Data and Algorithmic Governance: A Community Perspective

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

Sabrina Kirrane, 12th of June 2024

International Semantic Web Research Summer School (ISWS)

An Irish Perspective

Murphy's Law

My Previous Call to Action

The General Data Protection Regulation (2016)

European Commission

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 **transparency** and **accountability**.

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)

OJ L 119, 4.5.2016, p. 1–88 (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: This act has been changed. Current consolidated version: 04/05/2016

ELI: http://data.europa.eu/eli/reg/2016/679/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	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML
PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF	PDF
Official Journal	OJ	OJ	OJ	OJ	OJ	OJ	OJ	OJ	OJ	OJ	OJ	OJ	OJ	OJ	OJ	OJ	OJ	OJ	OJ	OJ	OJ	OJ	OJ	OJ

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

Privacy
A community perspective

KI - Künstliche Intelligenz (2020) 34:303–315
https://doi.org/10.1007/s13218-020-00677-4

TECHNICAL CONTRIBUTION

Check for updates

Machine Understandable Policies and GDPR Compliance Checking

Piero A. Bonatti[1] · Sabrina Kirrane[2] · Iliana M. Petrova[1] · Luigi Sauro[1]

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, stsepelakis@sba-research.org

Differential Privacy and SPARQL[1]

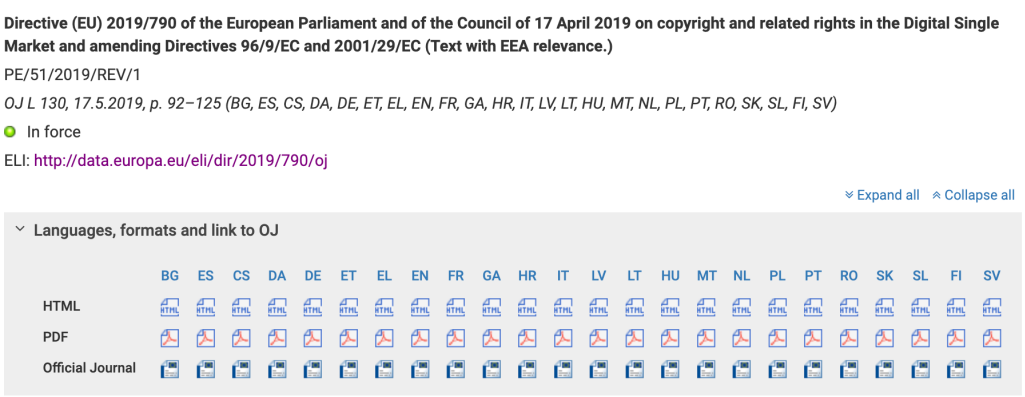
Carlos Buil-Aranda [a], Jorge Lobo [b] and Federico Olmedo [c]
[a] *Departamento de Informática, Universidad Técnica Federico Santa María and IMFD Chile Avda España 1680, Valparaíso Chile*
E-mail: cbuil@inf.utfsm.cl
[b] *ICREA and Universitat Pompeu Fabra, c/Roc Boronat 148, Barcelona, Spain*
E-mail: jorge.lobo@upf.edu
[c] *Departamento de Ciencias de la Computación, Universidad de Chile and IMFD, Beauchef 851, Santiago, Chile*
E-mail: folmedo@dcc.uchile.cl

Directive on Copyright in the Digital Single Market (2019)

European Commission

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.



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	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML
PDF																								
Official Journal																								

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0790&qid=1718022850003

Copyright
A community perspective

2018 | OriginalPaper | Chapter

14. Automated Rights Clearance Using Semantic Web Technologies: The DALICC Framework

Authors : Tassilo Pellegrini, Victor Mireles, Simon Steyskal, Oleksandra Panasiuk, Anna Fensel, Sabrina Kirrane

Published in: Semantic Applications

Publisher: Springer Berlin Heidelberg

PUBLISHED IN:

Modelling the Compatibility of Licenses

Benjamin Moreau[1,2], Patricia Serrano-Alvarado[1], Matthieu Perrin[1], and Emmanuel Desmontils[1]

