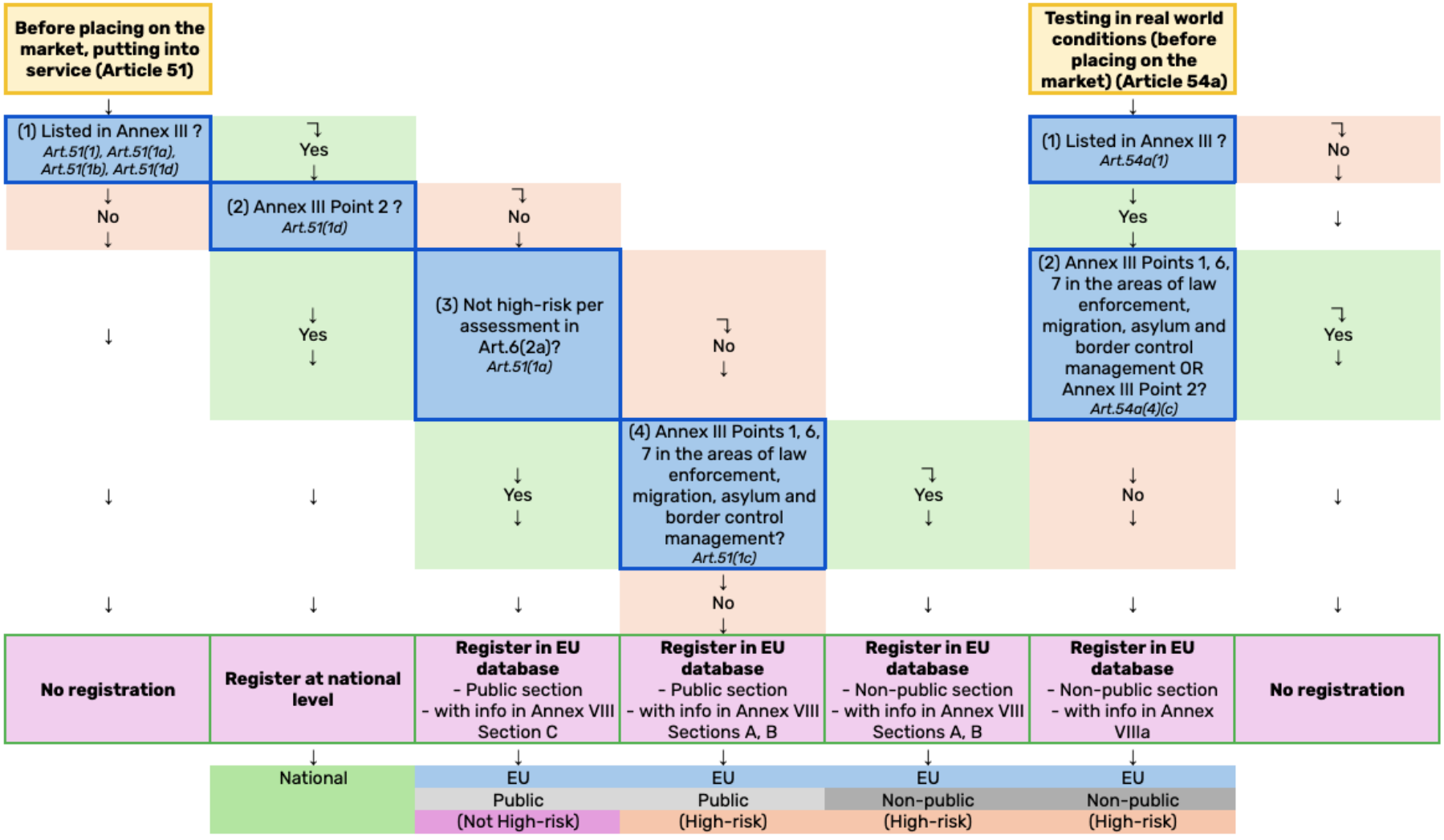
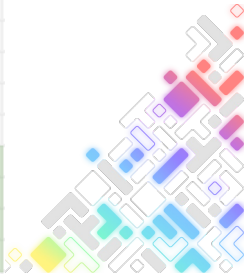
OPERATIONS MANAGEMENT SUMMIT @ THE LINUX FOUNDATION OPEN SOURCE SUMMIT NORTH AMERICA

Accountability Taxonomy for AI Software Bill of Materials

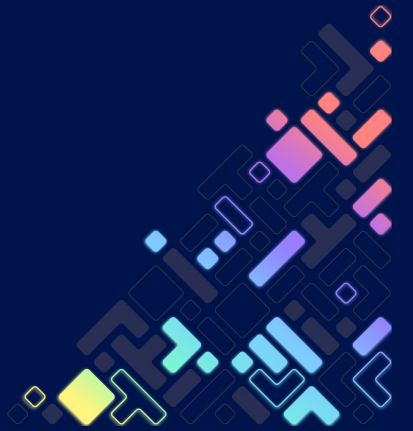
Arthit Suriyawongkul, ADAPT Centre, Trinity College Dublin

