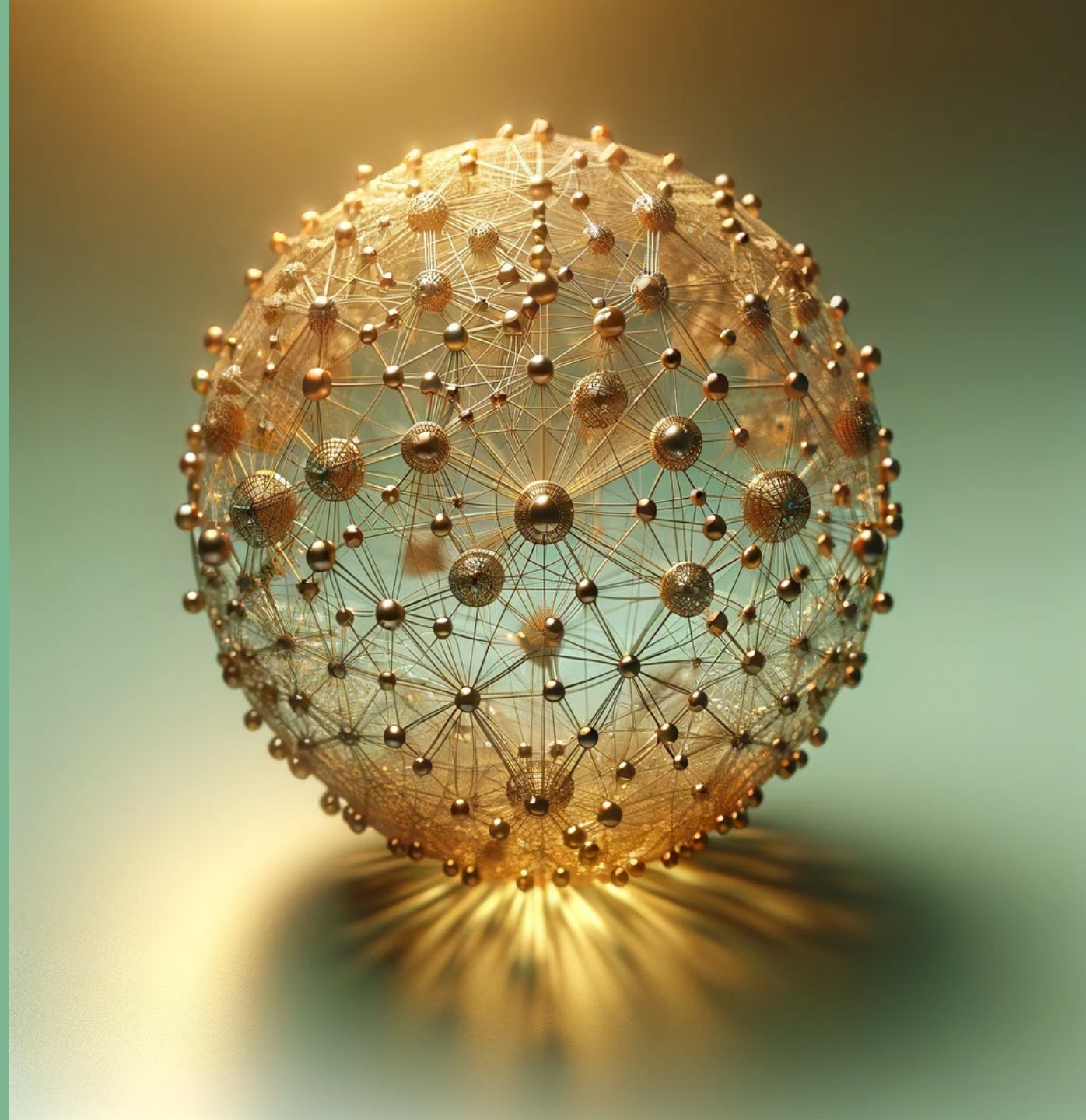
The EU AI Act

Legal Analysis and Implications from a Swiss Perspective

CSA SIGS Special Event

Martina Arioli, Arioli Law
10. April 2024

ariolilaw



OECD AI Principles

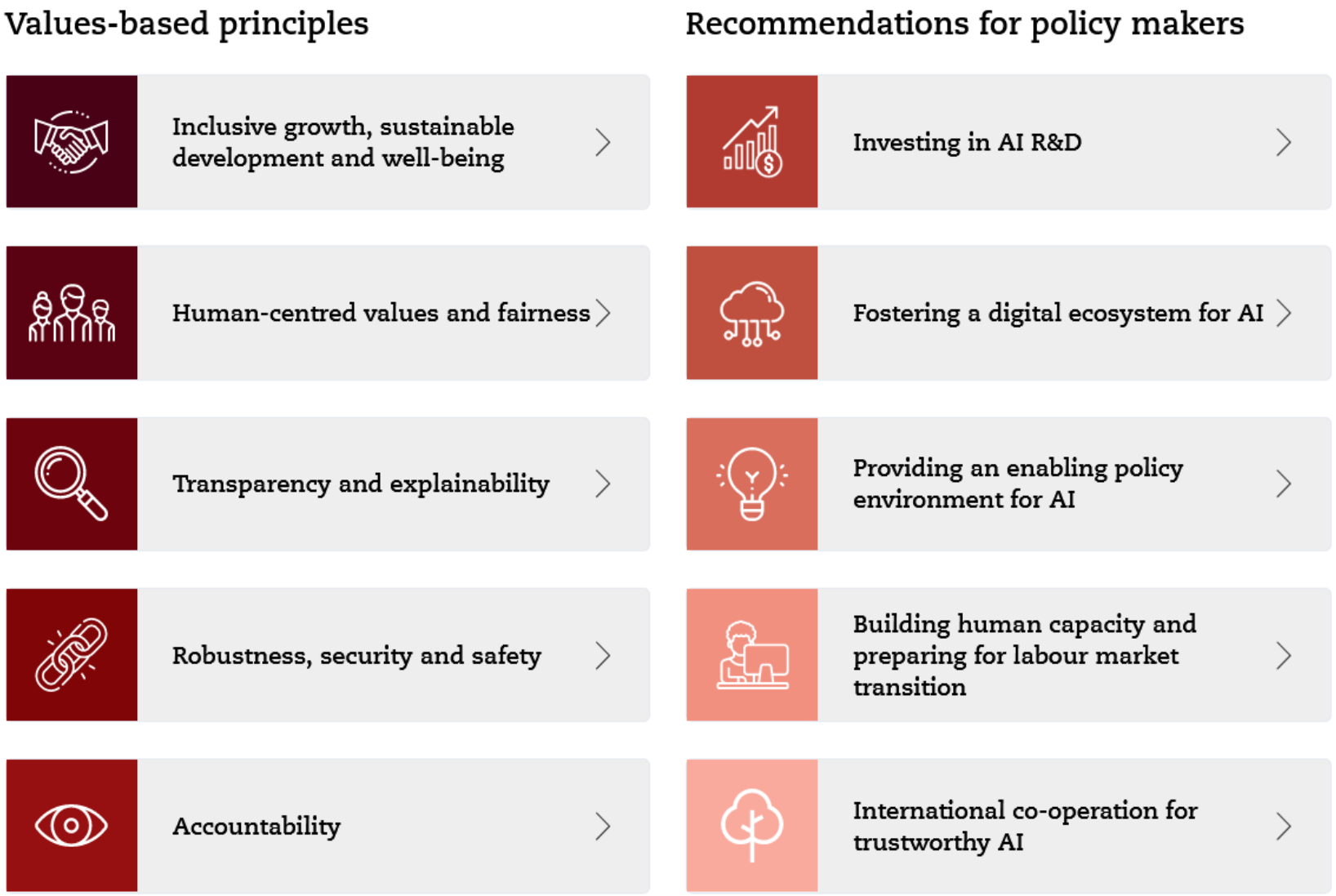
The OECD AI Principles promote use of AI that is innovative and trustworthy and that respects human rights and democratic values.

Adopted in **May 2019**, they set **standards** for AI that are practical and flexible enough to stand the test of time.

https://oecd.ai/en/ai-principles

According to the OECD there are currently **1000 AI policy initiatives** from **69** countries, territories and the EU.

https://oecd.ai



Global AI Law and Policy Tracker

iapp.org

- Argentina
- Australia
- Bangladesh
- Brazil
- Canada
- Chile China
- Colombia
- Egypt
- EU
- India
- Indonesia
- Israel
- Japan
- Mauritius
- New Zealand
- Peru
- Saudi Arabia
- Singapore
- South Korea
- Taiwan
- United Arab Emirates
- U.K.
- U.S.