[1] Nantes University, LS2N, CNRS, UMR6004, 44000 Nantes, France
{Name.LastName@}univ-nantes.fr
[2] OpenDataSoft {Name.Lastname}@opendatasoft.com

These Are Your Rights

A Natural Language Processing Approach to Automated RDF Licenses Generation

Elena Cabrio[1,2], Alessio Palmero Aprosio[3], and Serena Villata[1]

[1] INRIA Sophia Antipolis, France
{firstname.lastname}@inria.fr
[2] EURECOM, France
[3] Machine Linking Srl, Italy
alessio@machinelinking.com

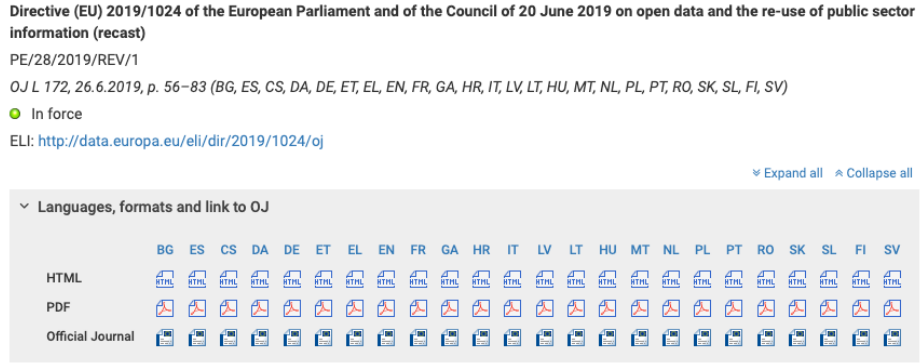
Panos Kudumakis, Thomas Wilmering, Mark Sandler, Víctor Rodríguez-Doncel, Laurent Boch, and Jaime Delgado

The Challenge: From MPEG Intellectual Property Rights Ontologies to Smart Contracts and Blockchains

Directive on Open Data (2019)

Objectives:

- Ensuring **fair competition and easy access public sector information**.
- Enhancing **cross-border innovation** based on data.
- Introducing a principle that **government data should be open by default** and design and provided (almost) free of charge **without (unnecessary) restrictions**.



Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast)

PE/28/2019/REV/1

OJ L 172, 26.6.2019, p. 56–83 (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/2019/1024/oj

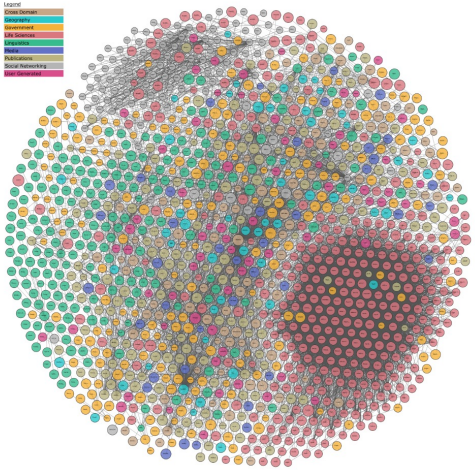
Expand all Collapse all

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	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML
PDF																								
Official Journal																								

https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561563110433&uri=CELEX:32019L1024

Open Data
A community perspective



https://lod-cloud.net/

https://webfoundation.org/2011/11/5-star-open-data-initiatives/

History

	White	Colored	Graph file	Dataset list	Dataset
2023-09-03		png	svg json		1314
2022-11-03		png	svg json		1268
2020-05-20		png	svg json		1,255
2019-03-29		png	svg	1,239	
2019-01-08		png	svg	1,234	
2018-11-26		png	svg	1,231	
2018-10-31		png	svg	1,229	
2018-08-28		png	svg	1,224	
2018-07-30		png	svg	1,220	
2018-06-28		png	svg	1,205	
2018-05-30		png	svg json		1,186
2018-04-30		png	svg json		1,184
2017-08-22		png	svg json	tsv	1,163
2017-02-20		png	svg		1,139
2017-01-26		png	svg		1,146
2014-08-30	png pdf svg	png pdf svg			570
2011-09-19	png pdf svg	png pdf svg			295
2010-09-22	png pdf svg	png pdf svg			203
2009-07-14	png pdf svg				95
2009-03-27	png pdf svg	png pdf svg			93
2009-03-05	png pdf svg	png pdf svg			89
2008-09-18	png pdf svg				45
2008-03-31	png pdf svg				34
2008-02-28	png pdf svg				32
2007-11-10	png pdf svg				28
2007-11-07	png				28
2007-10-08	png				25
2007-05-01	png				12