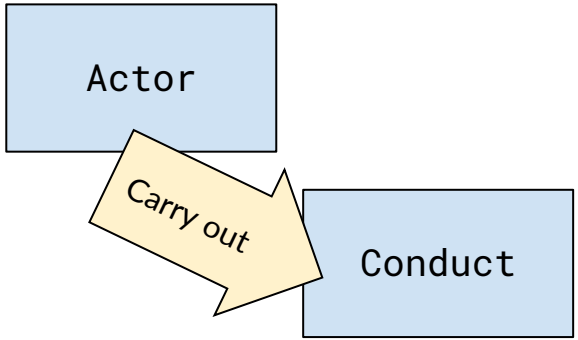

Before placing on the market, putting into service (Article 51)
(1) Listed in Annex III ?
Art.51(1), Art.51(1a), Art.51(1b), Art.51(1d)
Yes
No
(2) Annex III Point 2 ?
Art.51(1d)
Yes
No
(3) Not high-risk per assessment in Art.6(2a)?
Art.51(1a)
Yes
No
(4) Annex III Points 1, 6, 7 in the areas of law enforcement, migration, asylum and border control management?
Art.51(1c)
Yes
No
Testing in real world conditions (before placing on the market) (Article 54a)
(1) Listed in Annex III ?
Art.54a(1)
Yes
No
(2) Annex III Points 1, 6, 7 in the areas of law enforcement, migration, asylum and border control management OR Annex III Point 2?
Art.54a(4)(c)
Yes
No
No registration
Register at national level
Register in EU database
- Public section
- with info in Annex VIII Section C
Register in EU database
- Public section
- with info in Annex VIII Sections A, B
Register in EU database
- Non-public section
- with info in Annex VIII Sections A, B
Register in EU database
- Non-public section
- with info in Annex VIIIa
No registration
National
EU
Public
(Not High-risk)
EU
Public
(High-risk)
EU
Non-public
(High-risk)
EU
Non-public
(High-risk)

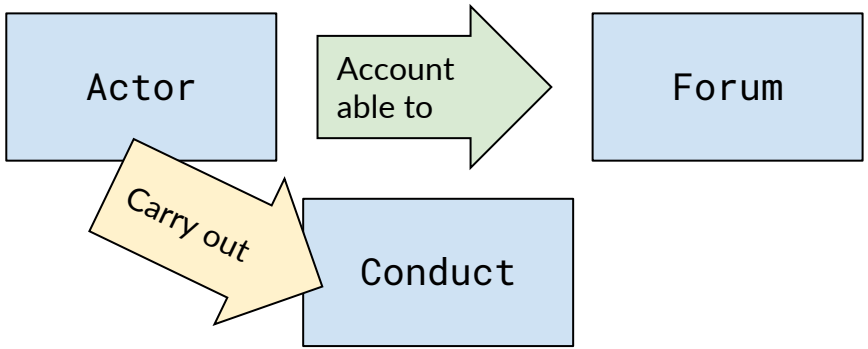
		Before placing on the market, putting into service (Article 51)			Testing in real world conditions (Article 54a)
		↓	↓	↓	↓
		with info in Annex VIII Section C	with info in Annex VIII Sections A, B	with info in Annex VIII Sections A, B	with info in Annex VIIIa
		↓	↓	↓	↓
		EU	EU	EU	EU
		Public	Public	Non-public	Non-public
		(Not High-risk)	(High-risk)	(High-risk)	(High-risk)
1	Name and contact details of the provider	Provider	Provider	Provider	Provider
4	AI system trade name	Provider	Provider	Provider	
5	Traceable ID	Provider	Provider	Provider	Provider
6	Intended purpose	Provider	Provider	Provider	Provider
7	Components and functions supported through this AI system;		Provider	Provider	
8	Information used by the system (data, inputs) and its operating logic;		Provider		
10	Summary of the grounds for considering the AI system as not high-risk	Provider			
11	Status of the AI system (on the market, or in service; no longer placed on the market/in service, recalled);	Provider	Provider	Provider	
13	Type, number and expiry date of the certificate issued by the notified body		Provider		
15	A copy of the EU declaration of conformity		Provider		
16	Instructions for use		Provider		
18	Name and contact details of the deployer		Deployer	Deployer	
20	A summary of the findings of the fundamental rights impact assessment		Deployer		
21	The URL of the entry of the AI system in the EU database by its provider		Deployer		
22	A summary of the data protection impact assessment		Deployer		
23	Union-wide unique single identification number of the testing				Provider
24	Name and contact details of users involved in the testing				Provider
26	A summary of the main characteristics of the plan for testing				Provider
27	Information on the suspension or termination of the testing				Provider

