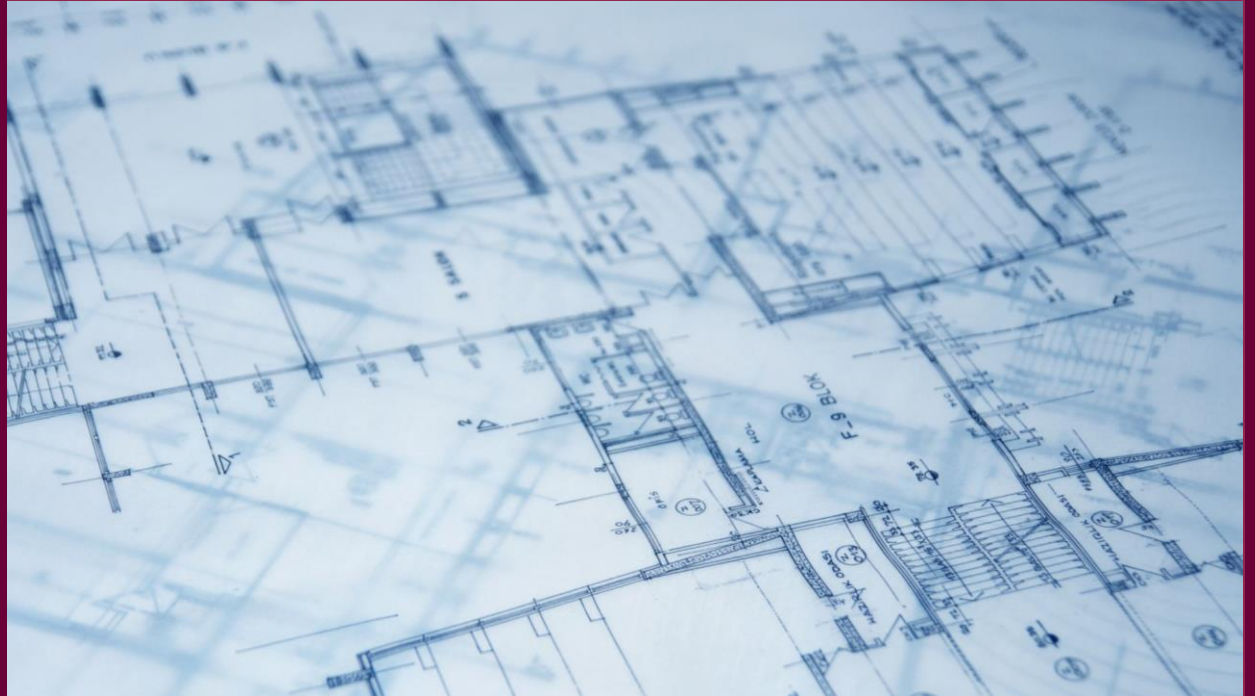


The invisible architect: Technical standardisation shaping EU digital law

Dr. Irene Kamara
Tilburg Law School

UC Chile Conference – InDiCo
Global (EU), 30 July 2025



Tilburg Institute for Law, Technology, and Society/ Tilburg Law School

Assistant Professor and Research coordinator

<https://www.tilburguniversity.edu/staff/i-kamara>

Specific standardisation activities:

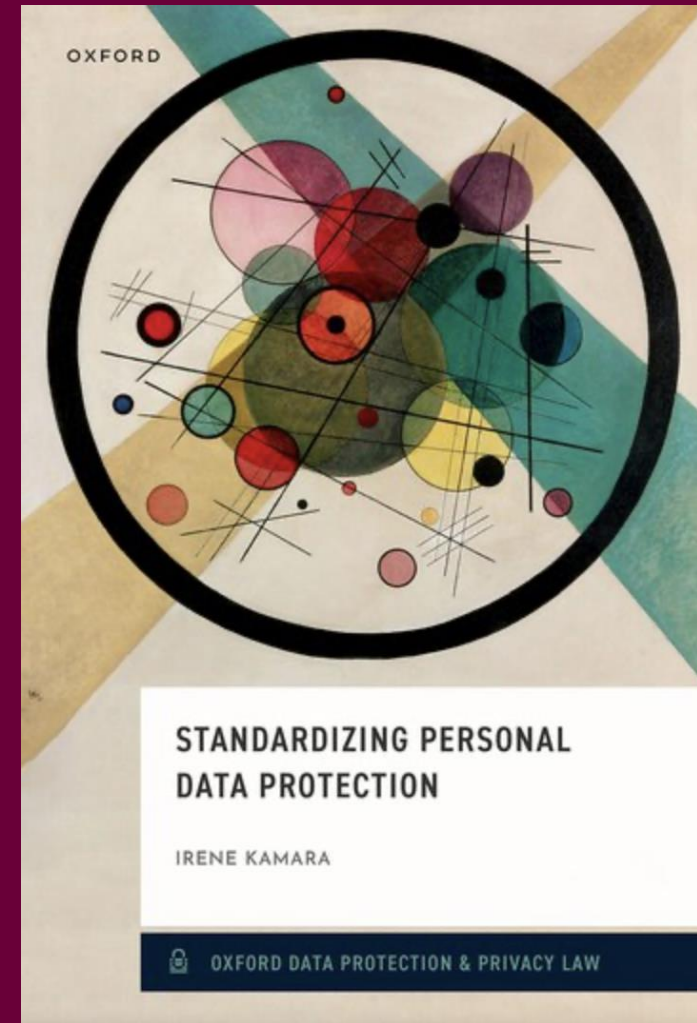
Invited member of NEN TC Cybersecurity & Privacy (2020-2024)

Studies for DG JUST, National Cybersecurity Centre NL, European Cybersecurity Agency ENISA on standards & certification