Open Data

A community perspective

LOD Laundromat: A Uniform Way of Publishing Other People's Dirty Data

Wouter Beek, Laurens Rietveld, Hamid R. Bazoobandi, Jan Wielemaker, and Stefan Schlobach

Dept. of Computer Science, VU University Amsterdam, NL
{w.g.j.beek,laurens.rietveld,h.bazoubandi, j.wielemaker,k.s.schlobach}@vu.nl

A Survey of Current Approaches for Transforming Open Data to Linked Data

MEHERHERA Amina[1], MEKIDECHE Imane[1], Dr. ZEMMOUCHI GHOMARI Leila[2], and Pr. GHOMARI Abdesamed Réda[1]

[1] LMCS - École Nationale Supérieure d'Informatique (ESI ex.INI), Oued Smar, Algiers.
[2] École Nationale Supérieure de Technologie (ENST), Bordj El Kiffan, Algiers.
fa_meherhera@esi.dz , fi_mekideche@esi.dz , leila.ghomari@enst.dz , a_ghomari@esi.dz

Journal of Information Science
Volume 48, Issue 1, February 2022, Pages 21-43

https://doi.org/10.1177/0165551520930951

SAGE journals

Article

Evaluating the quality of linked open data in digital libraries

Gustavo Candela [1], Pilar Escobar [2], Rafael C Carrasco[3], and Manuel Marco-Such[4]

International Journal of Computer and Information Technology (ISSN: 2279 – 0764)
Volume 10 – Issue 1, January 2021

Open Government Data (OGD) Publication as Linked Open Data (LOD): A Survey

Khadidja Bouchelouche
LMCS, Ecole nationale Supérieure d'Informatique, ESI
Algeria
Email : k_bouchelouche [AT] esi.dz

Abdessamed Réda Ghomari
LMCS, Ecole Nationale Supérieure d'Informatique, ESI
Algeria
Email : a_ghomari [AT] esi.dz

Leila Zemmouchi-Ghomari
Ecole Nationale Supérieure de Technologie, ENST
Algeria
Email : leila.ghomari [AT] enst.dz

The Data Governance Act (2022)

European Commission

Objectives:

- Strengthen mechanisms to **increase data availability**.
- Increase **trust in data sharing**.
- 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.
- Facilitate **sharing in a variety of sectors**: health, environment, energy, agriculture, mobility, finance, manufacturing, public administration and skills

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

The Data Governance Act (2022)

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.

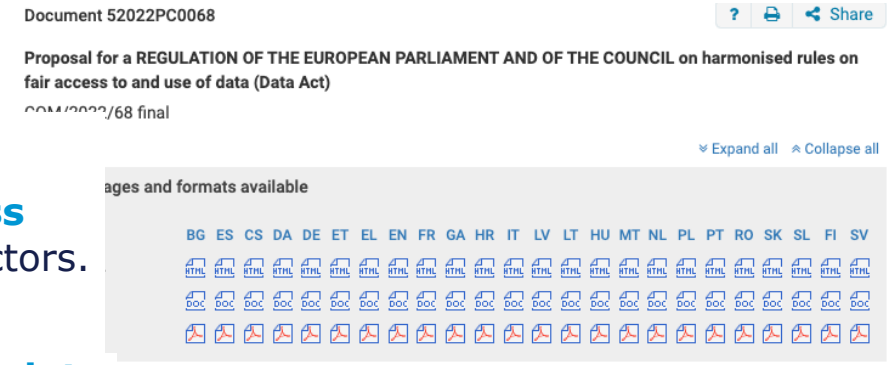
2. Measures to ensure that data intermediaries will function as trustworthy organisers of data sharing or pooling within the common European data spaces.

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.

