

Access Control, Policies, and Quality



Sabrina Kirrane

Dagstuhl 24061: Are KGs Ready for the Real World?

7.2.2023



Some Background Information

Access Policies

Consent Policies

Licenses

Regulatory Constraints

Encryption

Privacy

Enforcement

Administration

Transparency

Compliance

Web Standards

Normative Multi-Agent Systems

Intelligent Agents

Cyber Physical Social System

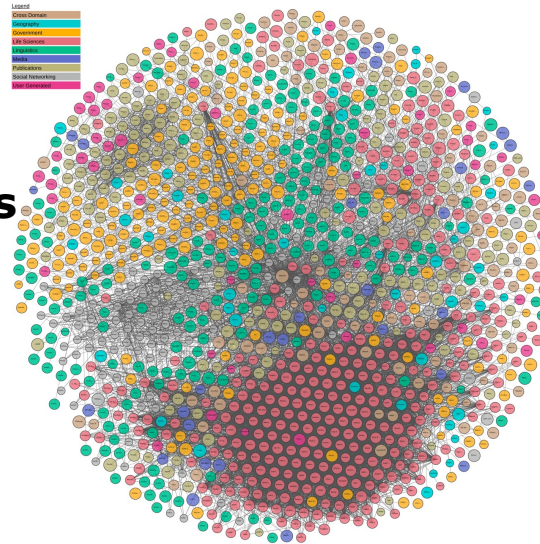
Blockchain

Decentralisation

Artificial Intelligence

Big Data

Data Science

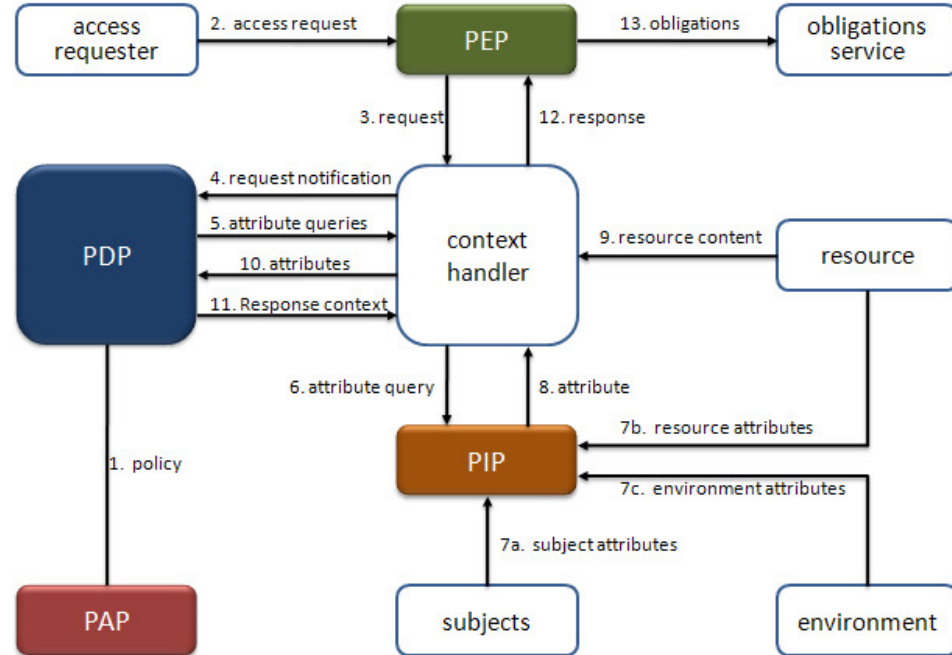


Let's take a quick look at some relevant standards!

Access Control



<https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-en.html>



Policy Administration Point (PAP)
Policy Enforcement Point (PEP)
Policy Decision Point (PDP)
Policy Information Point (PIP)

Licensing

Check out the work of the DALICC project,
Serena Villata, Víctor Rodríguez-Doncel &
Patricia Serrano-Alvarado

W3C Recommendation

ODRL Information Model 2.2

W3C Recommendation 15 February 2018

This version:

<https://www.w3.org/TR/2018/REC-odrl-model-20180215/>

Latest published version:

<https://www.w3.org/TR/odrl-model/>

Latest editor's draft:

<https://w3c.github.io/poe/model/>

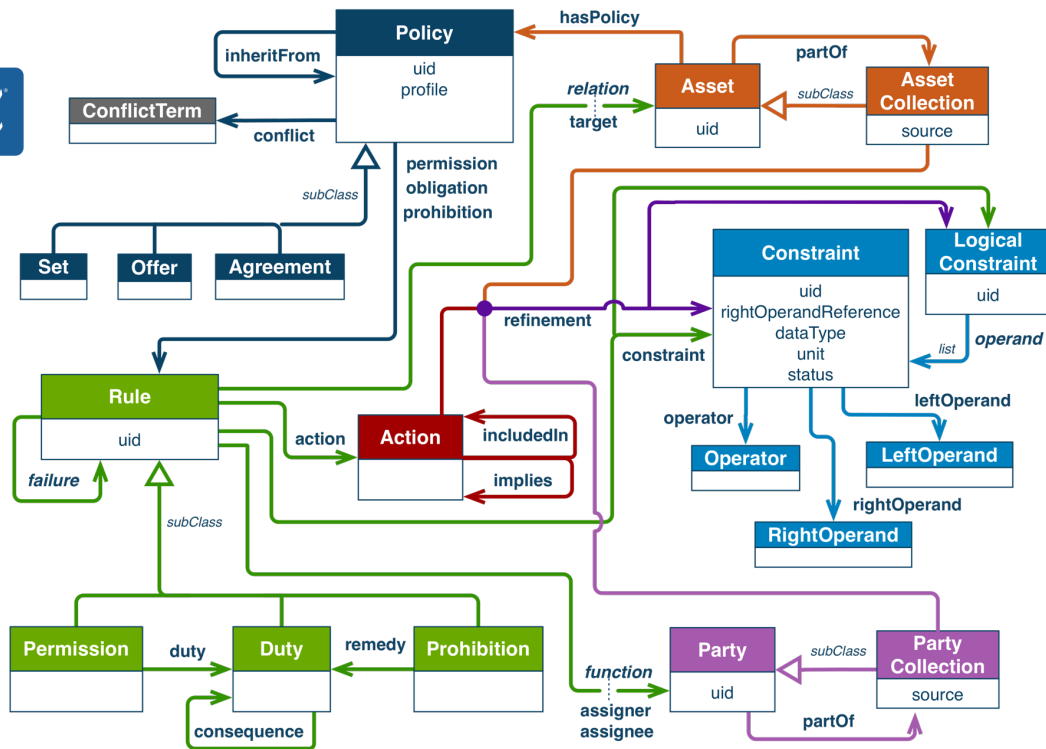
Implementation report:

<https://w3c.github.io/poe/test/implementors>

Previous version:

<https://www.w3.org/TR/2018/PR-odrl-model-20180104/>

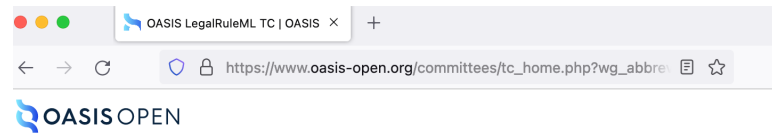
<https://www.w3.org/TR/odrl-model/>



Norms

Check out the work of Guido Governatori & Monica Palmirani

BUSINESS



OASIS LegalRuleML TC

[Join This TC](#) [TC Members Page](#) [Send A Comment](#)

Enabling legal arguments to be created, evaluated, and compared using rule representation tools

Guido Governatori,
guido.governatori2@unibo.it, Chair
Monica Palmirani,
monica.palmirani@unibo.it, Chair

[Table of Contents](#)

- [Announcements](#)
- [Overview](#)
- [Subcommittees](#)

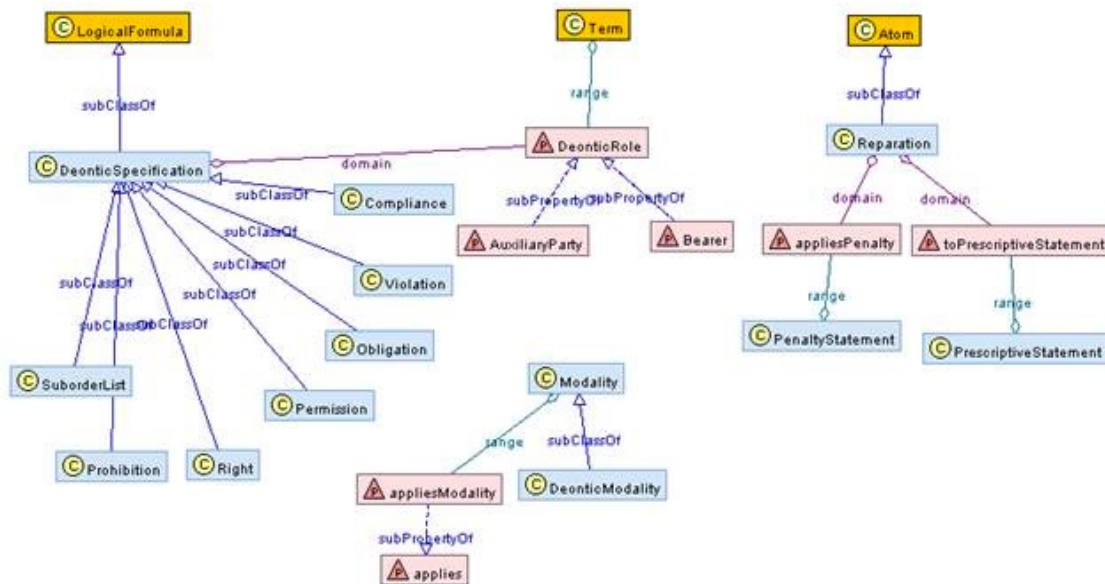
Related links

- [Charter](#)
- [IPR Statement](#)
- [Membership](#)
- [Obligated Members](#)
- [Email Archives](#)
- [Comments Archive](#)
- [Ballots](#)
- [Documents](#)
- [Schedule](#)

TC Participants

Representing these [OASIS Foundationals](#) and [Sponsors](#):

- [Red Hat](#)



https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=legalruleml

OWL-based Usage Policies

Check out the work of the
SPECIAL & TRAPEZE projects

OWL 2 Web Ontology Language Document Overview (Second Edition)