2021 CEN & CENELEC Standards & Innovation award: Individual researcher

CEN Workshop Agreement on evaluation criteria for security products and systems

Monograph on Technical standardisation & Data protection & Information security



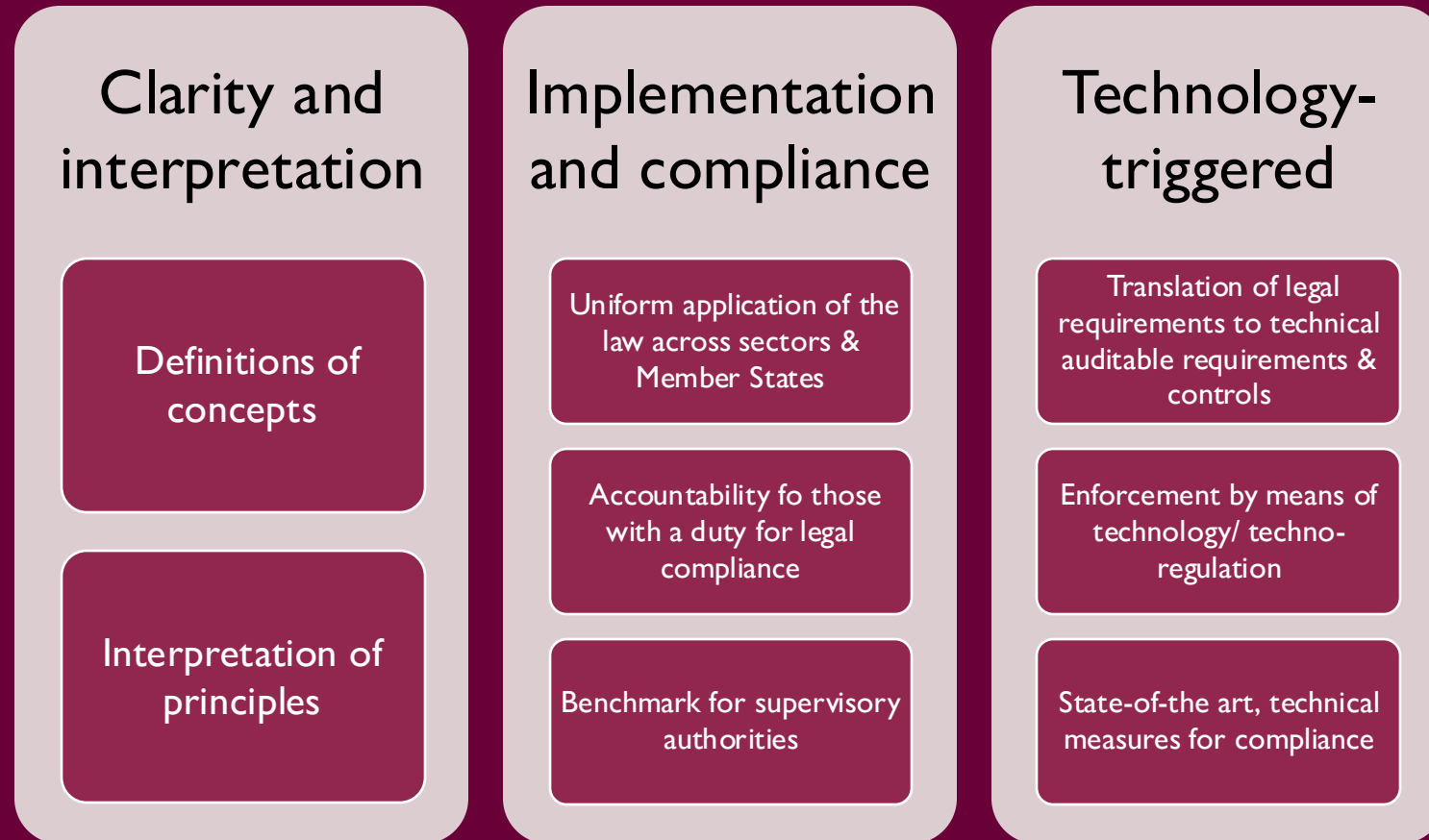
<https://global.oup.com/academic/product/standardizing-personal-data-protection-9780198893288?cc=nl&lang=en&>



What is essentially standardisation?

- Expert knowledge – good practices
- Provides input for empirically informed regulation
- Transnational private regulation (Cafaggi)
- Ecosystem of stakeholders: industry (mainly) but also other actors
- Consensus based process
- In the EU: regulatory technique (Elia Antonio & Cauffman)

What role for technical standards?



Source: I. Kamara, Standardizing Personal Data Protection (2025)

Why a need for compliance guidance?

--> EU digital laws recently..