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

The Data Act (2023)



Objectives:

- Proposing new rules on **who can use and access data** generated in the EU across all economic sectors.
- Ensure **fairness** in the digital environment, **stimulate a competitive data market**, open opportunities for data-driven innovation and make data more accessible.
- New rules setting the framework for **customers to effectively switch between different providers** of data-processing services to unlock the **EU cloud market**.

The Data Act (2023)

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.

https://digital-strategy.ec.europa.eu/en/polici

Data Access & Governance

A community perspective

A survey of trust in computer science and the Semantic Web

Donovan Artz, Yolanda Gil *

Information Sciences Institute, University of Southern California, 4677 Admiralty Way, Marina del Rey, CA 90292, United States

Received 9 February 2006; accepted 23 March 2007
Available online 31 March 2007

If you can't enforce it, contract it: Enforceability in Policy-Driven (Linked) Data Markets

Simon Steyskal *, Sabrina Kirrane
Vienna University of Economics and Business, Vienna, Austria
[firstname.lastname]@wu.ac.at

A Blockchain-driven Architecture for Usage Control in Solid

Davide Basile, Claudio Di Ciccio, and Valerio Goretti
Department of Computer Science
Sapienza University of Rome, Italy

Sabrina Kirrane
Department of Information Systems and Operations
Vienna University of Economics and Business, Austria

Blockchain based resource governance for decentralized web environments

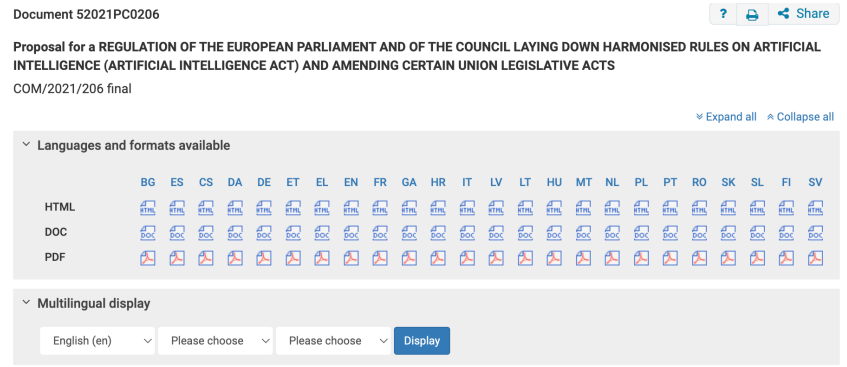
Davide Basile[1], Claudio Di Ciccio[1], Valerio Goretti[1]* and Sabrina Kirrane[2]

[1]Department of Computer Science, Sapienza University of Rome, Rome, Italy, [2]Institute for Information Systems and New Media, Vienna University of Economics and Business, Vienna, Austria

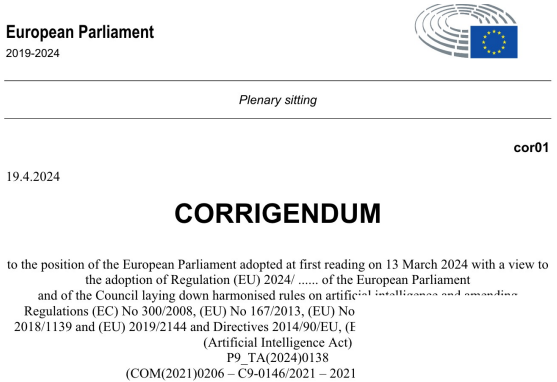
The Artificial Intelligence Act (2024)

Objectives:

- 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.
- It supports the objective of the Union being a **global leader** in the development of **secure, trustworthy and ethical** artificial intelligence.



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



European Parliament
2019-2024

Plenary sitting

cor01

19.4.2024

CORRIGENDUM

to the position of the European Parliament adopted at first reading on 13 March 2024 with a view to the adoption of Regulation (EU) 2024/ ..... of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (E (Artificial Intelligence Act)
P9_TA(2024)0138
(COM(2021)0206 – C9-0146/2021 – 2021

https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf

The Artificial Intelligence Act (2024)

What is meant by the term AI?

Machine Learning approaches *that learn from data how to achieve certain objectives,*

and

Logic- and Knowledge-based approaches *that infer from encoded knowledge or symbolic representation of the task to be solved.*

The Artificial Intelligence Act (2024)

Risk based approach

- 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

Artificial Intelligence Legislation

Prohibited 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 done by public authorities.