W3C Recommendation 11 December 2012

This version:

<http://www.w3.org/TR/2012/REC-owl2-overview-20121211/>

Latest version (series 2):

<http://www.w3.org/TR/owl2-overview/>

Latest Recommendation:

<http://www.w3.org/TR/owl-overview>

Previous version:

<http://www.w3.org/TR/2012/PER-owl2-overview-20121018/>

Editors:

W3C OWL Working Group (see [Acknowledgements](#))

<https://www.w3.org/TR/owl2-overview/>

SPECIAL's Usage Policy Language Grammar

```
UsagePolicy ::= 'ObjectUnionOf' '(' ' BasicUsagePolicy BasicUsagePolicy { BasicUsagePolicy } ')  
            | BasicUsagePolicy  
BasicUsagePolicy ::= 'ObjectIntersectionOf' '(' ' Data Purpose Processing Recipients Storage ')  
Data ::= 'ObjectSomeValueFrom' '(' 'spl:hasData' DataExpression ')'  
Purpose ::= 'ObjectSomeValueFrom' '(' 'spl:hasPurpose' PurposeExpression ')'  
Processing ::= 'ObjectSomeValueFrom' '(' 'spl:hasProcessing' ProcessingExpression ')'  
Recipients ::= 'ObjectSomeValueFrom' '(' 'spl:hasRecipient' RecipientExpression ')'  
Storage ::= 'ObjectSomeValueFrom' '(' 'spl:hasStorage' StorageExpression ')  
DataExpression ::= 'spl:AnyData' | DataVocabExpression  
PurposeExpression ::= 'spl:AnyPurpose' | PurposeVocabExpression  
ProcessingExpression ::= 'spl:AnyProcessing' | ProcessingVocabExpression  
RecipientsExpression ::= 'spl:AnyRecipient' | 'spl:Null' | RecipientVocabExpression  
StorageExpression ::= 'spl:AnyStorage' | 'spl:Null' |  
                    'ObjectIntersectionOf' '(' ' Location Duration ')'  
Location ::= 'ObjectSomeValueFrom' '(' 'spl:hasLocation' LocationExpression ')'  
Duration ::= 'ObjectSomeValueFrom' '(' 'spl:hasDuration' DurationExpression ')  
            | 'DataSomeValueFrom' '(' 'spl:durationInDays' IntervalExpression ')'
```

Data Privacy Vocabularies

Check out the work of the
SPECIAL & TRAPEZE projects

Data Privacy Vocabulary (DPV)

version 1

[Final Community Group Report](#) 05 December 2022

This version:

<https://www.w3.org/community/reports/dpvcg/CG-FINAL-dpv-20221205/>

Latest published version:

<https://w3id.org/dpv>

Latest editor's draft:

<https://w3id.org/dpv/ed/dpv>

Editor:

[Harshvardhan J. Pandit](#) (ADAPT Centre, Dublin City University)

Former editor:

[Axel Polleres](#) (Vienna University of Economics and Business) - Until 31 December 2019

final reports / licensing info

date	name	commitments
2022-12-05	Data Privacy Vocabulary (DPV)	Licensing commitments
2022-12-05	DPV-GDPR: GDPR Extension for DPV	Licensing commitments
2022-12-05	DPV-PD: Extended Personal Data categories for DPV	Licensing commitments
2022-12-05	Primer	Licensing commitments
2022-12-05	Guide for using DPV in OWL2	Licensing commitments

- **Entities** - different kinds of entities, the specific [Legal Roles](#) they can take, and categories of [Organisations](#), [Authorities](#), and [Data Subjects](#).
- **Purposes** that justify the need or goal for which personal data is processed.
- **Processing operations over personal data**.
- **Personal Data** that is relevant for processing.
- **Technical & Organisational Measures** with dedicated sections for [technical](#) and [organisational](#) measures.
- **Legal Bases** that justify the processing, with a dedicated section for [Consent](#).
- **Contextual information about Processing** such as storage conditions and automation, as well as [Scale of Processing](#).
- **Contextual information in general** such as frequency and duration, and [Statuses](#) associated with activities.
- **Locations & Jurisdictions** providing relevance to laws, authorities, and location contexts.
- **Risk & Impacts** for risk assessment, management, and expression of consequences and impacts associated with processing.
- **Rights and Rights Exercise** for specifying what rights are applicable, how they can be exercised, and how to provide information associated with rights.
- **Rules** for expressing constraints, requirements, and other forms of rules that can specify or assist in interpreting what is permitted, prohibited, mandatory, etc.

Constraints

Check out the survey “SHACL and ShEx in the wild: a community survey on validating shapes generation and adoption” by Kashif Rabbani, Matteo Lissandrini & Katja Hose

W3C Recommendation

Shapes Constraint Language (SHACL)

W3C Recommendation 20 July 2017

This version:

<https://www.w3.org/TR/2017/REC-shacl-20170720/>

Latest published version:

<https://www.w3.org/TR/shacl/>

Latest editor's draft:

<https://w3c.github.io/data-shapes/shacl/>

Implementation report:

<https://w3c.github.io/data-shapes/data-shapes-test-suite/>

Previous version:

<https://www.w3.org/TR/2017/PR-shacl-20170608/>

Editors:

[Holger Knublauch](#), [TopQuadrant, Inc.](#)

[Dimitris Kontokostas](#), [University of Leipzig](#)

<https://www.w3.org/TR/shacl/>

W3C Recommendation

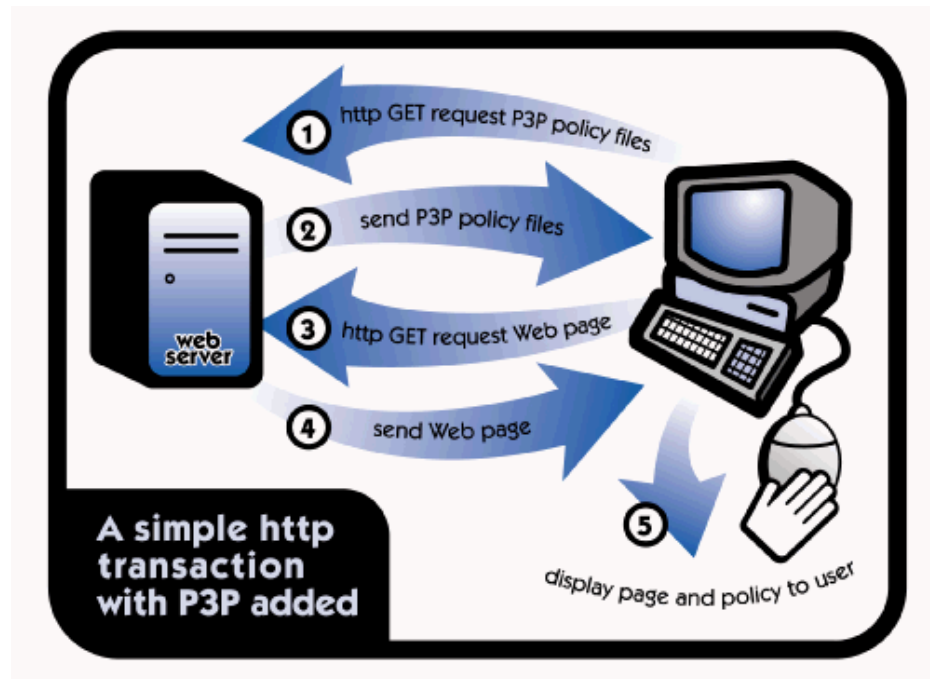
Example validation results

```
[ a sh:ValidationReport ;
  sh:conforms false ;
  sh:result
    [ a sh:ValidationResult ;
      sh:resultSeverity sh:Violation ;
      sh:focusNode ex:Alice ;
      sh:resultPath ex:ssn ;
      sh:value "987-65-432A" ;
      sh:sourceConstraintComponent sh:RegexConstraintComponent ;
      sh:sourceShape ... blank node _:b1 on ex:ssn above ... ;
    ] ,
```

Privacy Preferences

The screenshot shows a Mozilla Firefox browser window with the address bar at www.w3.org/P3P/. The page header includes the W3C logo and the text "Platform for Privacy Preferences Technology and Society Initiative domain". The main heading is "PLATFORM FOR PRIVACY PREFERENCES (P3P) PROJECT" with the subtitle "Enabling smarter Privacy Tools for the Web". Below this, there is a section for "PLING - W3C POLICY LANGUAGES INTEREST GROUP" dated 3 October 2007, and a "DOCUMENTS" section listing "P3P 1.1:" with links to "Final P3P 1.1 Working Group Note" and "P3P 1.0:" with links to "P3P 1.0 Recommendation" in Japanese and French. A status bar at the bottom indicates "STATUS: P3P WORK SUSPENDED".

<https://www.w3.org/P3P/>



From Access Control to Usage Control

Access Control for RDF - Policy Representation and Enforcement

	Policy Representation	Enforcement Framework
Abel et al. [1]	RDF patterns with WHERE clause	query rewriting via bindings
Amini and Jalili [3] Ehsan et al. [26]	-	reasoning framework
Bao et al. [4]		safe reasoning
Chen and Stuckenschmidt [14]	-	query rewriting via FILTERS
Dietzold and Auer [25]	ontology triples, classes and properties	using SPARQL views for data filtering
Flouris et al. [31]	RDF patterns with WHERE clause	-
Franzoni et al. [32]	-	query rewriting via bindings
Gabillon and Letouzey [33]	-	SPARQL views for data filtering
Jain and Farkas [41]	RDF patterns	RDFS inference to deduce annotations
Javanmardi et al. [43]	-	reasoning over ontology concepts, properties and individuals
Kim et al. [50]	-	RDFS inference to deduce authorisations
Kirrane et al. [53,52]	RDF patterns	flexible authorisation framework
Li and Cheung [57]	views	query rewriting via expanded views
Lopes et al. [58]	-	RDFS inference and rights propagation
Mühleisen et al. [60]	ontology triple patterns, resources and instances	temporary named graphs for data filtering
Oulmakhzoune et al. [64]	-	query rewriting via FILTERS
Papakonstantinou et al. [65]	-	RDFS inference and rights propagation
Qin and Atluri [69]	-	reasoning over ontology concepts
Reddivari et al. [70]	RDF patterns	-
Ryutov et al. [72,73]	-	reasoning based on the semantic network
Sacco et al. [77] Sacco and Passant [75,76] Sacco and Breslin [74]	using ontologies to extend WAC	SPARQL ASK queries
Steyskal and Polleres [86,87]	using ontologies to represent ODRL	
Villata et al. [100] Costabello et al. [17,18]	using ontologies to extend WAC	SPARQL ASK queries, query rewriting using named graphs