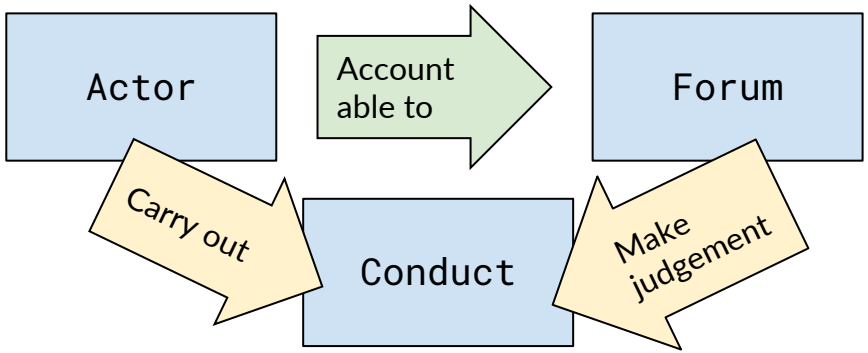


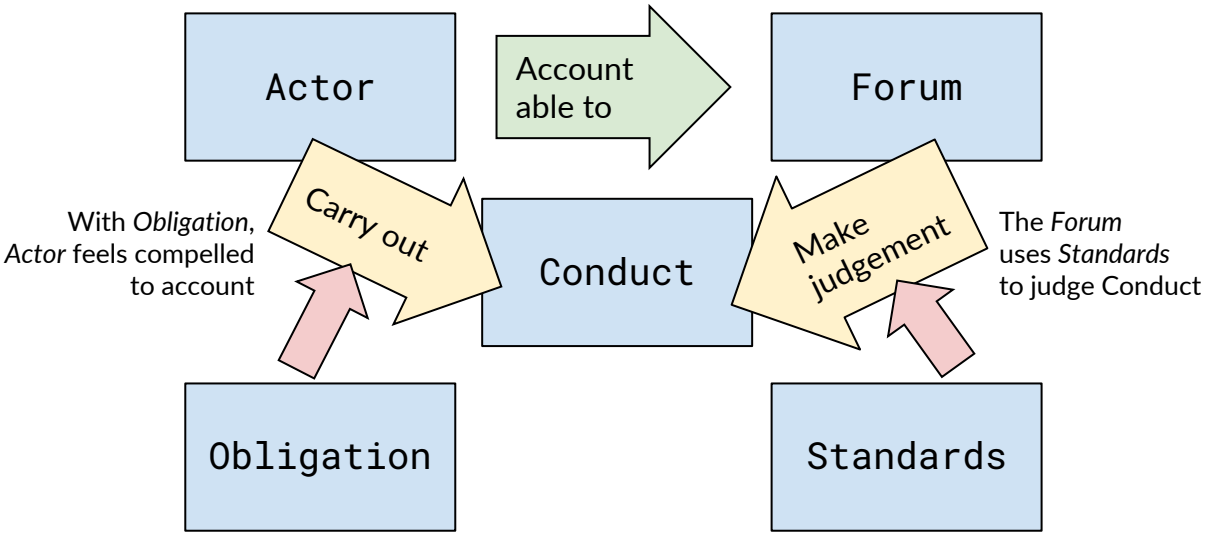
Accountability?