Table 1: Overview of EU legislation in the digital sector



Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition & Single Market	Media	Finance
Digital Europe Programme Regulation (EU) 2021/694	Recovery and Resilience Facility Regulation (EU) 2021/241	Frequency Bands Directive (EEC) 1987/372	ePrivacy Directive (EC) 2002/58	Database Directive (EC) 1996/9	Regulation for a Cybersecurity Act (EU) 2019/881	Law Enforcement Directive (EU) 2016/680	Toys Regulation (EC) 2009/48, 2023/0290(COD)	Unfair Contract Terms Directive (UCTD) (EEC) 1993/13	EC Merger regulation (EC) 2004/139	Satellite and Cable Directive (EEC) 1993/83	Common VAT system (EC) 2006/112, 2022/0407(CNS), 2022/0409(CNS)
Horizon Europe Regulation (EU) 2021/695, (EU) 2021/764	InvestEU Programme Regulation (EU) 2021/523	Radio Spectrum Decision (EC) 2002/676	European Statistics (EC) 2009/223	Community Design Directive (EC) 2002/6	Regulation to establish a European Cybersecurity Competence Centre (EU) 2021/887	Directive on combating fraud and counterfeiting of non-cash means of payment (EU) 2019/713	European Standardization Regulation (EU) 2012/1025	Price Indication Directive (EC) 1998/6	Technology Transfer Block Exemption (EC) 2014/316	Information Society Directive (EC) 2001/29	Administrative cooperation in the field of taxation (EU) 2011/16
Regulation on a pilot regime distributed ledger technology (EU) 2022/858	Connecting Europe Facility Regulation (EU) 2021/1153	Electromagnetic compatibility Directive (EMC) (EU) 2014/30	General Data Protection Regulation (GDPR) (EU) 2016/679	Enforcement Directive (IPR) (EC) 2004/48	NIS 2 Directive (EU) 2022/2535	Regulation on interoperability between EU information systems in the field of borders and visa (EU) 2019/817	Radio Equipment Directive (RED) (EU) 2014/53	E-commerce Directive (EC) 2000/31	Company Law Directive (EU) 2017/1132	Audio-visual Media Services Directive (AVMSD) (EU) 2010/13	Payment Service Directive 2 (PSD2) (EU) 2015/2366, 2023/0209(COD)
European Innovation Act	Regulation on High Performance Computing Joint Undertaking (EU) 2021/1173	Open Internet Access Regulation (EU) 2015/2120	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies (EU) 2018/1725	Protection of trade secrets (Directive) (EU) 2016/943	Cybersecurity Regulation (EU) 2023/2841	Regulation on terrorist content online (EU) 2021/784	eIDAS Regulation (European Digital Identity Framework) (EU) 2014/910	Unfair Commercial Practices Directive (UCPD) (EC) 2005/29	Screening of foreign direct investments Regulation (EU) 2019/452	Portability Regulation (EU) 2017/1128	Digital Operational Resilience Act (DORA Regulation) (EU) 2022/2554
European Research Area Act	Regulation on Joint Undertakings under Horizon Europe (EU) 2021/2085	European Electronic Communications Code Directive (EECC) (EU) 2018/1972	Free flow of non-personal data (Regulation) (EU) 2018/1907	Design Directive (EU) 2024/2823	Cyber Resilience Act (EU) 2024/2847	Temporary CSAM Regulation (EU) 2022/1232, 2022/0155(COD)	Regulation for a Single Digital Gateway (EU) 2018/1724	Directive on Consumer Rights (CRD) (EU) 2011/83	Market Surveillance Regulation (EU) 2019/1020	Satellite and Cable II Directive (EU) 2019/789	Crypto-assets Regulation (MICA) (EU) 2023/1114