Access Control and the Resource Description Framework: A Survey

Editor(s): Bernardo Cuenca Grau, University of Oxford, UK
Solicited review(s): Luca Costabello, Fujitsu, Ireland; One anonymous reviewer

Sabrina Kirrane ^{a,*}, Alessandra Mileo ^b, Stefan Decker ^c

^a Vienna University of Business and Economics, Austria

E-mail: sabrina.kirrane@wu.ac.at

^b Insight Centre for Data Analytics, National University of Ireland, Galway, Ireland

E-mail: alessandra.mileo@insight-centre.org

^c RWTH Aachen University, Germany

E-mail: stefan@stefandecker.org

Semantic Web Journal, 2017

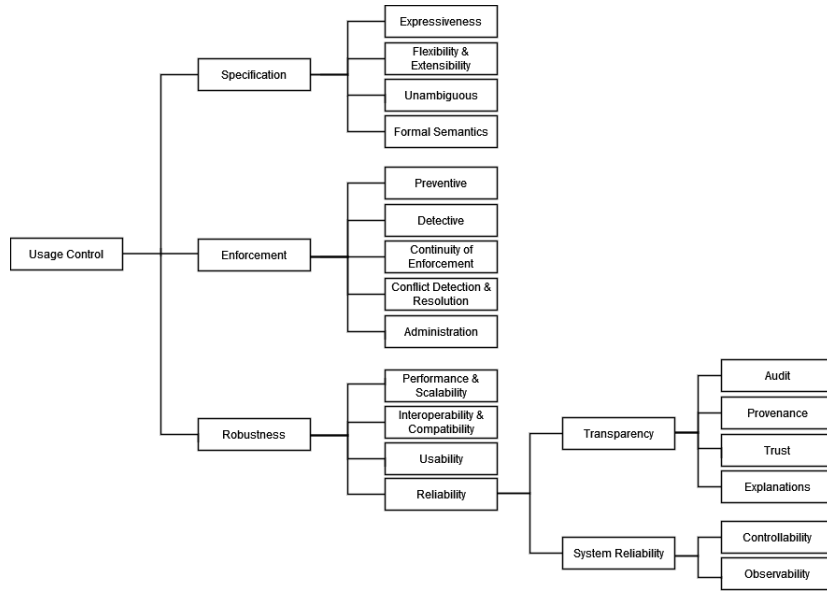
Areas that still need attention

- Usability
- Understandability
- Explanations & Negotiation
- Effectiveness

Usage Control Specification, Enforcement, and Robustness: A Survey

INES AKAICHI and SABRINA KIRRANE, Institute for Information Systems & New Media, Vienna
University of Economics and Business, Austria

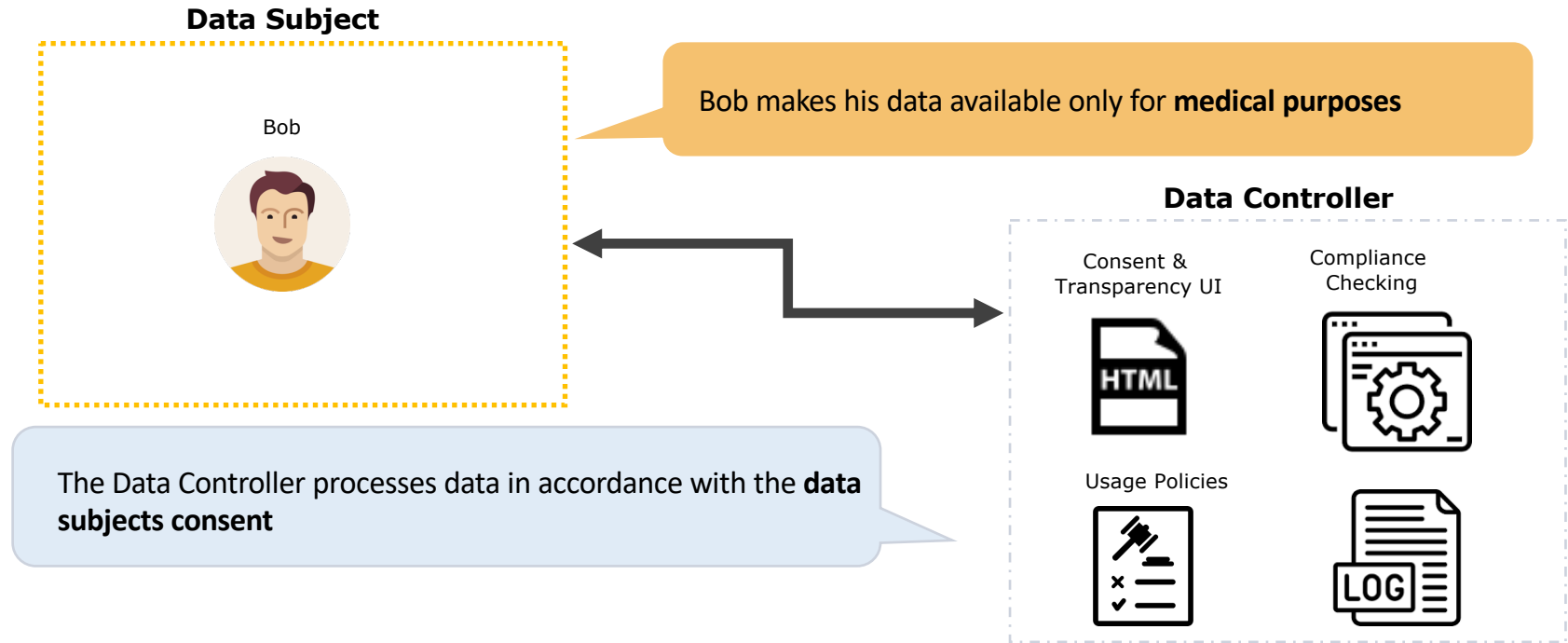
*arXiv Technical Report, CoRR,
arXiv:2203.04800, 2022*



Areas that still need attention:

- Different copies and derivations of the same data can be shared across the network
- Giving control to users (individuals and organizations) and empowering them
- Techniques that ensure continuous adherence to policies and data usage
- Assessing security and reliability

Consent as a Legal Basis for Data Processing



Bonatti, P.A., Kirrane, S., Petrova, I.M. and Sauro, L., 2020. Machine understandable policies and GDPR compliance checking. KI-Künstliche Intelligenz.

Fernández, J.D., Sabou, M., Kirrane, S., Kiesling, E., Ekaputra, F.J., Azzam, A. and Wenning, R., 2020. User consent modeling for ensuring transparency and compliance in smart cities. Personal and Ubiquitous Computing.

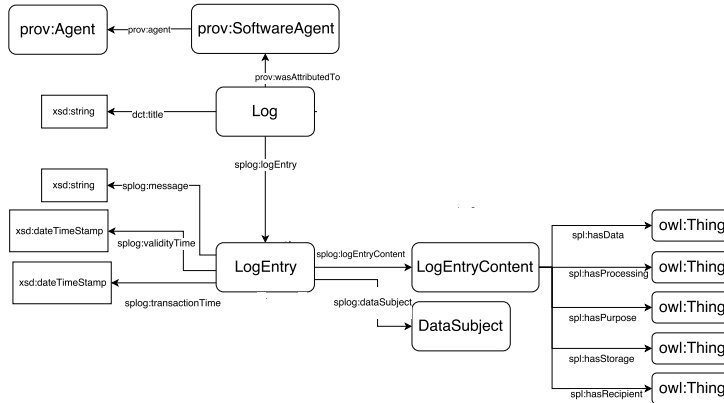
SPECIAL's Usage Policy Language Grammar

```
UsagePolicy := 'ObjectUnionOf' '(' ' BasicUsagePolicy BasicUsagePolicy { BasicUsagePolicy } ')'
              | BasicUsagePolicy
BasicUsagePolicy := 'ObjectIntersectionOf' '(' ' Data Purpose Processing Recipients Storage ')'
Data := 'ObjectSomeValueFrom' '(' 'spl:hasData' DataExpression ')'
Purpose := 'ObjectSomeValueFrom' '(' 'spl:hasPurpose' PurposeExpression ')'
Processing := 'ObjectSomeValueFrom' '(' 'spl:hasProcessing' ProcessingExpression ')'
Recipients := 'ObjectSomeValueFrom' '(' 'spl:hasRecipient' RecipientExpression ')'
Storage := 'ObjectSomeValueFrom' '(' 'spl:hasStorage' StorageExpression ')'

DataExpression := 'spl:AnyData' | DataVocabExpression
PurposeExpression := 'spl:AnyPurpose' | PurposeVocabExpression
ProcessingExpression := 'spl:AnyProcessing' | ProcessingVocabExpression
RecipientsExpression := 'spl:AnyRecipient' | 'spl:Null' | RecipientVocabExpression
StorageExpression := 'spl:AnyStorage' | 'spl:Null' |
                    'ObjectIntersectionOf' '(' ' Location Duration ')'
Location := 'ObjectSomeValueFrom' '(' 'spl:hasLocation' LocationExpression ')'
Duration := 'ObjectSomeValueFrom' '(' 'spl:hasDuration' DurationExpression ')'
           | 'DataSomeValueFrom' '(' 'spl:durationInDays' IntervalExpression ')'
```

- We propose a usage policy language that can be used to express:
 - ❖ data subject **consent**
 - ❖ data controllers **usage requests**
 - ❖ fragments of the **GDPR**
 - ❖ processing requirements as **business policies**
- We extensively **re-uses standards** based privacy-related vocabularies
- Policies are expressed using the **Web Ontology Language (OWL)**, thus we are able to **leverage existing OWL reasoners** out of the box