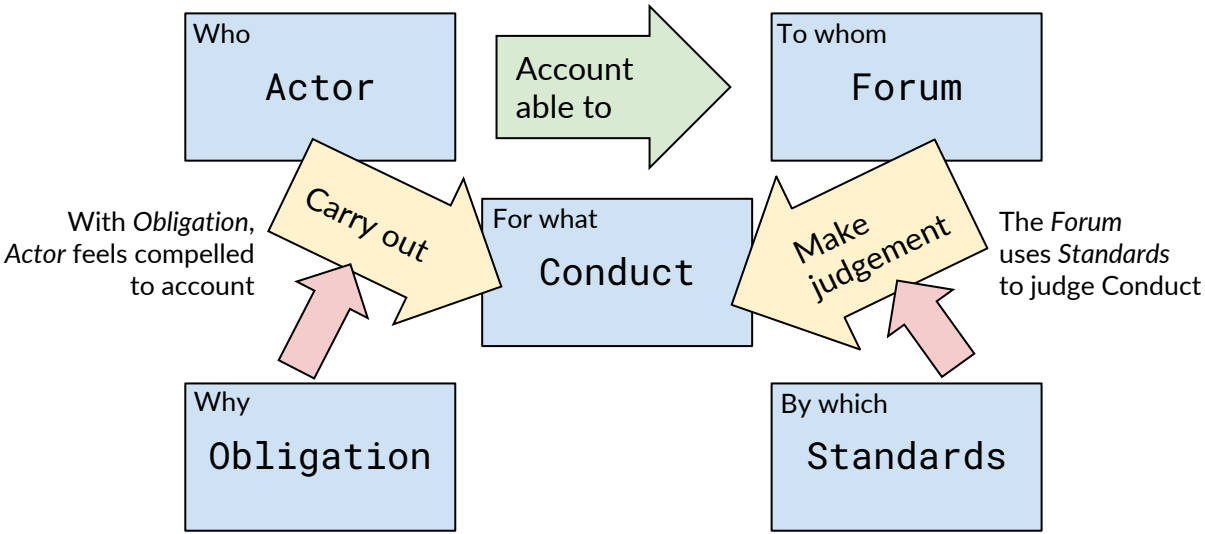

Actor
Carry out
Conduct


Actor
Account able to
Forum
Carry out
Conduct


Actor
Account able to
Forum
Carry out
Conduct
Make judgement

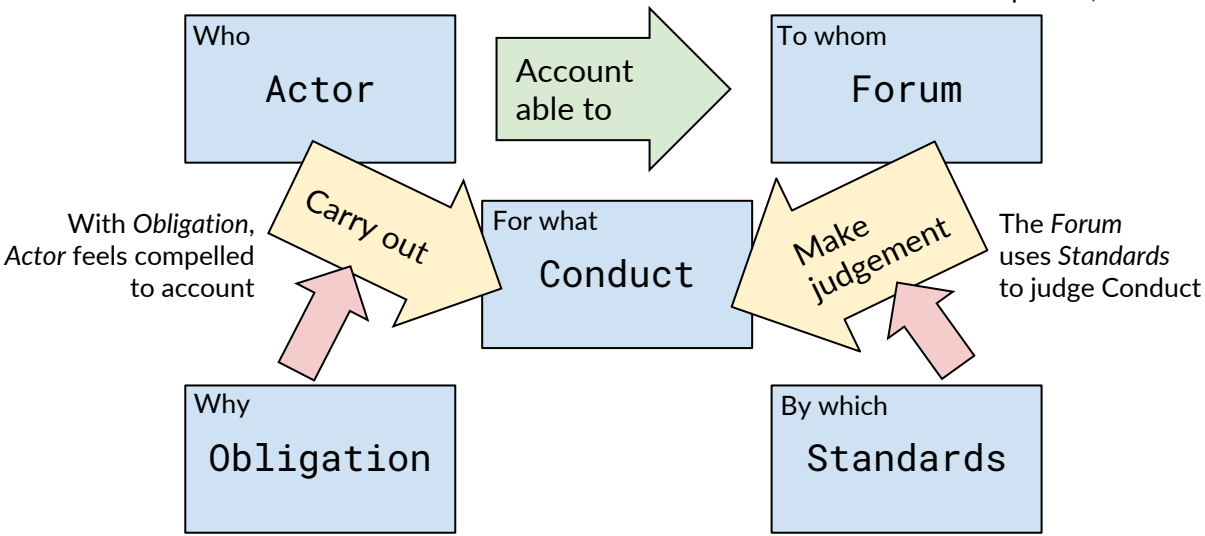

Actor
Account able to
Forum
With *Obligation*, *Actor* feels compelled to account
Carry out
Conduct
Make judgement
The *Forum* uses *Standards* to judge Conduct
Obligation
Standards

Who is accountable to **whom**, for **what**,
by **which** standards, and **why**?



Who is accountable to **whom**, for **what**, by **which** standards, and **why**?

Voters, Parliament (political accountability)
Management board, Minister (managerial)
Regulators, Ombudsmen (administrative)
Courts (legal)
Professional bodies
Affected 3rd parties, stakeholders (social)

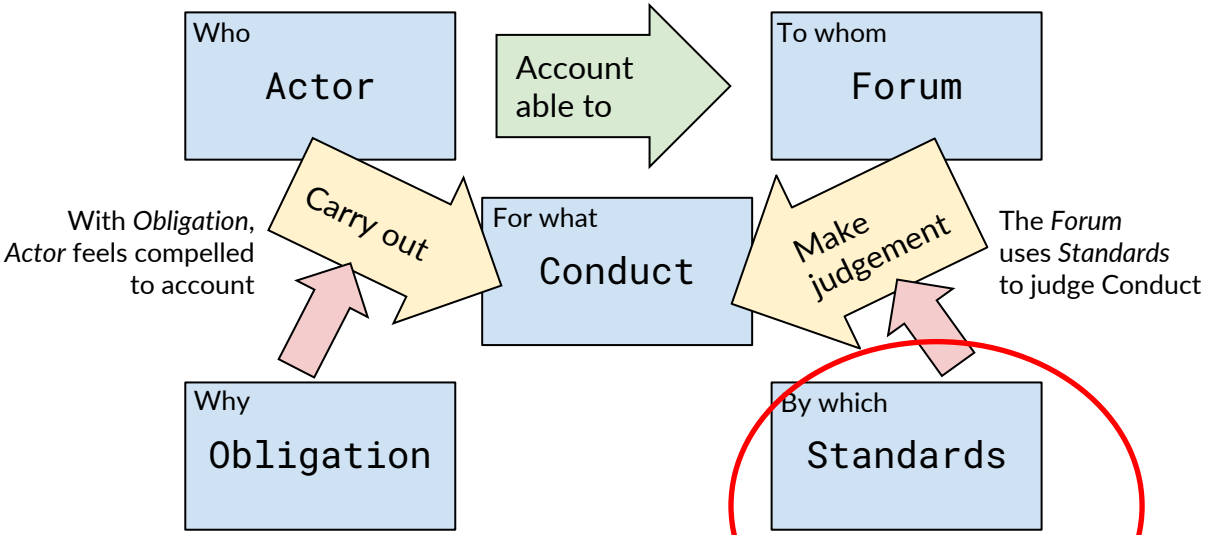


Mandatory accountability
Voluntary accountability
Quasi-voluntary accountability

Due process (legal accountability)
Professional norms and standards
Political demands

Who is accountable to **whom**, for **what**, by **which** standards, and **why**?

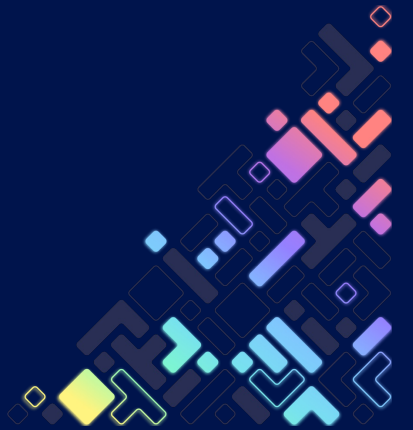
Voters, Parliament (political accountability)
Management board, Minister (managerial)
Regulators, Ombudsmen (administrative)
Courts (legal)
Professional bodies
Affected 3rd parties, stakeholders (social)



Mandatory accountability
Voluntary accountability
Quasi-voluntary accountability

Due process (legal accountability)
Professional norms and standards
Political demands

A working definition of accountability.