	Decision on a path to the Digital Decade (EU) 2022/2481	au top-level domain Regulation (EU) 2019/517	Open Data Directive (PSI) (EU) 2019/1024	Compulsory licensing of patents 2023/0129(COD)	Cyber Solidarity Act (Regulation) (EU) 2025/38	E-evidence Regulation (EU) 2023/1545	General Product Safety Regulation (EU) 2023/988	e-Invoicing Directive (EU) 2014/55	P2B Regulation (EU) 2019/1150	Copyright Directive (EU) 2019/790	Anti-money laundering Regulation (AML) (EU) 2024/1624
	European Chips Act (Regulation) (EU) 2023/1781	Roaming Regulation (EU) 2022/612	Data Governance Act (Regulation) (EU) 2022/868		Information Security Regulation 2022/0084(COD)	Digitalisation of cross-border judicial cooperation (EU) 2023/2844	Machinery Regulation (EU) 2023/1230	Consumer Protection Cooperation Regulation (EU) 2017/2394	Single Market Programme (EU) 2021/690	European Media Freedom Act (EU) 2024/1083	Financial Data Access Regulation 2023/0205(COD)
	Establishing the Strategic Technologies for Europe Platform (STEP) (EU) 2024/795	Union Secure Connectivity Programme (EU) 2023/588	Data Act (Regulation) (EU) 2023/2854		Digital package	Directive on combating violence against women (EU) 2024/1385	AI Act (Regulation) (EU) 2024/1689	Geo-Blocking Regulation (EU) 2018/302	Vertical Block Exemption Regulation (VBER) (EU) 2022/7720		Payment Services Regulation 2023/0210(COD)
	European Critical Raw Materials Act (Regulation) (EU) 2024/1252	Gigabit Infrastructure Act (EU) 2024/1309	Interoperable Europe Act (EU) 2024/903			Directive for combating sexual abuse and child sexual abuse material 2024/0035(COD)	Eco-Design Regulation (EU) 2024/1781	Digital content Directive (EU) 2019/770	Digital Market Act (DMA Regulation) (EU) 2022/1925		Digital Euro 2023/0212(COD)
	Net Zero Industry Act (EU) 2024/1735	Digital Networks Act	Regulation on data collection for short-term rental (EU) 2024/1028			EU Digital Travel application, 2024/0670(COD)	Product Liability Directive (PLD) (EU) 2024/2853	Digital Contracts for Goods Directive (EU) 2019/771	Regulation on distortive foreign subsidies (EU) 2022/2560		Regulation on combating late payment 2023/0323(COD)
	EU Space Act	EU Cloud and AI Development Act	European Health Data Space (Regulation) (EU) 2025/3927					Digital Services Act (DSA Regulation) (EU) 2022/2065	Horizontal Block Exemption Regulations (HBER) (EU) 2023/1066, (EU) 2023/1067		
	Quantum Act		Harmonization of GDPR enforcement procedures 2023/0202(COD)					Political Advertising Regulation (EU) 2024/900	Internal Market Emergency and Resilience Act (EU) 2024/2747		
	European Biotech Act		GreenDatafall					Right to repair Directive (EU) 2024/1799	Platform Work Directive (PWD) (EU) 2024/2831		
	Advanced Materials Act		European Data Union Strategy					Digital Fairness Act	28th regime		
	Circular Economy Act								Revision of directives on Public Procurement		