Consent as a Legal Basis for Data Processing

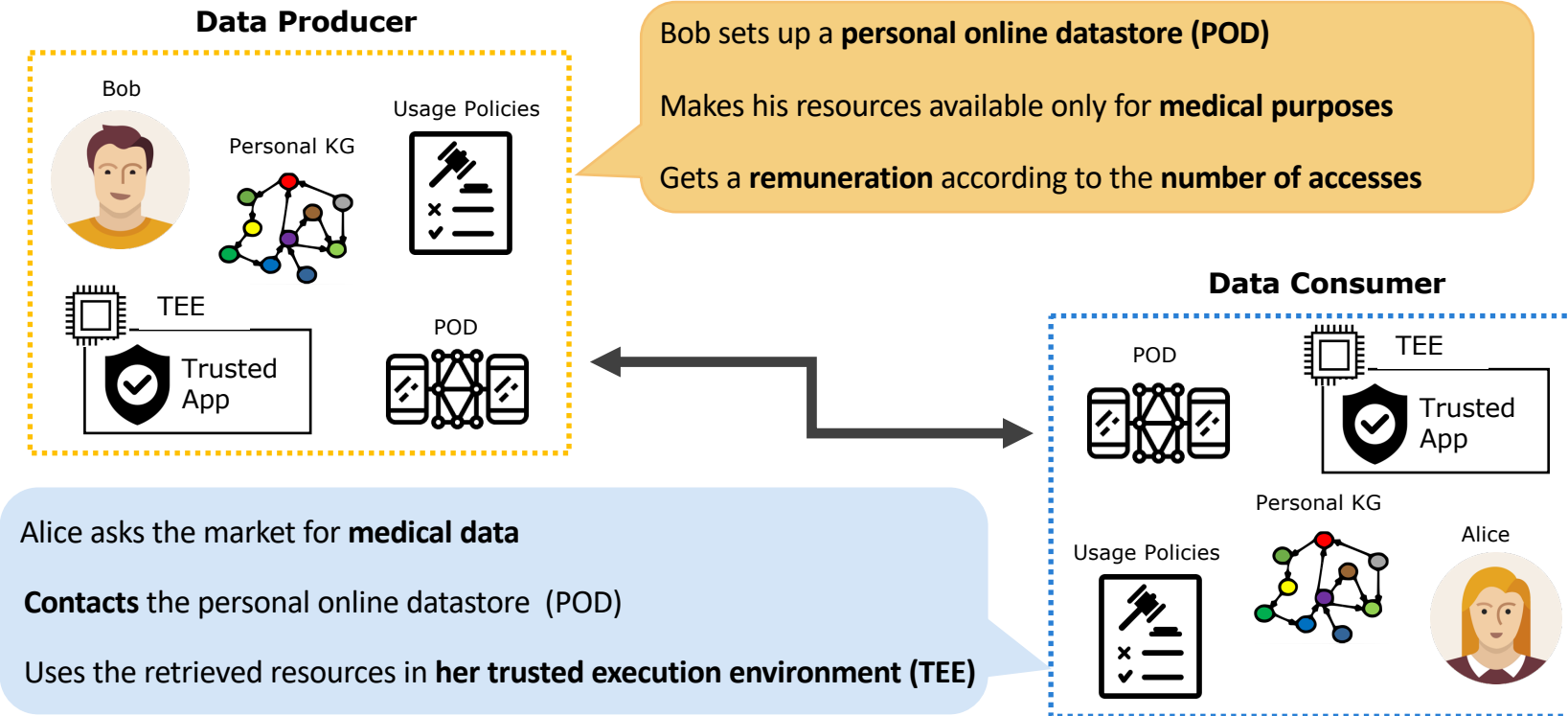


- We propose a **log vocabulary** that reuses well-known vocabularies such as **PROV** for representing provenance metadata
- Log entries are used to represent:
 - ❖ Data processing events
 - ❖ Policy events
- Optional components are provided for:
 - ❖ Immutability
 - ❖ Business process management (BPM)

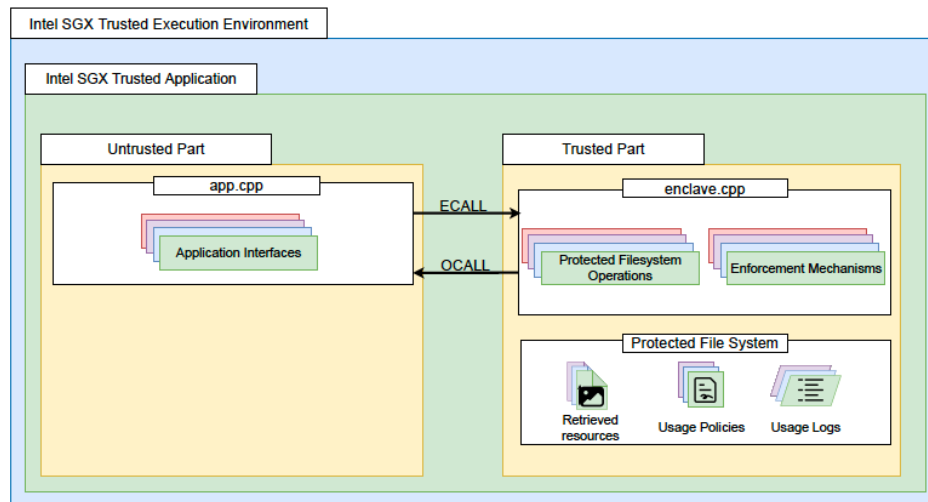
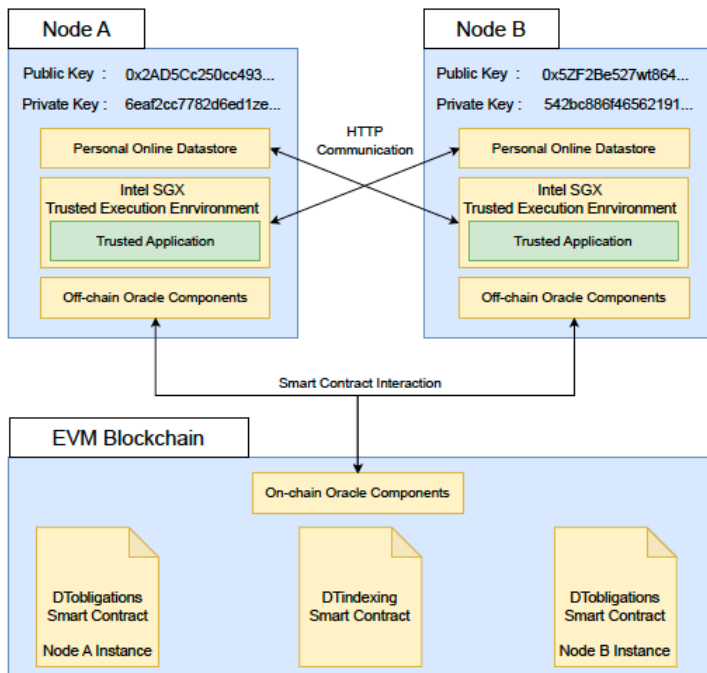
Bonatti, P.A., Kirrane, S., Petrova, I.M. and Sauro, L., 2020. Machine understandable policies and GDPR compliance checking. KI-Künstliche Intelligenz.

Fernández, J.D., Sabou, M., Kirrane, S., Kiesling, E., Ekaputra, F.J., Azzam, A. and Wenning, R., 2020. User consent modeling for ensuring transparency and compliance in smart cities. Personal and Ubiquitous Computing.

Resource Usage Governance



Resource Usage Governance



What about the data subjects?

*“Consent should be given by a clear affirmative act establishing a **freely given, specific, informed** and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement” (GDPR).*

The SPECIAL Tab Based Consent UI

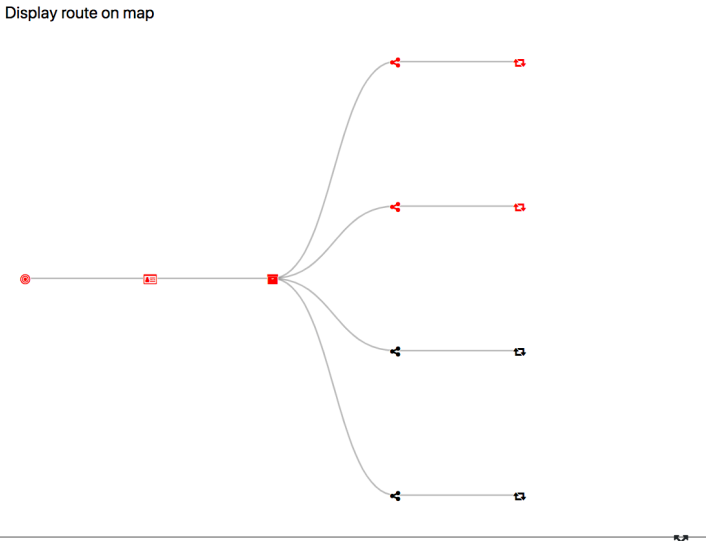
Purpose ⓘ Data ⓘ Storage ⓘ Sharing ⓘ Processing ⓘ

Purpose ⓘ ⓘ

We need to process your data to provide the following services:

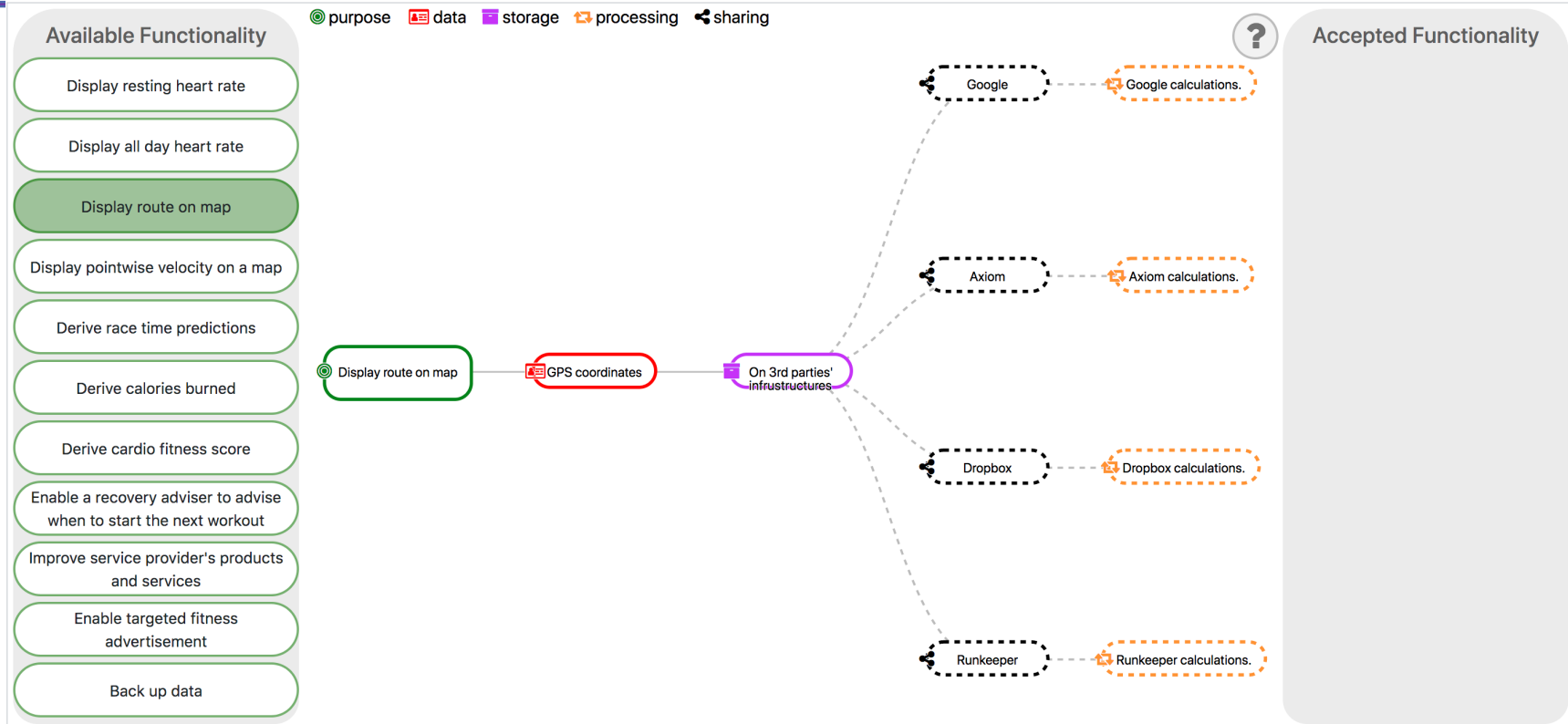
Display resting heart rate	ⓘ ⓘ ⓘ ⓘ ✓
Display all day heart rate	ⓘ ⓘ ⓘ ⓘ ✓
Display route on map	ⓘ ⓘ ⓘ ⓘ ✗
Display pointwise velocity on a map	ⓘ ⓘ ⓘ ⓘ ✗
Derive race time predictions	ⓘ ⓘ ⓘ ⓘ ✗
Derive calories burned	ⓘ ⓘ ⓘ ⓘ ✗
Derive cardio fitness score	ⓘ ⓘ ⓘ ⓘ ✗
Enable a recovery adviser to advise w...	ⓘ ⓘ ⓘ ⓘ ✗
Improve service provider's products ...	ⓘ ⓘ ⓘ ⓘ ✗
Enable targeted fitness advertisement	ⓘ ⓘ ⓘ ⓘ ✗
Back up data	ⓘ ⓘ ⓘ ⓘ ✗

Display route on map



Complete Consent Request

The SPECIAL Functionality Based Consent UI



The SPECIAL Slider Based Consent UI

Consent Request - BeFit

Please provide your preferences for data processing.

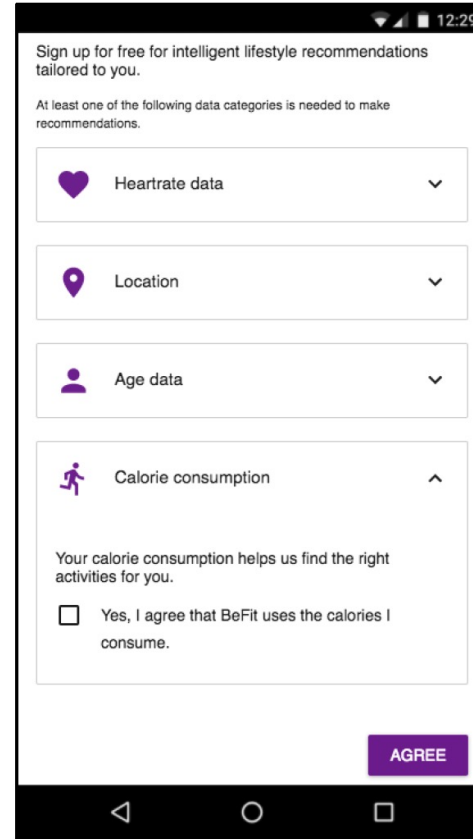
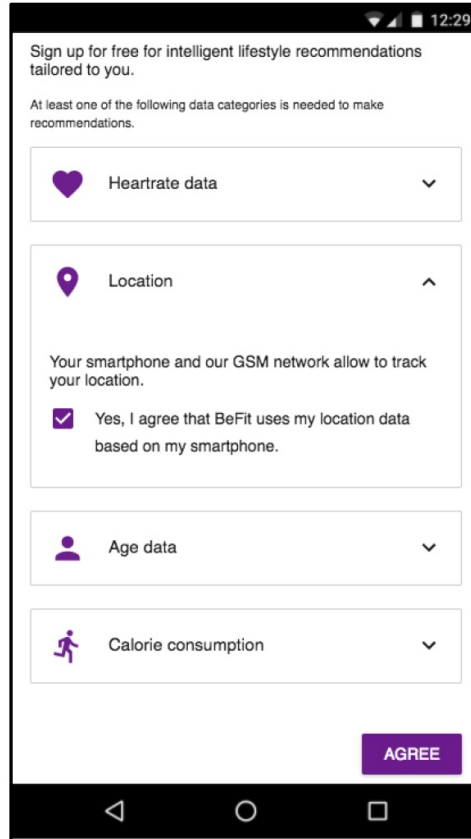


- No Functionality
- Health Data
- Map Visualization
- Fitness Adviser
- Back - Up
- Marketing & BI

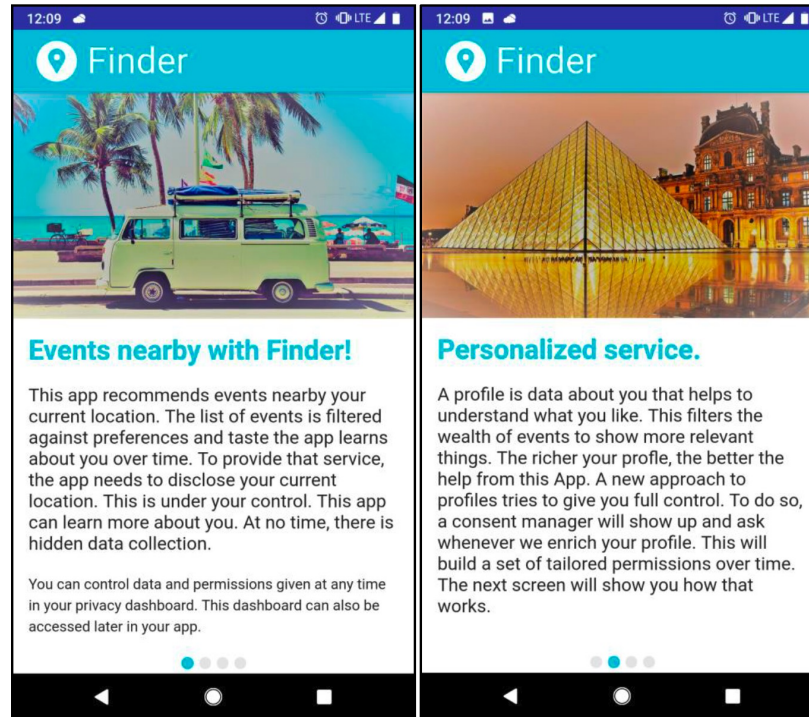
- Display resting heart rate
- Display all day heart rate
- Derive calories burned
- Derive cardio fitness score
- Display route on map
- Display pointwise velocity on a map
- Derive race time predictions
- Enable a recovery adviser to advise when to start the next workout
- Back up data
- Improve service provider's products and services
- Enable targeted fitness advertisement

SUBMIT PREFERENCES

The SPECIAL Mobile Consent UI



The SPECIAL Dynamic Consent UI



The SPECIAL Dashboard V1

Privacy dashboard



Processing context

- Data I provided
- Data of me provided by others
- Data of my behavior
- Inferred data about me

Data type

- Text
- Image
- Audio
- Video
- Location

Time range

1970-01-01

2017-11-01



Tue Aug 01 2017
You disclosed your first name to the controller.

Jonathan



Tue Aug 01 2017
You disclosed your last name to the controller.

Doe



Tue Aug 01 2017
You disclosed your email address to the controller.

jonathan.doe@example.com



Tue Aug 01 2017
You have been observed browsing this website.

/pellentesque/ultrices/mattis/odio/donec.jsp



Tue Aug 01 2017
You have been observed browsing this website.

/ac/heque/duis/bibendum/morbi.png



Tue Aug 01 2017
You have been observed browsing this website.

/parturient.jpg

Logo:



Name:

Technical University of Berlin

Address:

Ernst-Reuter-Platz 7 10587 Berlin

Email address:

privacy@tu-berlin.de

Privacy policy:

[Privacy policy](#)

Review consent:

[Review consent](#)

The SPECIAL Dashboard V2

Processing context

- Data I provided
- Data of me provided by others
- Data of my behavior
- Inferred data about me

Data type

- Text
- Image
- Audio
- Video
- Location

Time range

1970-01-01

2017-11-01

Data processed on Tue Aug 01 2017

Processed data categories:

- Data I provided
- Data of my behavior

Data processed on Wed Aug 02 2017

Processed data categories:

- Data of my behavior
- Inferred data about me

Data processed on Thu Aug 03 2017

Processed data categories:


- Data of my behavior

Data processed on Fri Aug 04 2017

Processed data categories:

- Data of my behavior

Logo:




Name:

Technical University of Berlin


Address:

Ernst-Reuter-Platz 7 10587 Berlin


Email address:

 privacy@tu-berlin.de

Privacy policy:

 [Privacy policy](#)

Review consent:

 [Review consent](#)

The SPECIAL Dashboard V3

SPECIAL Privacy Dashboard



Name: SPECIAL

Address: Rue Robert Stumper, 2350 Luxembourg, Luxembourg

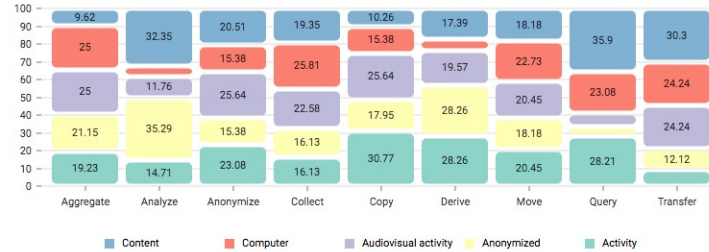
Description:

The SPECIAL (Scalable Policy-aware Linked Data Architecture For Privacy, Transparency and Compliance) project is a Research and Innovation Action funded under the H2020-ICT-2016-1 Big Data PPP call (Privacy-preserving Big Data technologies, ICT-18-2016). The project started on the 1st of January 2017 and will continue for three years.