“Accountability” definition

“A set of mechanisms, practices and attributes that sum to a governance structure which involves committing to legal and ethical obligations, policies, procedures and mechanism, explaining and demonstrating ethical implementation to internal and external stakeholders and remedying any failure to act properly”.

Derived from Felici et al. 2013. Used in IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems and in “A governance framework for algorithmic accountability and transparency” study report by European Parliamentary Research Service.

Purposes of Public Accountability

(adapted from Bovens et al. 2010)

Democratic perspective

Popular control

Explainability (legitimacy) + Human oversight (lawful + ethical)

Constitutional perspective

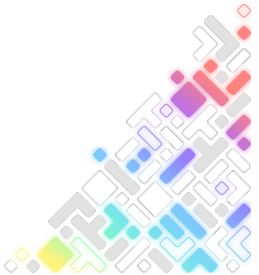
Prevention of corruption and abuse of power

Bias and drift detection (technically robust + ethical)

Learning perspective

Maximising public value

Information that allow the improvement of the system (technically robust, organizational learning)



Accountability as a virtue and as a mechanism

Accountability as a virtue	Accountability as a mechanism
Focus on Behaviour	**Focus on governance of behaviour**
Focus on actual performance of agencies	Focus on institutional relation or arrangement in which an agent can be held to account by another agent or institution
Accountability is dependent variable; accountability has effect on behaviour	Accountability is independent variable; accountability may or may not have effect on behaviour
Virtue is more domain-specific	Mechanism is less domain-specific
In AI context: How the AI system performs (accuracy, drift, etc.)	In AI context: How the AI system get built and served
AI regulations: Post-market monitoring	**AI regulations: Quality management system, Technical documentation**

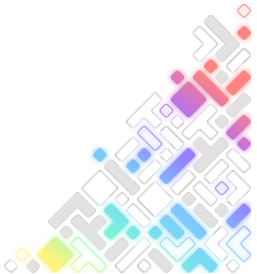
Adapted from Bovens, M., Schillemans, T., Goodin, R.E., 2014. Public Accountability, in: The Oxford Handbook of Public Accountability. Oxford University Press, Oxford, New York, pp. 1–20. https://doi.org/10.1093/oxfordhb/9780199641253.013.0012

“Non-algorithmic” accountability

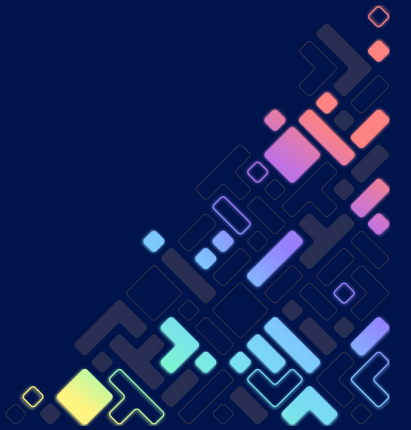
“Technical issues in algorithmic accountability are largely a question if the system behaves according to specifications.

Accountability issues such as redress are beyond the technical challenges of the algorithm; these are more a question about the actions implied by the specifications.”

European Parliament. Directorate General for Parliamentary Research Services. "A Governance Framework for Algorithmic Accountability and Transparency."



Information obligations



Information obligations in EU AI Act that can support accountability (partial)

For high-risk AI systems
Provider name, registered trade name
Intended purpose
Instruction for use
Design choices
Standards applicable
Data origin, Collection original purpose
Possible biases, Measures to detect

For general purpose AI models
Intended tasks, Limitations
Instruction for use
Model design specification
Training process, Testing process
Information on the data used
Copyright protection policy
Acceptable use policies applicable

Ensuring Transparency in AI Life-Cycle

AI Developer

Experience Designer

Technical Writer

Create AI model
- Prioritise explanations by considering domain, use case, impact
- Record explainability method limits

Design UX
- User can interpret #A13(1)
- Interface, mental model

Write documents
- Clear language for target (e.g. deployer)
- e.g. accuray #A15(2), instructions of use Annex IV (1) (g)

AT ST | IT | IT

New version

Provider

ST

Technical documentation, including provenance #A11, #A18. Software Bill of Materials may facilitate the description of elements of AI systems Annex IV (2)

Documenting

AI System Product Cycle

Deployer

IT ST

Provider

Deployer

Monitoring

AT ST

Record-keeping #A12 and monitoring #A29(4) (planned in #A61). Report serious incidents to MSA #A62, preferably with a standardized risks and harms taxonomy – for example, AIAAIC.

