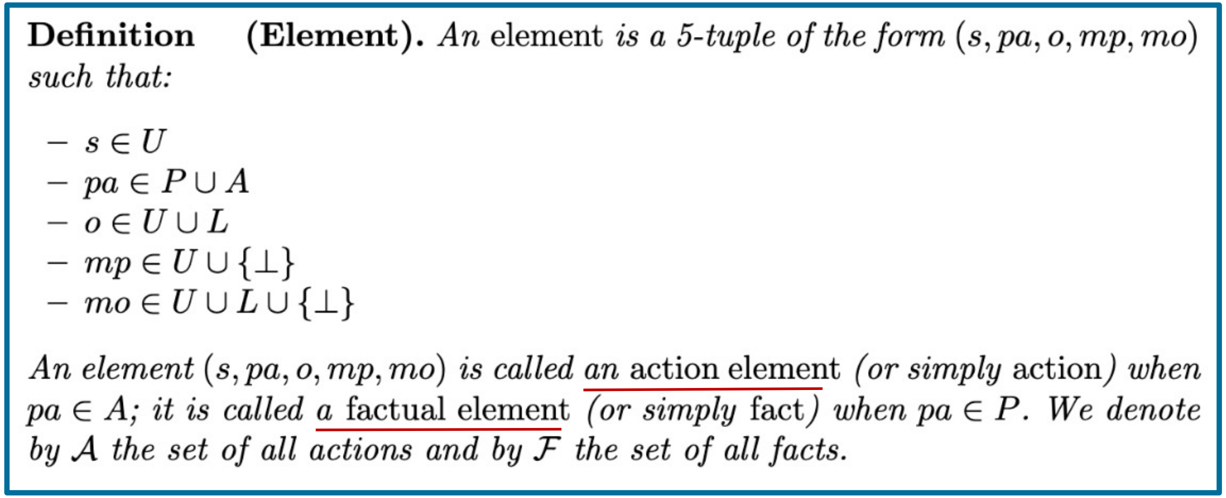
Policy Querying

KG Usage Control Policy Framework
Notation

- **O, D, P, A** denote the deontic operators **Obligation**, **Dispensation**, **Prohibition**, and **Permission** (allowance)
- ***U*** and ***L*** denote the set of ***URIs*** and ***literals*** respectively.
- ***T*** denote the union of ***U*** ∪ ***L***
- ***P*** , ***A*** such that ***P*** ⊆ ***U*** **,** ***A*** ⊆ ***U***

KG Usage Control Policy Framework

Basic Elements: Action and Factual Elements



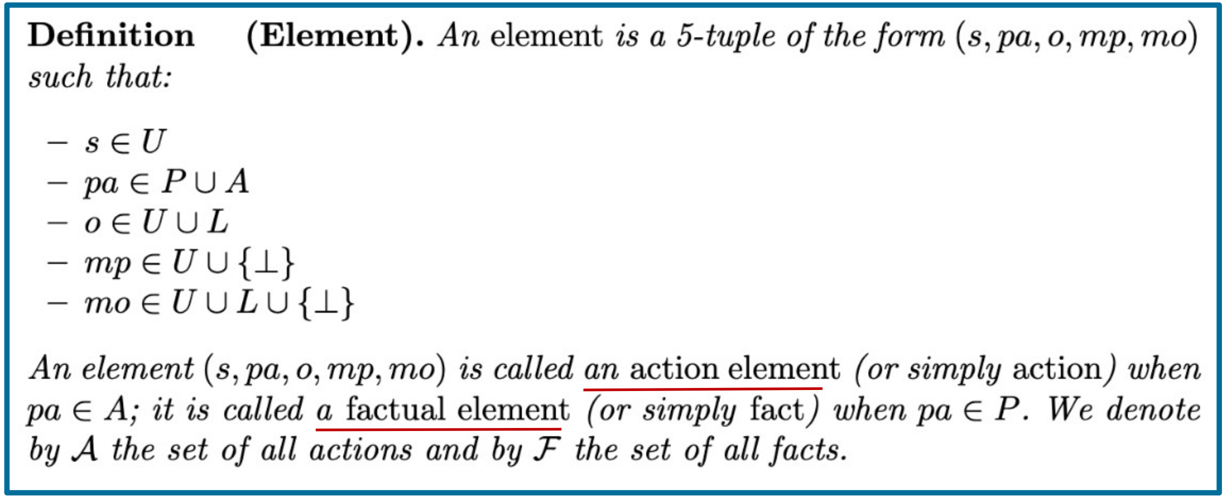
Definition (Element). *An* element *is a 5-tuple of the form* (s, pa, o, mp, mo) *such that:*