Website: <https://www.specialprivacy.eu/>

Email address: privacy@specialprivacy.eu

What kind of processing took place? Which data was used?



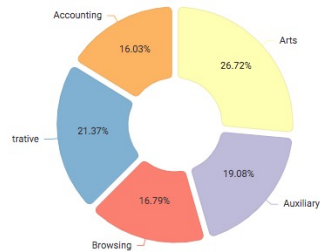
GENERAL INFORMATION

TIMELINE

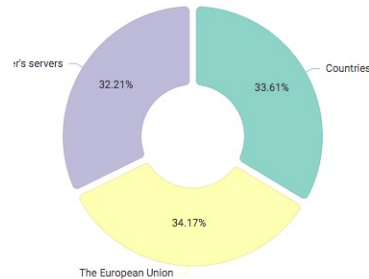
POLICIES

What data is processed and for what purposes?

Data category	%
Activity data	24.43%
Audiovisual activity data	24.43%
Computer data	21.37%
Content data	17.56%
Anonymized data	12.21%



Where is data stored? With whom was it shared?



Data recipients	%
The controller, legal entities that act a...	18.49%
Legal entities following the controller's...	17.65%
Legal entities following different practi...	16.25%
Unrelated third parties	16.25%
Public fora	15.69%

What has been happening more broadly?

SWJ Special Issue: Data and Algorithmic Governance

Consent Through the Lens of Semantics: State of the Art Survey and Best Practices

Anelia Kurteva^{a,*}, Tek Raj Chhetri^a, Harshvardhan J. Pandit^b, and Anna Fensel^a

^a *Semantic Technology Institute (STI) Innsbruck, Department of Computer Science, University of Innsbruck, Innsbruck, Austria*

^b *ADAPT Centre, School of Computer Science and Statistics Trinity College Dublin, Dublin, Ireland*
E-mails: anelia.kurteva@sti2.at, tekraj.chhetri@sti2.at, pandith@tcd.ie, anna.fensel@sti2.at

Analysis of Ontologies and Policy Languages to Represent Information Flows in GDPR

Beatriz Esteves^{a,*}, Víctor Rodríguez-Doncel^a

^a *Ontology Engineering Group, Universidad Politécnica de Madrid, Spain*
E-mail: beatriz.gesteves@upm.es

Semantic-enabled Architecture for Auditable Privacy-Preserving Data Analysis

Fajar J. Ekaputra^{a,*}, Andreas Ekelhart^b, Rudolf Mayer^{b,a}, Tomasz Miksa^{b,a}, Tanja Šarčević^b,
Sotirios Tsepelakis^b, and Laura Waltersdorfer^a

^a *Information and Software Engineering Research Group, TU Wien, Vienna, Austria*
E-mails: fajar.ekaputra@tuwien.ac.at, laura.waltersdorfer@tuwien.ac.at

^b *SBA Research, Vienna, Austria*
E-mails: rmayer@sba-research.org, tmiksa@sba-research.org, tsarcevic@sba-research.org,
ssepelakis@sba-research.org

Differential Privacy and SPARQL¹

Carlos Buil-Aranda^a, Jorge Lobo^b and Federico Olmedo^c

^a *Departamento de Informática, Universidad Técnica Federico Santa María and IMFD Chile Avda España 1680, Valparaíso Chile*

E-mail: cbuil@inf.ufsm.cl

^b *ICREA and Universitat Pompeu Fabra, c/Roc Boronat 148, Barcelona, Spain*

E-mail: jorge.lopez@upf.edu

^c *Departamento de Ciencias de la Computación, Universidad de Chile and IMFD, Beauchef 851, Santiago, Chile*
E-mail: folmedo@dcc.uchile.cl

SWJ Special Issue: Knowledge Graphs Validation & Quality

Instance Level Analysis on Linked Open Data Connectivity for Cultural Heritage Entity Linking and Data Integration

Go Sugimoto*

*Austrian Centre for Digital Humanities and Cultural Heritage, Sonnenfelsgasse 19, 1010, Vienna, Austria
Donau University Krems, Dr.-Karl-Dorrek-Straße 30, 3500 Krems, Austria
Vrije Universiteit Amsterdam, De Boelelaan 1081, NU Building, 1081 HV, Amsterdam, The Netherlands

Learning SHACL Shapes from Knowledge Graphs

Pouya Ghiasnezhad Omran^{a,*}, Kerry Taylor^a, Sergio Rodríguez Méndez^a, and Armin Haller^a

^a School of Computing, The Australian National University, ACT, Australia

E-mails: P.G.Omran@anu.edu.au, Kerry.Taylor@anu.edu.au, Sergio.RodriguezMendez@anu.edu.au, Armin.Haller@anu.edu.au

The OneGraph Vision: Challenges of Breaking the Graph Model Lock-In*

Ora Lassila^{a,**}, Michael Schmidt^a, Olaf Hartig^{a,b}, Brad Bebee^a, Dave Bechberger^a, Willem Broekema^a, Ankesh Khandelwal^a, Kelvin Lawrence^a, Carlos Manuel Lopez Enriquez^a, Ronak Sharda^a and Bryan Thompson^a

^a Amazon Neptune Team, Amazon Web Services, Seattle, WA, USA

^b Dept. of Computer and Information Science (IDA), Linköping University, Sweden

An Assertion and Alignment Correction Framework for Large Scale Knowledge Bases

Jiaoyan Chen^a, Ernesto Jiménez-Ruiz^{b,d}, Ian Horrocks^a, Xi Chen^c and Erik Bryhn Myklebust^{d,e}

^a Department of Computer Science, University of Oxford, Oxford, UK

E-mails: jiaoyan.chen@cs.ox.ac.uk, ian.horrocks@cs.ox.ac.uk

^b City, University of London, London, UK

E-mail: Ernesto.Jimenez-Ruiz@city.ac.uk

^c Jarvis Lab Tencent, Shenzhen, China

E-mail: ian.horrocks@cs.ox.ac.uk

^d Centre for Scalable Data Access (SIRIUS), University of Oslo, Oslo, Norway

E-mail: jasonxchen@tencent.com

^e Norwegian Institute for Water Research, Oslo, Norway

E-mail: erik.bmyklebust@niva.no

Using the W3C *Generating RDF from Tabular Data on the Web* Recommendation to manage small Wikidata datasets

Steven J. Baskauf^{a,*} and Jessica K. Baskauf^b

^a Jean and Alexander Heard Libraries, Vanderbilt University, Nashville, Tennessee, USA

E-mail: steve.baskauf@vanderbilt.edu, <https://orcid.org/0000-0003-4365-3135>

^b Carleton College, Northfield, Minnesota, USA¹

<https://orcid.org/0000-0002-1772-1045>

Components.js: Semantic Dependency Injection

Ruben Taelman¹, Joachim Van Herwegen¹, Miel Vander Sande² and Ruben Verborgh¹

¹ IDLab, Department of Electronics and Information Systems, Ghent University – imec

E-mail: ruben.taelman@ugent.be

² meemoo, Flemish Institute for Archives

Trusting Decentralised Knowledge Graphs and Web Data

“

Trusting Decentralised Knowledge Graphs
and Web Data (TrusDeKW)

#KnowledgeGraph #Decentralisation #Trust

**Juan Cano, John Domingue, Sabrina Kirrane, Philipp D. Rohde,
Aisling Third and Ruben Taelman**

Universidad Politécnica de Madrid, Spain; The Open University, UK; Vienna University of
Economics and Business, Austria; TIB Leibniz Information Centre for Science and
Technology and Leibniz University Hannover, Germany; and Ghent University, Belgium

WORKSHOP



ESWC23

May 28 - June 1, 2023
Hersonissos, Greece

14th Workshop on Ontology Design and Patterns (WOP 2023)

Colocated with the 22nd International Semantic Web Conference (ISWC 2023)
November 6-10, 2023. Athens, Greece.

The WOP workshop series covers issues related to quality in ontology design and ontology design patterns (ODPs) for data and knowledge engineering in Semantic Web.

MEPDaW'23 - Managing the Evolution and Preservation of the Data Web

9th MEPDaW Workshop at ISWC'23, November 6th (afternoon), 2023

More specifically, these solutions are expected to tackle major issues such as the synchronisation problem (monitoring changes), the curation problem (repairing data imperfections), the appraisal problem (assessing the quality of a dataset), the citation problem (how to cite a particular version of a dataset), the archiving problem (retrieving a specific version of a dataset), and the sustainability problem (preserving at scale, ensuring long-term access).

VOILA! 2023

8th International Workshop on Visualization and Interaction for Ontologies, Linked Data and Knowledge Graphs, co-located with [ISWC 2023](#), November 6, 2023, Athens, Greece

Ultimately, providing better user interfaces, visual representations and interaction techniques will foster user engagement and likely lead to higher quality results in different applications employing semantics, and proliferate the consumption of Ontologies, Linked Data and Knowledge Graphs.