IT ST

User + Society

Place onto the market

Regulators

AT ST

AT: Algorithmic transparency

IT: Interactive transparency

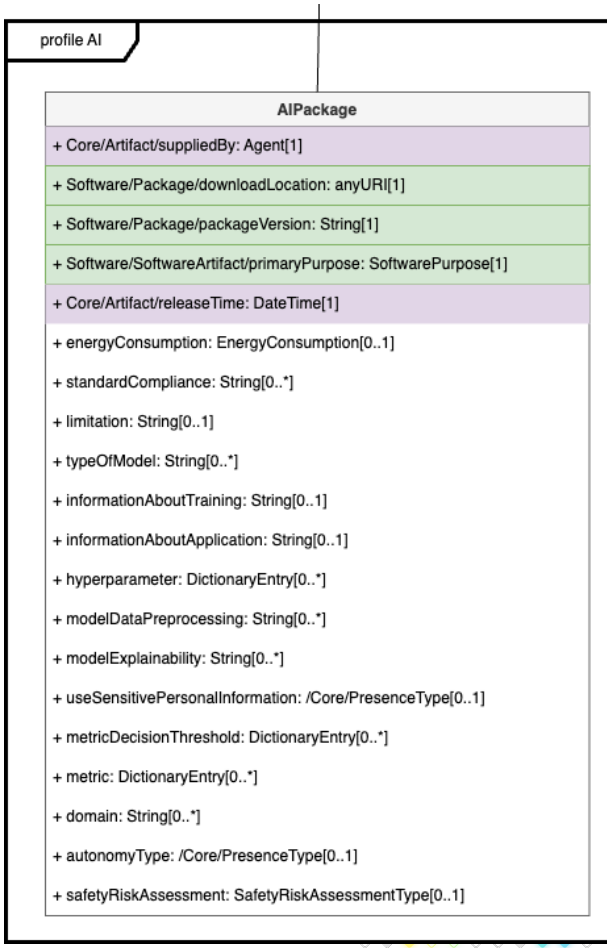
ST: Social transparency

	Algorithmic	Interaction	Social
Developer	X		
Designer		X	
Owner			X
User		X	X
Regulator	X		X
Society			X

An example stakeholder transparency matrix purposed. Will differ by the AI system, domain, and context.

Software Bill of Materials

"formal record containing the details and supply chain relationships of various components used in building software" – Executive Order on Improving the Nation's Cybersecurity (EO 14028)
"analogous to a list of ingredients" "can help organisations or persons avoid consumption of software that could harm them." – Wikipedia
"communicating a release: name, version, components, licenses, copyrights, and useful security references." – SPDX
ISO/IEC 5962:2021 Software Package Data Exchange (SPDX) Specification V2.2.1