The Artificial Intelligence Act (2024)

Charter of Fundamental Rights of the European Union

DIGNITY

Human dignity
Right to life
Right to the integrity of the person
Prohibition of torture and inhuman or degrading treatment or punishment
Prohibition of slavery and forced labour

FREEDOMS

Right to liberty and security
Respect for private and family life
Protection of personal data
Right to marry and right to found a family
Freedom of thought, conscience and religion
Freedom of expression and information
Freedom of assembly and of association
Freedom of the arts and sciences
Right to education
Freedom to choose an occupation and right to engage in work
Freedom to conduct a business
Right to property
Right to asylum
Protection in the event of removal, expulsion or extradition

The Artificial Intelligence Act (2024)

Charter of Fundamental Rights of the European Union

EQUALITY

Equality before the law
Non-discrimination
Cultural, religious and linguistic diversity
Equality between women and men
The rights of the child
The rights of the elderly
Integration of persons with disabilities

SOLIDARITY

Workers' right to information and consultation within the undertaking
Right of collective bargaining and action
Right of access to placement services
Protection in the event of unjustified dismissal
Fair and just working conditions
Prohibition of child labour and protection of young people at work
Family and professional life
Social security and social assistance
Health care
Access to services of general economic interest
Environmental protection
Consumer protection

The Artificial Intelligence Act (2024)

Charter of Fundamental Rights of the European Union

CITIZENS' RIGHTS

Right to vote and to stand as a candidate at elections to the European Parliament
Right to vote and to stand as a candidate at municipal elections
Right to good administration
Right of access to documents
European Ombudsman
Right to petition
Freedom of movement and of residence
Diplomatic and consular protection

JUSTICE

Right to an effective remedy and to a fair trial
Presumption of innocence and right of defence
Principles of legality and proportionality of criminal offences and penalties
Right not to be tried or punished twice in criminal proceedings for the same criminal offence

Artificial Intelligence Legislation

High Risk AI

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;

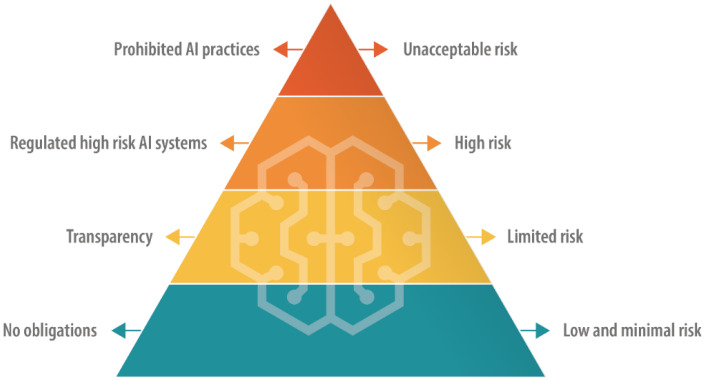
2. Management and operation of critical infrastructure:

   (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.



Data source: European Commission.

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;

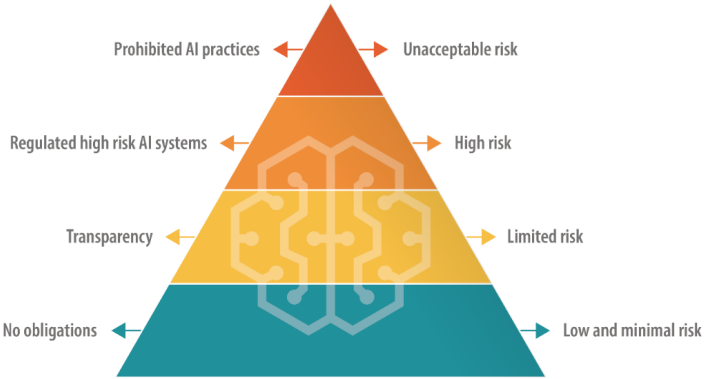
   (b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships.

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.



Data source: European Commission.