*Let's take a quick look at some other EU directives
and regulations!*

The General Data Protection Regulation (came into force 2018)

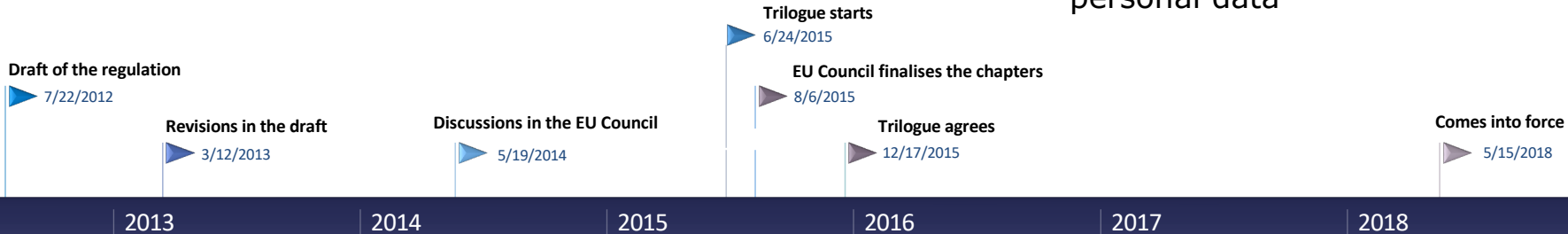
In the context of the European Union's ordinary legislative procedure, a trilogue is an informal interinstitutional negotiation bringing together representatives of the European Parliament, the Council of the European Union and the European Commission.

The screenshot shows the EUR-Lex website interface. At the top, there are navigation links like 'About EUR-Lex', 'Site map', 'A-Z', 'FAQ', 'Help', 'Links', and 'Legal notice'. Below that is a search bar with the text 'Quick search: insert free text, CELEX number or descriptor'. The main content area displays the document '32016R0679' under the heading 'EU law and publications'. It includes a 'Document information' tab and a 'Summary of legislation' section. The title and reference are 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)'. It also shows the date 'In force' as 'OJ L 119, 4.5.2016, p. 1-88' and the EUI URL: 'http://data.europa.eu/eli/reg/2016/679/oj'. At the bottom, there are options for different languages and formats (HTML, PDF, Official Journal).

<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>

Objectives:

- Protect individuals' fundamental rights and freedoms, particularly their right to protection of their personal data
- Homogeneous protection of personal data across the EU Member States
- Increased accountability.
- A simplified and lighter legal framework on the processing of personal data



Copyright in the Digital Single Market (came into force 2021)

Document 32019L0790

? 📄 ↻ Share

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.)

PE/51/2019/REV/1

OJ L 130, 17.5.2019, p. 92–125 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

🟢 In force

ELI: <http://data.europa.eu/eli/dir/2019/790/oj>

⌵ Expand all ⏴ Collapse all

⌵ Languages, formats and link to OJ

	BG	ES	CS	DA	DE	ET	EL	EN	FR	GA	HR	IT	LV	LT	HU	MT	NL	PL	PT	RO	SK	SL	FI	SV
HTML																								
PDF																								
Official Journal																								

<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32019L0790>

Objectives:

- Protects creativity in the digital age, bringing concrete benefits to citizens, the creative sectors, the press, researchers, educators and cultural heritage institutions across the EU
- Ensure that creators are fairly remunerated in the digital space
- Protecting freedom of expression, a core value in our democracies.

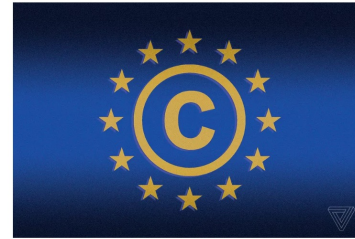
VIDEO 📄 📄 📄 📄

Europe's controversial overhaul of online copyright receives final approval

The much-criticized 'upload filter' and 'link tax' will soon become law in EU nations

By James Vincent | Mar 28, 2019, 8:00am EDT

f 📄 SHARE



Graphics by Mitchell Coating / The Verge

The European Parliament has given final approval to the Copyright Directive, a controversial package of legislation designed to update copyright law in Europe for the internet age.

Members of parliament voted 348 in favor of the law and 274 against. A last-minute proposal to remove the law's most controversial clause — known as Article 13 or the 'upload filter' — was narrowly rejected by just five votes. The directive will now be passed on to EU member states, who will have 24 months to translate it into national law.

<https://www.theverge.com/2019/3/26/18280726/europe-copyright-directive>

Advocates of the directive say it will balance the playing field between American tech giants and European content creators, giving copyright holders power over how internet platforms distribute their content. But critics say the law is vague and poorly thought-out, and will end up restricting how content is shared online, stifling innovation and free speech.

The EU Data Governance Act (came into force Sept 2023)



Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance)

PE/85/2021/REV/1

OJ L 152, 3.6.2022, p. 1–44 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

● In force

ELI: <http://data.europa.eu/eli/reg/2022/868/oj>

▼ Expand all ▲ Collapse all

▼ Languages, formats and link to OJ	
	BG ES CS DA DE ET EL EN FR GA HR IT LV LT HU MT NL PL PT RO SK SL FI SV
HTML	BG ES CS DA DE ET EL EN FR GA HR IT LV LT HU MT NL PL PT RO SK SL FI SV
PDF	BG ES CS DA DE ET EL EN FR GA HR IT LV LT HU MT NL PL PT RO SK SL FI SV
Official Journal	BG ES CS DA DE ET EL EN FR GA HR IT LV LT HU MT NL PL PT RO SK SL FI SV

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868>

European Data Governance Act

A European Data Governance Act, which is fully in line with EU values and principles, will bring significant benefits to EU citizens and companies.

A key pillar of the [European strategy for data](#), the [Data Governance Act](#) seeks to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical obstacles to the reuse of data.

The Data Governance Act will also support the set-up and development of common European data spaces in strategic domains, involving both private and public players, in sectors such as health, environment, energy, agriculture, mobility, finance, manufacturing, public administration and skills.

The Data Governance Act entered into force on 23 June 2022 and, following a 15-month grace period, will be applicable from September 2023.

<https://digital-strategy.ec.europa.eu/en/policies/data-governance-act>

Objectives:

- Increase trust in data sharing
- Strengthen mechanisms to increase data availability
- Overcome technical obstacles to the reuse of data
- Support the set-up and development of common European data spaces involving both private and public players
- Sectors: health, environment, energy, agriculture, mobility, finance, manufacturing, public administration and skills

The EU Data Governance Act (came into force Sept 2023)

How will this work in practice?

The EU will boost the development of trustworthy data-sharing systems through 4 broad sets of measures:

1. Mechanisms to facilitate the reuse of certain public sector data that cannot be made available as open data. For example, the reuse of health data could advance research to find cures for rare or chronic diseases.
2. Measures to ensure that data intermediaries will function as trustworthy organisers of data sharing or pooling within the common European data spaces.
3. Measures to make it easier for citizens and businesses to make their data available for the benefit of society.
4. Measures to facilitate data sharing, in particular to make it possible for data to be used across sectors and borders, and to enable the right data to be found for the right purpose.

The EU Data Act (Came into force Jan 2024)



Data Act

The Data Act is a key measure for making more data available for use in line with EU rules and values.

The proposed Regulation on harmonised rules on fair access to and use of data — also known as the Data Act — was adopted by the Commission on 23 February 2022. [The Data Act](#) is a key pillar of the European strategy for data. It will make an important contribution to the digital transformation objective of the Digital Decade.

The new measures complement the Data Governance Regulation proposed in November 2020, the first deliverable of the European strategy for data. While the Data Governance Regulation creates the processes and structures to facilitate data, the Data Act clarifies who can create value from data and under which conditions.

The Data Act will ensure fairness by setting up rules regarding the use of data generated by Internet of Things (IoT) devices.

<https://digital-strategy.ec.europa.eu/en/policies/data-act>

Document 52022PC0068

? 🖨️ Share

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act)

COM/2022/68 final

Expand all Collapse all

Languages and formats available

	BG	ES	CS	DA	DE	ET	EL	EN	FR	GA	HR	IT	LV	LT	HU	MT	NL	PL	PT	RO	SK	SL	FI	SV
HTML																								
DOC																								
PDF																								

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN>

Objectives:

- Establish clear and fair rules for accessing and using data within the European data economy
- Empower users (businesses or consumers) to easily and securely access, use and share the generated data.

The EU Data Act (Came into force Jan 2024)

How will this work in practice?

The Data Act will make more data available for the benefit of companies, citizens and public administrations through a set of measures such as:

- Measures to **increase legal certainty** for companies and consumers who generate data on who can use what such data and under which conditions, and incentives for manufacturers to continue investing in high-quality data generation. These measures will make it easier to transfer data between service providers and will encourage more actors, regardless of their size, to participate in the data economy.
- Measures to **prevent abuse of contractual imbalances** that hinder fair data sharing. SMEs will be protected against unfair contractual terms imposed by a party enjoying a significantly stronger market position. The Commission will also develop model contract clauses in order to help such market participants draft and negotiate fair data-sharing contracts.
- Means for **public sector bodies to access and use data** held by the private sector that is necessary for specific public interest purposes. For instance, to develop insights to respond quickly and securely to a public emergency, while minimising the burden on businesses.
- New rules setting the right framework conditions for customers to effectively switch between different providers of data-processing services to unlock the EU cloud market. These will also contribute to an overall framework for efficient data interoperability.

The EU Artificial Intelligence Act (Text will be finalised Q1 2024)

A European approach to artificial intelligence

The EU's approach to artificial intelligence centers on excellence and trust, aiming to boost research and industrial capacity while ensuring safety and fundamental rights.

The way we approach Artificial Intelligence (AI) will define the world we live in the future. To help building a resilient [Europe for the Digital Decade](#), people and businesses should be able to enjoy the benefits of AI while feeling safe and protected.

The [European AI Strategy](#) aims at making the EU a world-class hub for AI and ensuring that AI is human-centric and trustworthy. Such an objective translates into the [European approach to excellence and trust](#) through concrete rules and actions.

In April 2021, the Commission presented its AI package, including:

- its [Communication on fostering a European approach to AI](#);
- a [review of the Coordinated Plan on Artificial Intelligence](#) (with EU Member States);
- its [Regulatory framework proposal on artificial intelligence](#) and [relevant Impact assessment](#).

In January 2024, the Commission adopted the [AI@EC Communication](#), outlining strategies for improving the Commission's own capabilities in the field of Artificial Intelligence (AI) while emphasizing the importance of safe, transparent, and human-centered use of AI technologies. The guidance (included in the Communication), encourages the Commission to internally adapt, innovate, and adopt AI early on to set an example of best practices.