- $s \in U$
- $pa \in P \cup A$
- $o \in U \cup L$
- $mp \in U \cup \{\perp\}$
- $mo \in U \cup L \cup \{\perp\}$

An element (s, pa, o, mp, mo) *is called an* action element *(or simply* action*) when* $pa \in A$*; it is called a* factual element *(or simply* fact*) when* $pa \in P$*. We denote by* $\mathcal{A}$ *the set of all actions and by* $\mathcal{F}$ *the set of all facts.*

s, pa, o, mp, and mo denote respectively the concepts of subject, property action, object, meta-property, and metaobject.

KG Usage Control Policy Framework
Basic Elements: Action and Factual Elements



Definition (Element). *An element is a 5-tuple of the form* (s, pa, o, mp, mo) *such that:*

- $s \in U$
- $pa \in P \cup A$
- $o \in U \cup L$
- $mp \in U \cup \{\bot\}$
- $mo \in U \cup L \cup \{\bot\}$

An element (s, pa, o, mp, mo) *is called an* action element *(or simply* action*) when* $pa \in A$*; it is called a* factual element *(or simply* fact*) when* $pa \in P$*. We denote by* $\mathcal{A}$ *the set of all actions and by* $\mathcal{F}$ *the set of all facts.*

s, pa, o, mp, and mo denote respectively the concepts of subject, property action, object, meta-property, and metaobject.

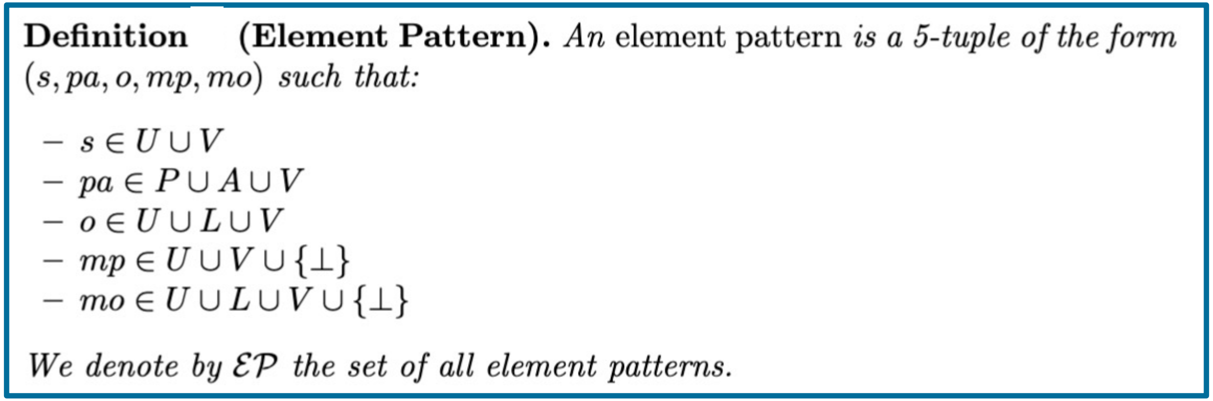
Action Element:

```
(:alice, :register, :boulevard18, :on, :21-08-2022)
```

Factual Elements:

```
(:alice, :type, :Person)
(:alice, :movedTo, :boulevard18, :on, :22-08-2022)
(:boulevard18, :type, :Address)
```