Colour coding:



Applicable Law
Published in the Official Journal of the EU



In process
Proposal by the Commission entered the legislative process



Planned initiative
Mentioned by the Commission as potential initiative

<https://www.ceps.eu/ceps-publications/a-dataset-of-international-legal-and-policy-instruments-for-the-digital-world/>

For whom?

Regulated entities

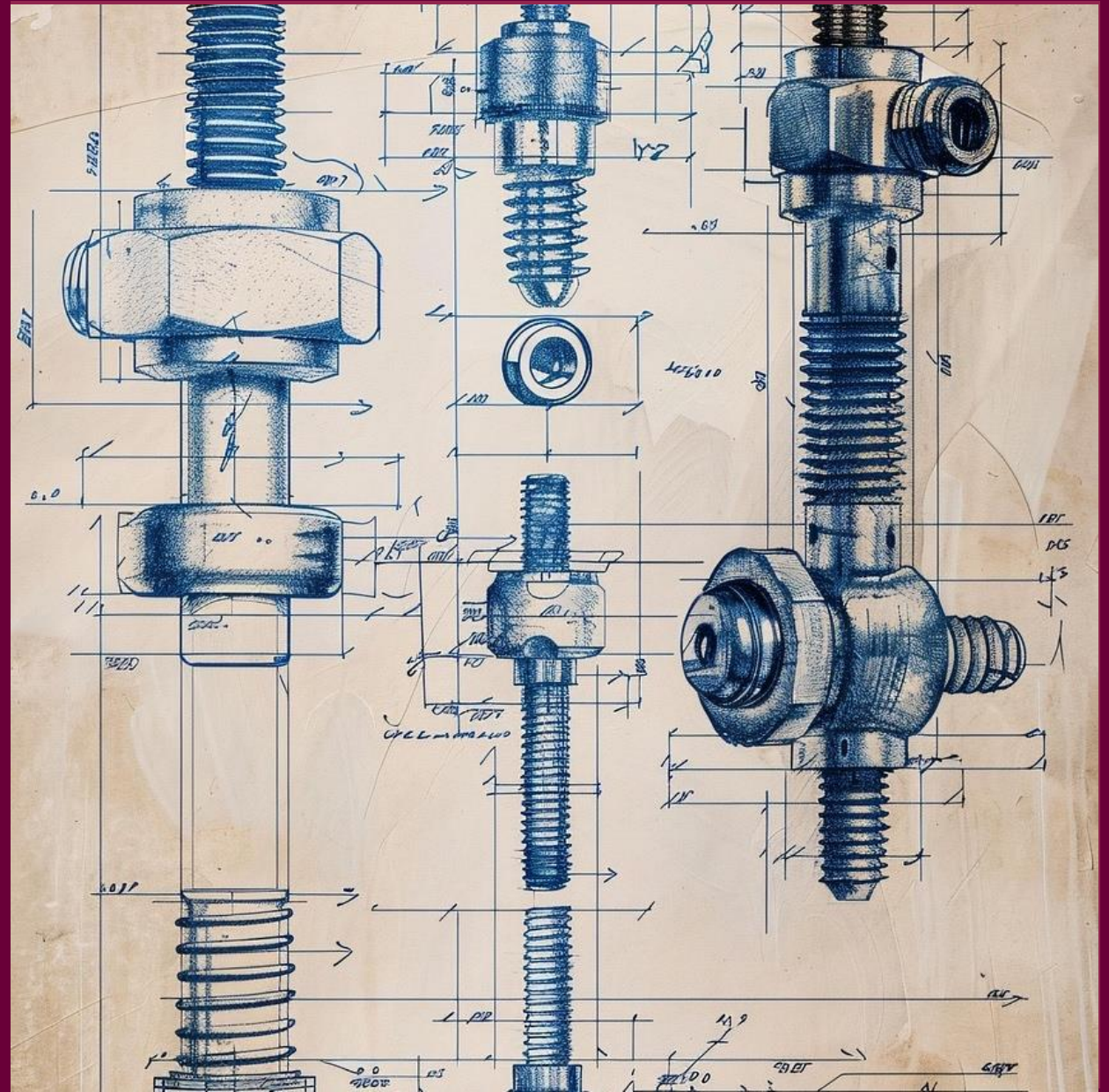
- e.g. data controllers
- AI system providers

Beneficiaries

- Data subjects – e.g. exercise of rights or transparency e.g. privacy icons
- Individuals impacted by non-compliance

Meta-regulation (Parker, Binns)

- The working and implementation of the law itself.



The EU standardisation model: key ingredients



Ingredient 1: need for standard

Who decides which standards support EU law & policy?

- *European Commission -> Annual Union Standardisation Work Program*
- *Priority areas for 2025*

The actions on the digital transition aim to support the following ⁽¹⁾:

- Cybersecurity requirements for products with digital elements (Action 6)
- Online verification of age (Action 7)
- EU Trusted Data Framework (Action 8)
- Interoperability for data processing services (Action 9)
- Secure, interoperable virtual and augmented reality ecosystem and virtual economy (Action 10)
- Support of EU policy on artificial intelligence (Action 11)
- Intermediary digital services (Action 12)
- Data dictionaries in the engineering sector (Action 13)
- EU Digital Identity Wallet (Action 14)
- Digitalisation of construction products information (Action 15)
- Customisation of the media offering in devices and user interfaces (Action 16)
- Local Digital Twins and Smart Cities (Action 17)
- Multimodal and multi-operator ticketing services (Action 18)
- Standards driving quantum technology development and the implementation of Post-Quantum Cryptography protocols (Action 19)

Ingredient 2: the legal basis

NIS 2 Directive

Article 25

Standardisation

1. In order to promote the convergent implementation of Article 21(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European and international standards and technical specifications relevant to the security of network and information systems.
2. ENISA, in cooperation with Member States, and, where appropriate, after consulting relevant stakeholders, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including national standards, which would allow for those areas to be covered.

Cyber Resilience Act

Article 27

Presumption of conformity

1. Products with digital elements and processes put in place by the manufacturer which are in conformity with harmonised standards or parts thereof, the references of which have been published in the *Official Journal of the European Union*, shall be presumed to be in conformity with the essential cybersecurity requirements set out in Annex I covered by those standards or parts thereof.