Artificial Intelligence Legislation

High Risk AI

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;

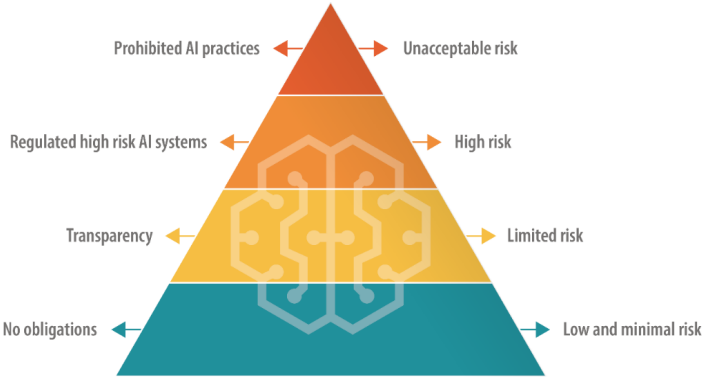
(c) AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in article 52(3);

(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.



Data source: European Commission.

Artificial Intelligence Legislation

High Risk AI

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;

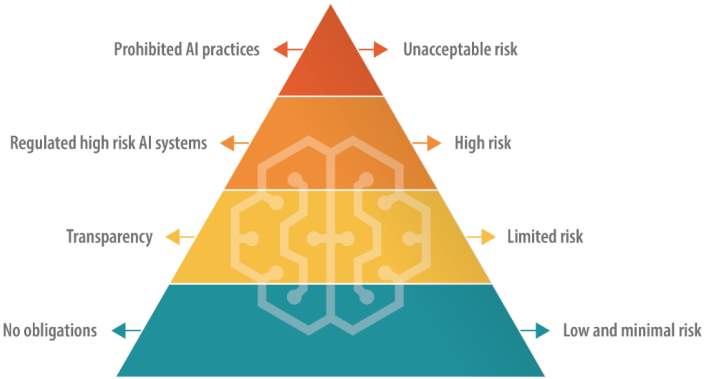
   (b) AI systems intended to be used by competent public authorities to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;

   (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.



Data source: European Commission.

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** compose representatives fr
States and the Commission.

Artificial Intelligence Governance:
A community perspective

Towards a Knowledge-Aware AI
A. Dimou et al. (Eds.)

doi:10.3233/SSW220008

AIRO: An Ontology for Representing AI Risks Based on the Proposed EU AI Act and ISO Risk Management Standards

To Be High-Risk, or Not To Be—Semantic Specifications and Implications of the AI Act's High-Risk AI Applications and Harmonised Standards

Delaram Golpayegani
ADAPT Centre, Trinity College Dublin
Dublin, Ireland
sgolpays@tcd.ie

Harshvardhan J. Pandit
ADAPT Centre, Dublin City University
Dublin, Ireland
harshvardhan.pandit@dcu.ie

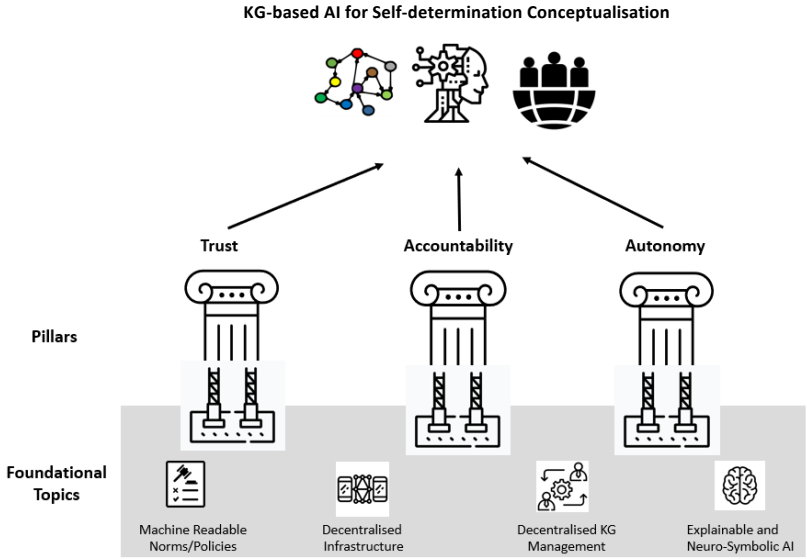
Dave Lewis
ADAPT Centre, Trinity College Dublin
Dublin, Ireland
delewis@tcd.ie