KG Usage Control Policy Framework
Basic Elements: Element Pattern



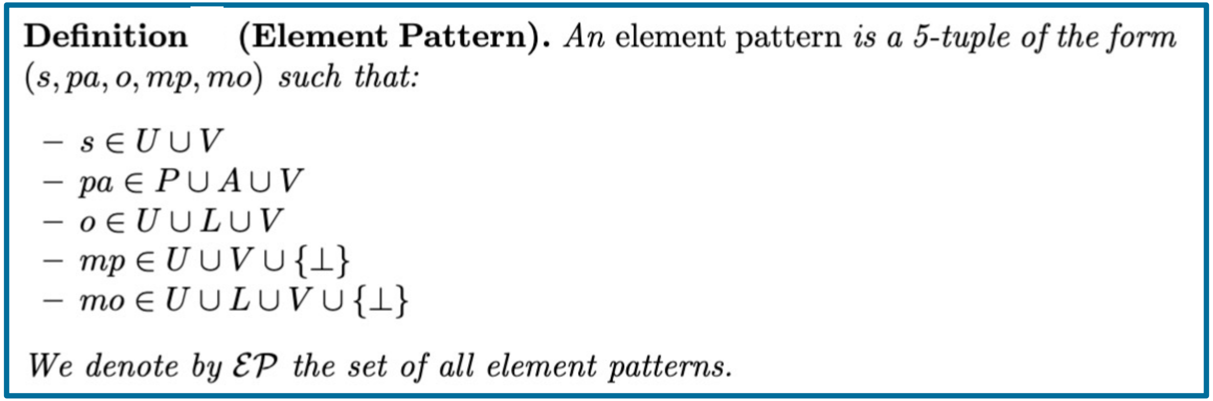
Definition (Element Pattern). *An* element pattern *is a 5-tuple of the form* (s, pa, o, mp, mo) *such that:*

- $s \in U \cup V$
- $pa \in P \cup A \cup V$
- $o \in U \cup L \cup V$
- $mp \in U \cup V \cup \{\perp\}$
- $mo \in U \cup L \cup V \cup \{\perp\}$

We denote by $\mathcal{EP}$ *the set of all element patterns.*

KG Usage Control Policy Framework

Basic Elements: Element Pattern



Definition (Element Pattern). *An* element pattern *is a 5-tuple of the form* (s, pa, o, mp, mo) *such that:*

- $s \in U \cup V$
- $pa \in P \cup A \cup V$
- $o \in U \cup L \cup V$
- $mp \in U \cup V \cup \{\perp\}$
- $mo \in U \cup L \cup V \cup \{\perp\}$

We denote by $\mathcal{EP}$ *the set of all element patterns.*

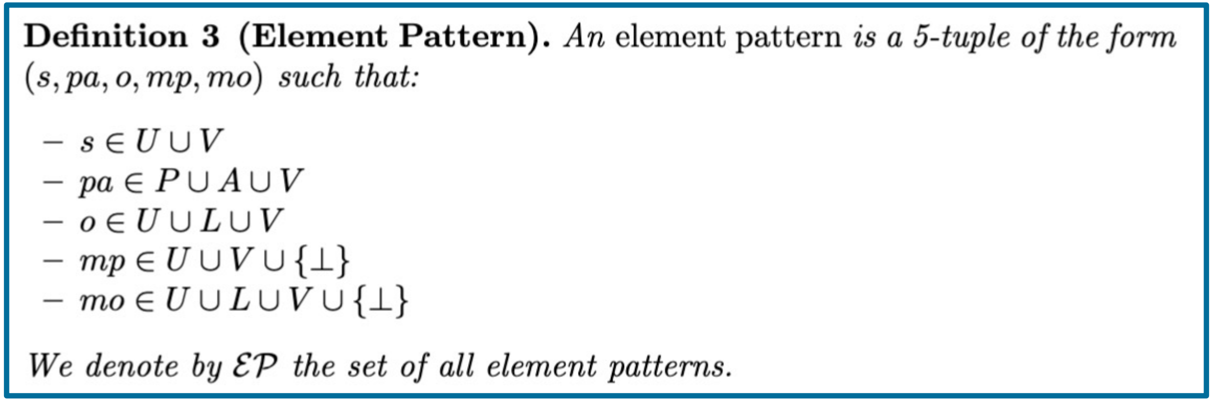
A person is obliged to register their address if they move.