<https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>

Document 52021PC0206



Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

COM/2021/206 final

Expand all Collapse all

▼ Languages and formats available

	BG	ES	CS	DA	DE	ET	EL	EN	FR	GA	HR	IT	LV	LT	HU	MT	NL	PL	PT	RO	SK	SL	FI	SV
HTML																								
DOC																								
PDF																								

▼ Multilingual display

English (en) Please choose Please choose **Display**

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>

Objectives:

- Boost research and industrial capacity while ensuring safety and fundamental rights
- Ensuring that AI is human-centric and trustworthy

The EU Artificial Intelligence Act (Text will be finalised Q1 2024)

A European approach to artificial intelligence

The EU's approach to artificial intelligence centers on excellence and trust, aiming to boost research and industrial capacity while ensuring safety and fundamental rights.

The way we approach Artificial Intelligence (AI) will define the world we live in the future. To help building a resilient [Europe for the Digital Decade](#), people and businesses should be able to enjoy the benefits of AI while feeling safe and protected.

The [European AI Strategy](#) aims at making the EU a world-class hub for AI and ensuring that AI is human-centric and trustworthy. Such an objective translates into the [European approach to excellence and trust](#) through concrete rules and actions.

In April 2021, the Commission presented its AI package, including:

- its [Communication on fostering a European approach to AI](#);
- a [review of the Coordinated Plan on Artificial Intelligence](#) (with EU Member States);
- its [Regulatory framework proposal on artificial intelligence](#) and [relevant Impact assessment](#).

In January 2024, the Commission adopted the [AI@EC Communication](#), outlining strategies for improving the Commission's own capabilities in the field of Artificial Intelligence (AI) while emphasizing the importance of safe, transparent, and human-centered use of AI technologies. The guidance (included in the Communication), encourages the Commission to internally adapt, innovate, and adopt AI early on to set an example of best practices.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

2021/0106(COD)
DRAFT [Final draft as updated on 21/01/
21-01-2024 at 17h11]

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Formula				
1	2021/0106 (COD)	2021/0106 (COD)	2021/0106 (COD)	2021/0106 (COD) <small>Text Origin: Commission Proposal</small>
Proposal Title				
2	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS <small>Text Origin: Commission Proposal</small>
Formula				
3	THE EUROPEAN PARLIAMENT	THE EUROPEAN PARLIAMENT	THE EUROPEAN PARLIAMENT	THE EUROPEAN PARLIAMENT

<https://artificialintelligenceact.eu/wp-content/uploads/2024/01/AIA-Final-Draft-21-January-2024.pdf>

The EU Artificial Intelligence Act (Text will be finalised Q1 2024)

Appears to be moved from the annexes to the recitals

ANNEX I ARTIFICIAL INTELLIGENCE TECHNIQUES AND APPROACHES referred to in Article 3, point 1

- (a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
- (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;
- (c) Statistical approaches, Bayesian estimation, search and optimization methods.

The EU Artificial Intelligence Act (2024)

Reasons for and objectives of the proposal

- Bring a wide array of **economic and societal benefits** across the entire spectrum of industries and social activities.
- **AI can also bring about new risks or negative consequences** for individuals or the society.
- **Twin objective of promoting the uptake of AI and of addressing the risks** associated with certain uses of such technology.
- Rules for AI available in the Union market or otherwise affecting people in the Union should therefore be **human centric**.
- It supports the **objective of the Union being a global leader** in the development of secure, trustworthy and ethical artificial intelligence.

The EU Artificial Intelligence Act (2024)

Proportionality

- The regulation follows a **risk-based approach**, differentiating between
 - (i) an unacceptable risk
 - (ii) a high risk
 - (iii) low or minimal risk
- For non-high-risk AI systems, only **very limited transparency obligations are imposed**, for example in terms of the provision of information to flag the use of an AI system when interacting with humans.
- For high-risk AI systems, the **requirements of high-quality data, documentation and traceability, transparency, human oversight, accuracy and robustness**, are strictly necessary to mitigate the risks to fundamental rights and safety posed by AI

- All those AI systems whose use is considered unacceptable as contravening Union values, for instance by **violating fundamental rights**.
- The prohibitions covers practices that have a significant potential to **manipulate persons through subliminal techniques** beyond their consciousness;
- Or **exploit vulnerabilities of specific vulnerable groups** such as children or persons with disabilities in order to materially distort their behaviour in a manner that is likely to cause them or another person psychological or physical harm.
- The proposal also prohibits **AI-based social scoring** for general purposes done by public authorities.
- The use of **‘real time’ remote biometric identification systems** in publicly accessible spaces for the purpose of law enforcement is also prohibited unless certain limited exceptions apply.

ANNEX III **HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)**

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:

1. Biometric identification and categorisation of natural persons:
 - (a) AI systems intended to be used for the ‘real-time’ and ‘post’ remote biometric identification of natural persons;
2. Management and operation of critical infrastructure:
 - (a) AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity.
3. Education and vocational training:
 - (a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions;
 - (b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions.

Artificial Intelligence Legislation

High Risk AI

4. Employment, workers management and access to self-employment:
 - (a) AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;
 - (b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships.
5. Access to and enjoyment of essential private services and public services and benefits:
 - (a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services;
 - (b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems put into service by small scale providers for their own use;
 - (c) AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid.

Artificial Intelligence Legislation

High Risk AI

4. Employment, workers management and access to self-employment:
 - (a) AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;
 - (b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships.
5. Access to and enjoyment of essential private services and public services and benefits:
 - (a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services;
 - (b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems put into service by small scale providers for their own use;
 - (c) AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid.

6. Law enforcement:
 - (a) AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences;
 - (b) AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person;
 - (c) AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in article 52(3);
 - (d) AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences;
 - (e) AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups;
 - (f) AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences;
 - (g) AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.

7. Migration, asylum and border control management:
 - (a) AI systems intended to be used by competent public authorities as polygraphs and similar tools or to detect the emotional state of a natural person;
 - (b) AI systems intended to be used by competent public authorities to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;
 - (c) AI systems intended to be used by competent public authorities for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features;
 - (d) AI systems intended to assist competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.

8. Administration of justice and democratic processes:
 - (a) AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts.

The EU Artificial Intelligence Act (2024)

Governance

- Legal requirements for high-risk AI systems in relation to data and data governance, **documentation and recording keeping, transparency and provision of information to users, human oversight, robustness, accuracy and security**.
- The precise technical solutions to achieve compliance with those requirements may be provided by **standards or by other technical specifications**
- A comprehensive **ex-ante conformity assessment** through internal checks, combined with a strong **ex-post enforcement**
- The setup of an **EU database that will be managed by the Commission** to increase public transparency and oversight
- The **establishment of a European Artificial Intelligence Board** composed of representatives from the Member States and the Commission.

Looking to the Future!

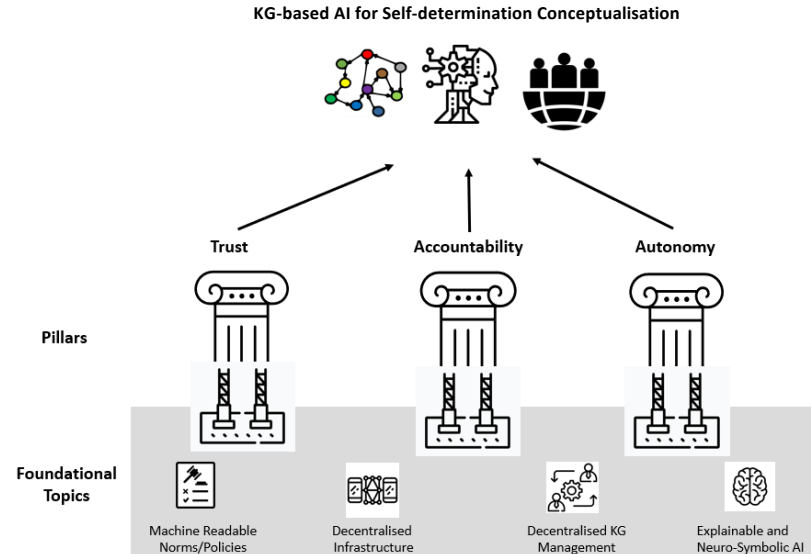
KG-based AI for Self-Determination



KG-based AI for Self-Determination

The Vision

- The three pillar research topics - trust, accountability, and autonomy - represent the **desired goals for how AI can benefit society and facilitate self-determination**
- The pillars combine **fundamental principles of the proposed EU AI Act and self-determination theory**.
- The pillars are supported via four foundational research topics that represent the **tools and techniques needed to support the three research pillars**:
 - machine-readable norms and policies
 - decentralised infrastructure
 - decentralised KG management
 - explainable and neuro-symbolic AI



KG-based AI for Self-Determination

The Pillars

Trust

- Machine-readable policies must **faithfully represent** human policies and norms
- **Enforcement** and **compliance** checking:
 - ❖ (semi-)automated techniques
 - ❖ auditing and tracing
 - ❖ trusted execution environments
 - ❖ certification mechanisms

Accountability

- Detecting if any party **violated** policies and norms
- Facilitating learning **transparency**
- Providing **explanations** for recommendations and decisions
- Integrating, querying, and aggregating knowledge from **disparate sources**

Autonomy

- **Controlling** who has access to our personal data
- **Negotiating** terms of use
- Fostering collaboration via **aggregation and strong privacy** guarantees (e.g., anonymisation)
- **Continuous monitoring** via auditing, tracing, and certification
- **Self-sovereign identities**

Opportunities and Challenges

- We need to put more emphasis on tech transfer and develop best practices for software engineers and architects
- Performance, scalability, and usability need to be assessed in practical real world settings
- There is no standard general purpose policy language capable of representing various policies, norms, and preferences
- Machine-readable policies must faithfully represent human policies and norms
- Technical usage control is difficult, which means we often need to rely on legal agreements
- We need to get into the practice of defining attacker models for privacy and security use case scenarios
- EU research is greatly influenced by regulations and directives - this can be both a help and a hinderance

Thank you / contact details



VIENNA UNIVERSITY OF
ECONOMICS AND BUSINESS

Department of Information Systems & Operations

Institute for Information Systems & New Media
Welthandelsplatz 1, 1020 Vienna, Austria

Dr. Sabrina Kirrane

T +43-1-313 36-4494
F +43-1-313 36-90 4494
sabrina.kirrane@wu.ac.at
www.wu.ac.at
www.sabrinakirrane.com
[@SabrinaKirrane](#)