The Commission shall, in accordance with Article 10(1) of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards for the essential cybersecurity requirements set out in Annex I to this Regulation. When preparing standardisation requests for this Regulation, the Commission shall strive to take into account existing European and international standards for cybersecurity that are in place or under development in order to simplify the development of harmonised standards, in accordance with Regulation (EU) No 1025/2012.

AI Act

Article 40

Harmonised standards and standardisation deliverables

1. High-risk AI systems or general-purpose AI models which are in conformity with harmonised standards or parts thereof the references of which have been published in the *Official Journal of the European Union* in accordance with Regulation (EU) No 1025/2012 shall be presumed to be in conformity with the requirements set out in Section 2 of this Chapter or, as applicable, with the obligations set out in of Chapter V, Sections 2 and 3, of this Regulation, to the extent that those standards cover those requirements or obligations.

Data Act

Article 36

Essential requirements regarding smart contracts for executing data sharing agreements

4. A smart contract that meets the harmonised standards or the relevant parts thereof, the references of which are published in the *Official Journal of the European Union*, shall be presumed to be in conformity with the essential requirements laid down in paragraph 1 to the extent that those requirements are covered by such harmonised standards or parts thereof.
5. The Commission shall, pursuant to Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements laid down in paragraph 1 of this Article.

Ingredient 2 but different



General Data Protection Regulation: no legal basis for technical standards



However --> COM has the power to issue standardisation requests based on (general) **Standardisation Regulation 1025/2012**



Practically – also standardisation request and development by European Standardisation Organisations, but NO publication in OJ or presumption of conformity with the law

Ingredient 3: standardisation request

- AI ACT basis for standardisation request: C(2023)3215

Article 1

Requested standardisation activities

The European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC) are requested to draft the new European standards or European standardisation deliverables, as listed in Annex I, in support of Union policy on artificial intelligence by 30 April 2025.

The European standards or European standardisation deliverables referred to in paragraph 1 shall meet the requirements set out in Annex II.

ANNEX I

List of new European Standards and European standardisation deliverables to be drafted

Reference information	
1.	European standard(s) and/or European standardisation deliverable(s) on risk management systems for AI systems
2.	European standard(s) and/or European standardisation deliverable(s) on governance and quality of datasets used to build AI systems
3.	European standard(s) and/or European standardisation deliverable(s) on record keeping through logging capabilities by AI systems
4.	European standard(s) and/or European standardisation deliverable(s) on transparency and information provisions for users of AI systems
5.	European standard(s) and/or European standardisation deliverable(s) on human oversight of AI systems
6.	European standard(s) and/or European standardisation deliverable(s) on accuracy specifications for AI systems
7.	European standard(s) and/or European standardisation deliverable(s) on robustness specifications for AI systems
8.	European standard(s) and/or European standardisation deliverable(s) on cybersecurity

Ingredient 4: Technical committees carry out the requests

- **On Cyber: CEN-CLC/JTC 13 AND ETSI TC Cyber**
 - All 3 European Stand. Orgs (ESOs)

prEN XXX (WI=JT013089)

Cybersecurity requirements for products with digital elements - Principles for cyber resilience

prEN XXX (WI=JT013091)

Cybersecurity requirements for products with digital elements – Generic Security Requirements

prEN XXX (WI=JT013031)

Managed Security Services Providers Requirements

On AI: CEN-CENELEC JTC 21

2 ESOs

Project reference

EN ISO/IEC 22989:2023/prA1 (WI=JT021031)

Information technology — Artificial intelligence — Artificial intelligence concepts and terminology — Amendment 1

EN ISO/IEC 23053:2023/prA1 (WI=JT021032)

Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) — Amendment 1

prCEN/CLC/TR XXX (WI=JT021009)