Element Pattern:

```
(?x, :register, ?y, ?mp, ?mo)
```

KG Usage Control Policy Framework

Basic Elements: Element Pattern



Definition 3 (Element Pattern). *An* element pattern *is a 5-tuple of the form* (s, pa, o, mp, mo) *such that:*

- $s \in U \cup V$
- $pa \in P \cup A \cup V$
- $o \in U \cup L \cup V$
- $mp \in U \cup V \cup \{\perp\}$
- $mo \in U \cup L \cup V \cup \{\perp\}$

We denote by $\mathcal{EP}$ *the set of all element patterns.*

A person is obliged to register their address if they move.

Element Pattern:

```
(?x, :register, ?y, ?mp, ?mo)
```

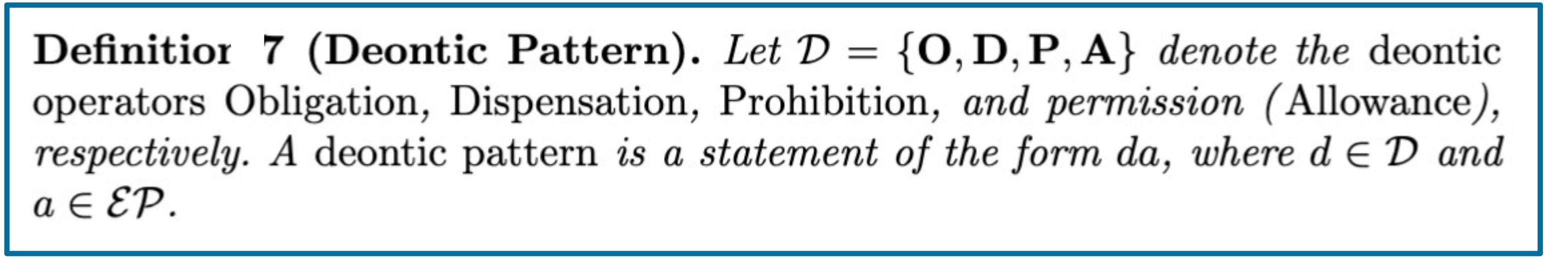
Conditions:

```
(?x, :type, :Person)
(?x, :movedTo, ?y)
(?y, :type, :Address)
```

We’ll come back to this

KG Usage Control Policy Framework

Basic Elements: Deontic Pattern



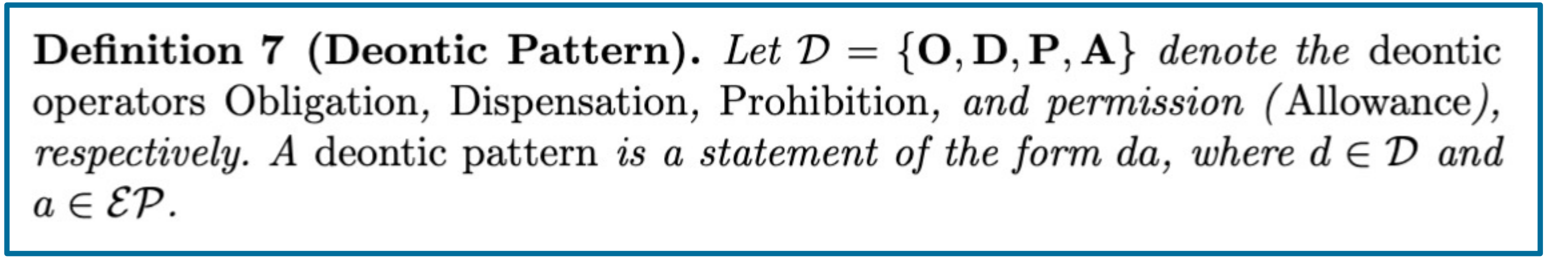
Definitior 7 (Deontic Pattern). *Let* $\mathcal{D} = \{\mathbf{O}, \mathbf{D}, \mathbf{P}, \mathbf{A}\}$ *denote the* deontic operators Obligation, Dispensation, Prohibition, *and permission (*Allowance*), respectively. A* deontic pattern *is a statement of the form da, where* $d \in \mathcal{D}$ *and* $a \in \mathcal{EP}$.