Trust, Accountability, and Autonomy in Knowledge Graph-Based AI for Self-Determination

Luis-Daniel Ibáñez
Department of Electronics and Computer Science, University of Southampton, UK
John Domingue
Knowledge Media Institute, The Open University, Milton Keynes, UK
Sabrina Kirrane
Institute for Information Systems & New Media, Vienna University of Economics and Business, Austria
Oshani Seneviratne
Department of Computer Science, Rensselaer Polytechnic Institute, USA
Aisling Third
Knowledge Media Institute, The Open University, Milton Keynes, UK
Maria-Esther Vidal
Leibniz University of Hannover, Germany
TIB-Leibniz Information Centre of Science and Technology, Hannover, Germany
L3S Research Centre, Hannover, Germany

KG-based AI for Self-Determination

- 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



Ibáñez, L., Domingue, J., Kirrane, S., Seneviratne, O., Third, A., Vidal, M., 2023. Trust, Accountability, and Autonomy in Knowledge Graph-based AI for Self-determination. Transactions on Graph Data and Knowledge (TGDK)

AI literacy

AI literacy should equip providers, deployers and affected persons with the necessary notions to make informed decisions regarding AI systems.

Those notions may vary with regard to the relevant context can include:

- understanding the correct **application of technical elements** during the AI system's development phase;
- the **measures** to be applied during its use;
- the suitable ways in which to **interpret** the AI system's output; and
- in the case of affected persons, the **knowledge necessary to understand how decisions taken** with the assistance of AI will have an impact on them.

Transparency

To address concerns related to opacity and complexity of certain AI systems and help deployers to fulfil their obligations under this Regulation, transparency should be required for high-risk AI systems before they are placed on the market or put it into service.

In order to enhance legibility and accessibility of the information included in the instructions of use, where appropriate,

- illustrative examples, for instance on the **limitations and on the intended and precluded uses** of the AI system, should be included.
- Providers should ensure that all documentation, including the instructions for use, contains **meaningful, comprehensive, accessible and understandable information,** taking into account the needs and foreseeable **knowledge of the target deployers**

Context

Whilst risks related to AI systems can result from the way such systems are designed, risks can as well stem from how such AI systems are used. Deployers of high-risk AI system therefore play a critical role in ensuring that fundamental rights are protected, complementing the obligations of the provider when developing the AI system.

Deployers are best placed to understand

- how the high-risk AI system will be **used concretely**; and
- can **identify potential significant risks** that were not foreseen in the development phase,
- due to a more **precise knowledge of the context of use**, the persons or groups of persons likely to be affected, including vulnerable group

My Current Call to Action

Call for papers: Special Issue on Semantic Technologies for Data and Algorithmic Governance

Guest editors

Michel Dumontier, Maastricht University, The Netherlands
Sabrina Kirrane, Vienna University of Economics and Business, Austria
Oshani Seneviratne, Rensselaer Polytechnic Institute, USA

Topics of Interest

We welcome original high quality submissions on (but are not restricted to) the following topics:

- Findable, Accessible, Interoperable, and Reusable (FAIR) data management
- Techniques for enabling ownership, control, and access
- Identifying fake news and misinformation
- Managing bias and ensuring fairness
- Enabling transparency, explainability, and accountability
- Methods for policy governance
- Information flow control and accountability
- Measuring data quality
- Managing the data life cycle
- Metrics for assessing the effectiveness of governance algorithms
- Data privacy, regulations and compliance
- Provenance, trust and metadata for authoritative sources
- Privacy and security enforcement
- Methods for information flow control and accountability
- Frameworks and systems for personal data storage and control
- Ensuring data authenticity and integrity
- Privacy-preserving data mining and machine learning methods
- Protecting against identity theft and data falsification
- User-friendly interface design for data and algorithmic governance
- Standards for data and algorithmic governance
- Tackling legal issues with respect to data and algorithms
- Law and governance in e-democracy and e-participation
- Benchmarking approaches to data and algorithmic governance
- Building trust and transparency mechanisms in the fabric of the Web
- Participatory frameworks for fair and efficient algorithmic governance

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