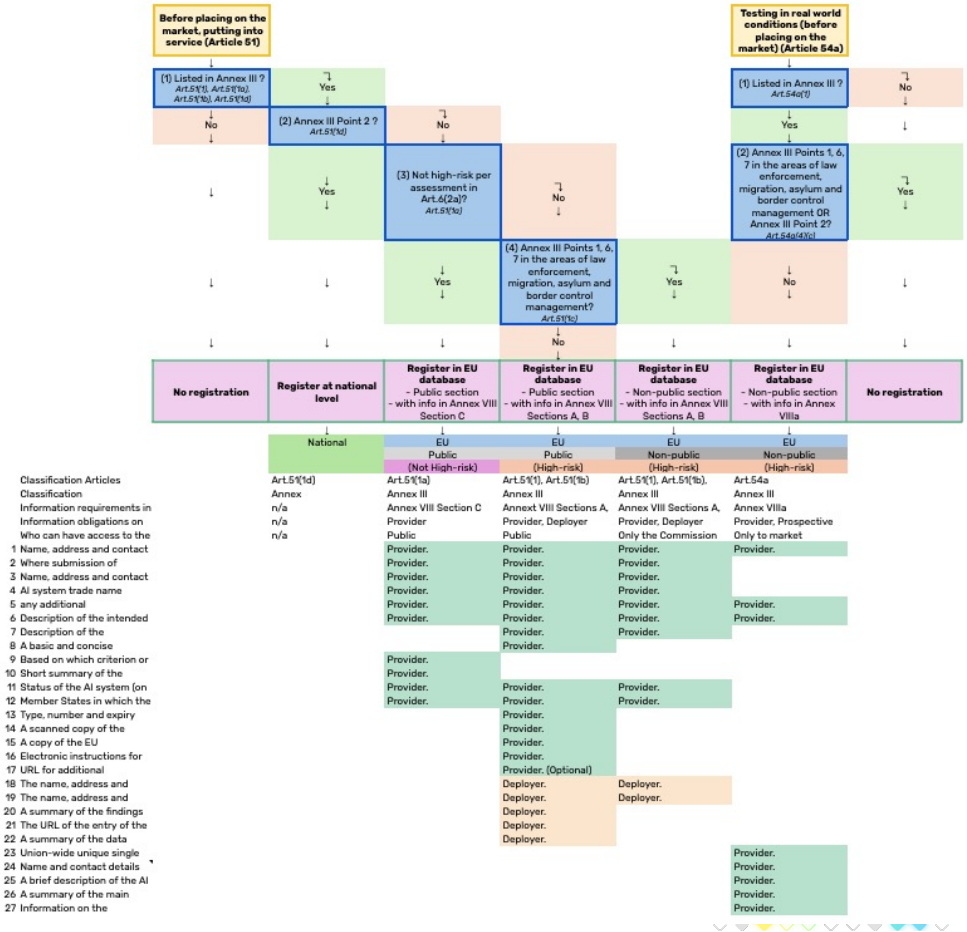
Use cases

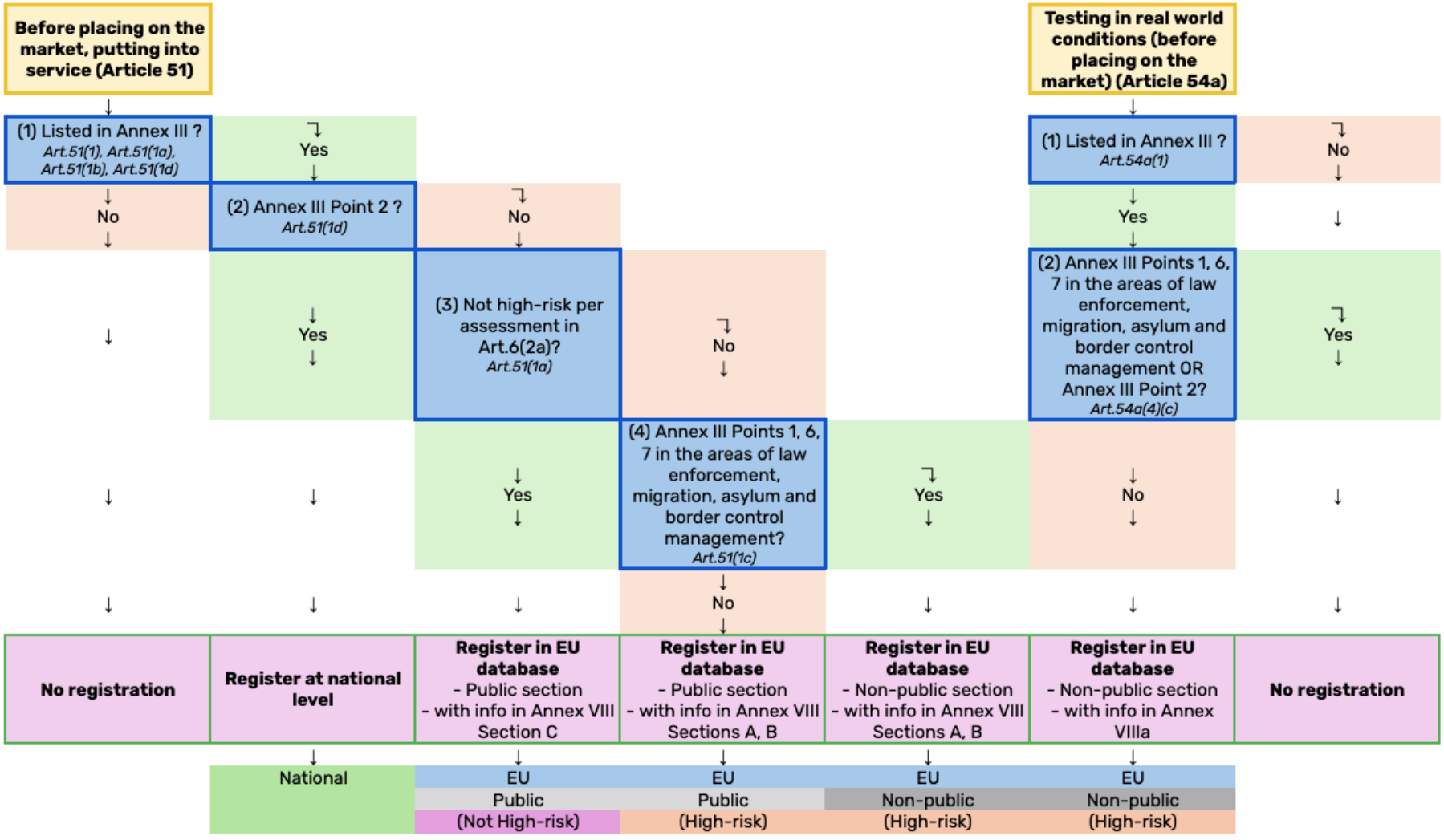
For AI providers/deployers

- **To register in national/supranational database**
- **To get permission for testing in real-world conditions**
- To get the declaration of conformity
- To report serious incident post-market
- To estimate remaining information obligations to fulfil to enter a new market

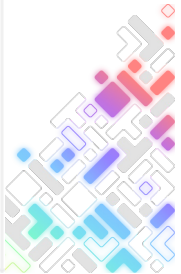
For regulators

- To estimate resource for regulatory compliance

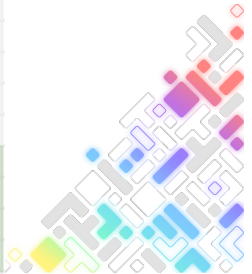



Before placing on the market, putting into service (Article 51)
(1) Listed in Annex III ?
Art.51(1), Art.51(1a), Art.51(1b), Art.51(1d)
Yes
No
(2) Annex III Point 2 ?
Art.51(1d)
Yes
No
(3) Not high-risk per assessment in Art.6(2a)?
Art.51(1a)
Yes
No
(4) Annex III Points 1, 6, 7 in the areas of law enforcement, migration, asylum and border control management?
Art.51(1c)
Yes
No
Testing in real world conditions (before placing on the market) (Article 54a)
(1) Listed in Annex III ?
Art.54a(1)
Yes
No
(2) Annex III Points 1, 6, 7 in the areas of law enforcement, migration, asylum and border control management OR Annex III Point 2?
Art.54a(4)(c)
Yes
No
No registration
Register at national level
Register in EU database
- Public section
- with info in Annex VIII Section C
Register in EU database
- Public section
- with info in Annex VIII Sections A, B
Register in EU database
- Non-public section
- with info in Annex VIII Sections A, B
Register in EU database
- Non-public section
- with info in Annex VIIIa
No registration
National
EU
Public
(Not High-risk)
EU
Public
(High-risk)
EU
Non-public
(High-risk)
EU
Non-public
(High-risk)