Denotic Pattern:
A person is obliged to register their address if they move.

```
O(?x, :register, ?y, ?mp, ?mo)
```

KG Usage Control Policy Framework

Basic Elements: Deontic Pattern



Definition 7 (Deontic Pattern). *Let* $\mathcal{D} = \{\mathbf{O}, \mathbf{D}, \mathbf{P}, \mathbf{A}\}$ *denote the* deontic operators Obligation, Dispensation, Prohibition, *and permission (*Allowance*), respectively. A* deontic pattern *is a statement of the form* da*, where* $d \in \mathcal{D}$ *and* $a \in \mathcal{EP}$*.*

Denotic Pattern:

A person is obliged to register their address if they move.

```
O(?x, :register, ?y, ?mp, ?mo)
```

Conditions:

```
(?x, :type, :Person)
(?x, :movedTo, ?y)
(?y, :type, :Address)
```

We'll look at this next

KG Usage Control Policy Framework

Usage Control Policies

- A set of rules
- Each rule follows the form: IF **condition** THEN **Aa** | **Pa** | **Oa** | **Da**

A person is obliged to register their address if they move.

```
(?x, :moveTo, ?y).(?x, :type, :Person).(?y, :type, :Address)
⇝ O(?x, :register, ?y, ?mp, ?mo)
```

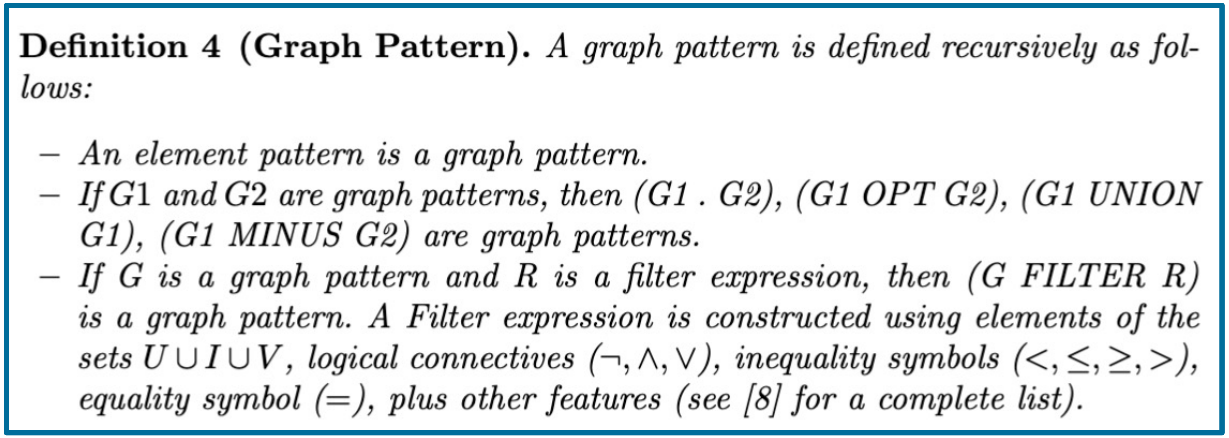
KG Usage Control Policy Framework

Usage Control Policies

- A set of rules
- Each rule follows the form: IF **condition** THEN **Aa** | **Pa** | **Oa** | **Da**

A person is obliged to register their address if they move.

```
(?x, :moveTo, ?y).(?x, :type, :Person).(?y, :type, :Address)
⇝ O(?x, :register, ?y, ?mp, ?mo)
```



Definition 4 (Graph Pattern). *A graph pattern is defined recursively as follows:*

- *An element pattern is a graph pattern.*
- *If G1 and G2 are graph patterns, then (G1 . G2), (G1 OPT G2), (G1 UNION G1), (G1 MINUS G2) are graph patterns.*
- *If G is a graph pattern and R is a filter expression, then (G FILTER R) is a graph pattern. A Filter expression is constructed using elements of the sets $U \cup I \cup V$, logical connectives $(\neg, \wedge, \vee)$, inequality symbols $(<, \leq, \geq, >)$, equality symbol $(=)$, plus other features (see [8] for a complete list).*

Use Case

Legal Requirements

The legal requirements regarding the registration process in Austria:

Rule 1. A person is obliged to register their address with one of the local authorities within three days of changing residence or having moved from abroad to Austria.