AI Risks - Check List for AI Risks Management

prCEN/CLC/TR XXX (WI=JT021026)

Impact assessment in the context of the EU Fundamental Rights

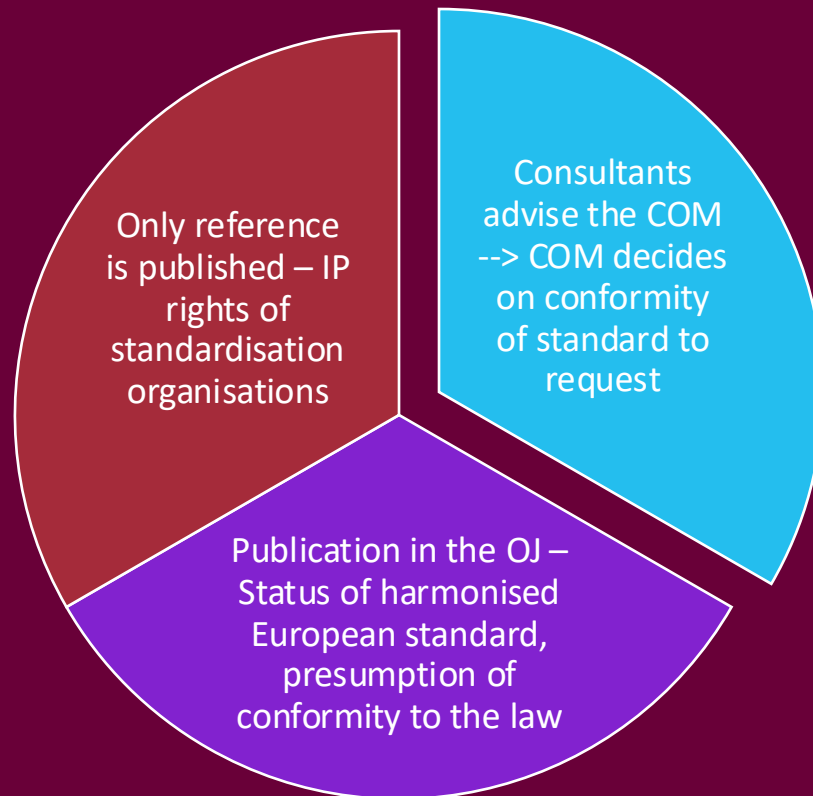
prCEN/TS (WI=JT021035)

Sustainable Artificial Intelligence – Guidelines and metrics for the environmental impact of artificial intelligence systems and services

prCEN/TS (WI=JT021034)

Guidelines on tools for handling ethical issues in AI system life cycle

Ingredient 5: assessment & publication



ANNEX I

PART ONE

A-TYPE STANDARDS

1. Explanatory note.

A-type standards specify basic concepts, terminology and design principles applicable to all categories of machinery. Application of such standards alone, although providing an essential framework for the correct application of the Machinery Directive, is not sufficient to ensure conformity with the relevant essential health and safety requirements of the Directive and therefore does not give a full presumption of conformity.

2. List of references of standards.

1.	EN 1127-2:2014 Explosive atmospheres - Explosion prevention and protection - Part 2: Basic concepts and methodology for mining
2.	EN ISO 12100:2010 Safety of machinery - General principles for design - Risk assessment and risk reduction (ISO 12100:2010)

Legitimacy issues

01

WHO PARTICIPATES IN
THE TECHNICAL
COMMITTEES?

02

ARE CIVIL RIGHTS AND
CONSUMER
ORGANISATIONS WELL
REPRESENTED?

03

ARE THE PROCEDURES
OPEN AND
TRANSPARENT?

04

STANDARDS ARE
PART OF EU LAW,
BUT ACCESSIBLE
FOR A FEE

05

HOW
THOROUGHLY IS
THE QUALITY OF THE
ADOPTED STANDARDS
ASSESSED?

Thank you

[Contact me at: I.kamara@tilburguniversity.edu](mailto:I.kamara@tilburguniversity.edu)