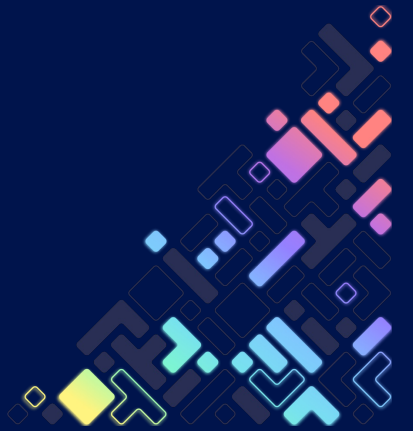
	Register at national level	**Register in EU database** - Public section - with info in Annex VIII Section C	**Register in EU database** - Public section - with info in Annex VIII Sections A, B	**Register in EU database** - Non-public section - with info in Annex VIII Sections A, B	**Register in EU database** - Non-public section - with info in Annex VIIIa
	↓	↓	↓	↓	↓
	National	EU	EU	EU	EU
		Public	Public	Non-public	Non-public
		(Not High-risk)	(High-risk)	(High-risk)	(High-risk)
Classification Articles	Art.51(1d)	Art.51(1a)	Art.51(1), Art.51(1b)	Art.51(1), Art.51(1b), Art.51(1c)	Art.54a
Classification	Annex III Point 2	Annex III Points 1, 3, 4, 5, 6, 7, 8	Annex III Points 3, 4, 5, 8 AND Annex III 1, 6, 7 that is not in the areas of law enforcement, migration, asylum and border control management	Annex III Points 1, 6, 7 in the areas of law enforcement, migration, asylum and border control management	Annex III Points 3, 4, 5, 8 AND Annex III 1, 6, 7 that is not in the areas of law enforcement, migration, asylum and border control management
Information requirements in the EU database	n/a	Annex VIII Section C	Annext VIII Sections A, B	Annex VIII Sections A, B with Exceptions in Art.51(1c)	Annex VIIIa
Information obligations on	n/a	Provider	Provider, Deployer	Provider, Deployer	Provider, Prospective provider
Who can have access to the information	n/a	Public *Art.60(3)*	Public *Art.60(3)*	Only the Commission and national authorities referred to in Art. 63(5) (Market surveillance authorities) *Art.51(1c)*	Only to market surveillance authorities and the Commission, unless the prospective provider or provider has given consent for making this information also accessible the public. *Art.60(3)*



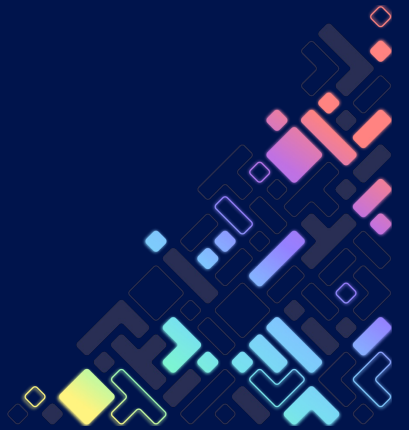
		Before placing on the market, putting into service (Article 51)			Testing in real world conditions (Article 54a)
		↓	↓	↓	↓
		with info in Annex VIII Section C	with info in Annex VIII Sections A, B	with info in Annex VIII Sections A, B	with info in Annex VIIIa
		↓	↓	↓	↓
		EU	EU	EU	EU
		Public	Public	Non-public	Non-public
		(Not High-risk)	(High-risk)	(High-risk)	(High-risk)
1	Name and contact details of the provider	Provider	Provider	Provider	Provider
4	AI system trade name	Provider	Provider	Provider	
5	Traceable ID	Provider	Provider	Provider	Provider
6	Intended purpose	Provider	Provider	Provider	Provider
7	Components and functions supported through this AI system;		Provider	Provider	
8	Information used by the system (data, inputs) and its operating logic;		Provider		
10	Summary of the grounds for considering the AI system as not high-risk	Provider			
11	Status of the AI system (on the market, or in service; no longer placed on the market/in service, recalled);	Provider	Provider	Provider	
13	Type, number and expiry date of the certificate issued by the notified body		Provider		
15	A copy of the EU declaration of conformity		Provider		
16	Instructions for use		Provider		
18	Name and contact details of the deployer		Deployer	Deployer	
20	A summary of the findings of the fundamental rights impact assessment		Deployer		
21	The URL of the entry of the AI system in the EU database by its provider		Deployer		
22	A summary of the data protection impact assessment		Deployer		
23	Union-wide unique single identification number of the testing				Provider
24	Name and contact details of users involved in the testing				Provider
26	A summary of the main characteristics of the plan for testing				Provider
27	Information on the suspension or termination of the testing				Provider



Demo



regtech.adaptcentre.ie



d-real SFI centre for research training in digitally-enhanced reality

Centre for Research Training | Science Foundation Ireland sfi For what's next

Thank you

Arthit Suriyawongkul
suriyawa@tcd.ie

HOST INSTITUTION

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

PARTNER INSTITUTIONS

DCU Ollscoil Chathair Bhaile Átha Cliath Dublin City University

DUBLIN

University College Dublin An Coláiste Ollscoile, Baile Átha Cliath Ireland's Global University

Ollscoil na Gaillimhe University of Galway

THE LINUX FOUNDATION

OPEN SOURCE SUMMIT

NORTH AMERICA