Rule 2. A person is obliged to deregister their old address within three days of changing their place of residence, or of leaving the country.

Rule 3. Tourists in Austria are exempt from registering their address.

Rule 4. If the person stays in a hotel, they are allowed to request a signature from the hotel.

Rule 5. If the person stays in with friends or family members, they are allowed to request a signature from the property owner.

Rule 6. A person is not allowed to open a bank account if they do not have a certificate of registration.

KG Usage Control Policy Framework

Instantiations

- Different Initiatives:
    - ODRL (*Ontology Engineering Group at Universidad Politécnica de Madrid*)
    - SHACL (*L3S research center at Leibniz Universität Hannover*)
    - RDF surfaces (*IDLab at Ghent University*)
    - Description Logics (*us*)

    - Other suggestions?

References

Park, J., & Sandhu, R. (2004). The UCON ABC Usage Control Model. *ACM Transactions on Information and System Security, 7*(1), 128–174. https://doi.org/10.1145/984334.984339

Colombo, M., Lazouski, A., Martinelli, F., Mori, P. (2010). A Proposal on Enhancing XACML with Continuous Usage Control Features. In: Desprez, F., Getov, V., Priol, T., Yahyapour, R. (Eds.), *Grids, P2P and Services Computing*. Springer. https://doi.org/10.1007/978-1-4419-6794-7_11

Quintero, A.M.R., Pérez, S., Varela-Vaca, A., López, M.T.G., & Cabot, J. (2021). A domain-specific language for the specification of UCON policies. *Journal of Information Security and Applications, 64. https://doi.org/10.1016/j.jisa.2021.103006*

Hilty, M., Pretschner, A., Basin, D.A., Schaefer, C., & Walter, T. (2007). A Policy Language for Distributed Usage Control. In: Biskup, J., López, J. (Eds.), *Computer Security – ESORICS 2007, 4734*. Springer. https://doi.org/10.1007/978-3-540-74835-9_35

Uszok, A., Bradshaw, J., Jeffers, R., Suri, N., Hayes, P., Breedy, M., Bunch, L., Johnson, M. , Kulkarni, S., & Lott, J. (2003). KAoS Policy and Domain Services: Toward a Description-Logic Approach to Policy Representation, Deconfliction, and Enforcement. *In Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks (93-96)*. IEEE Computer Society. https://doi.org/10.1109/POLICY.2003.1206963

Kagal, L., Finin, T., & Joshi, A. (2003). A Policy Based Approach to Security for the Semantic Web. *In: Fensel, D., Sycara, K., Mylopoulos, J. (Eds.) The Semantic Web - ISWC 2003, 2870*. Springer. https://doi.org/10.1007/978-3-540-39718-2_26

Iannella, R. & Villata, S. (2018). The Open Digital Rights Language (ODRL). https://www.w3.org/TR/odrl-model/

Bonatti, P.A., Kirrane, S., Petrova, I.M. & Sauro, L. (2020). Machine Understandable Policies and GDPR Compliance Checking. *Künstl Intell* 34, 303–315. https://doi.org/10.1007/s13218-020-00677-4

Cao,Q., Giyyarpuram,M., Farahbakhsh,R., & Crespi, N. (2020). Policy-based usage control for a trustworthy data sharing platform in smart cities. *Future Gener. Comput. Syst., 107*, 998–1010. https://doi.org/10.1016/j.future.2017.05.039

Perez, J., Arenas, M., Gutierrez, C. (2006). Semantics and Complexity of SPARQL. *In: The Semantic Web - ISWC 2006, 4273.* Springer. https://doi.org/10.1145/1567274.1567278

Kirrane, S., Fernandez, J.D, Bonatti, P., Milosevic, U., Polleres, A., & Wenning, R. (2020). The SPECIAL-K Personal Data Processing Transparency and Compliance Platform. https://arxiv.org/abs/2001.09461