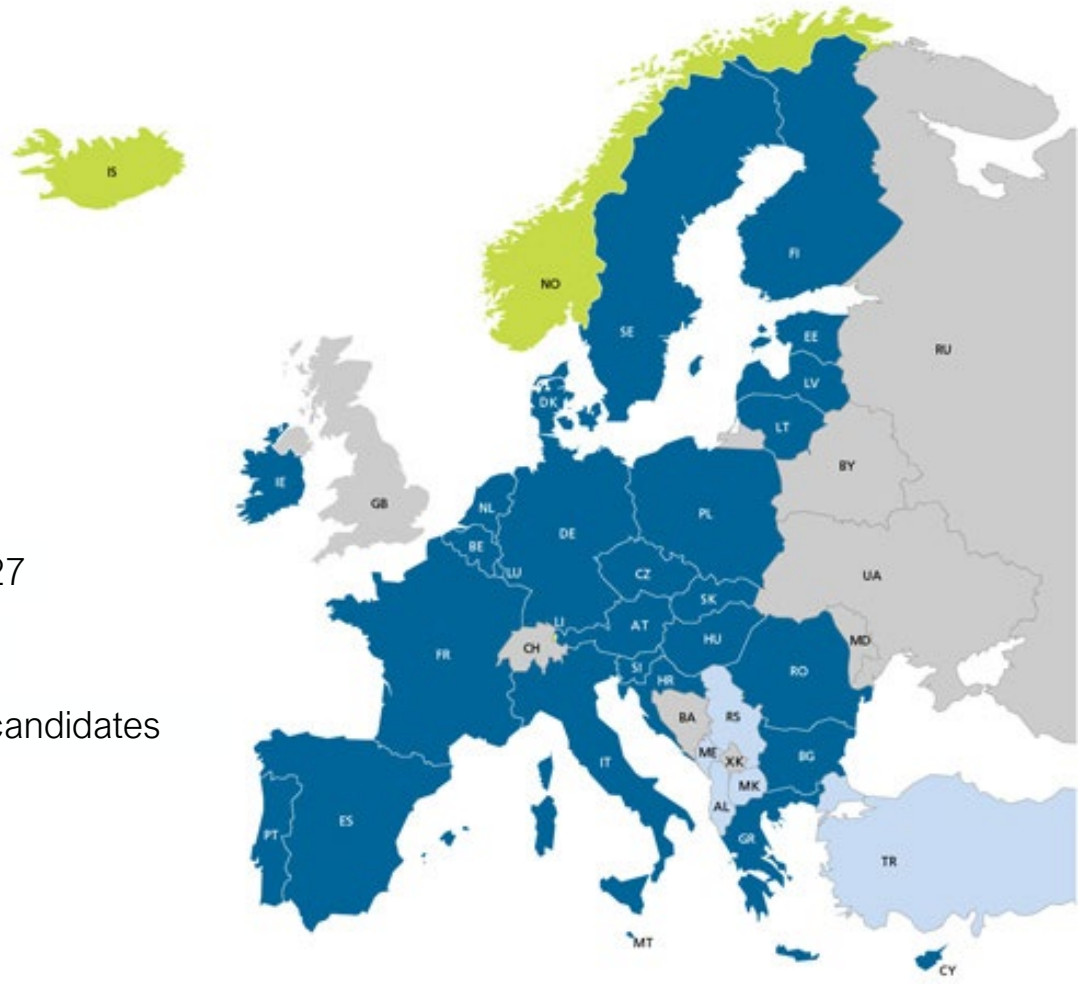
Scope and Applicability of the EU AI Act

The AI Act applies to anyone who:

- puts an AI system on the EU market,
- uses and AI System in the EU,
- uses a system to generate outputs, and these outputs are used in the EU.

➢ extraterritorial effect: AI Act is applicable if services are used within the EU market, regardless of where the company is established

- Obligations primarily on "**providers**", but also on "**deployers**" - both private *and* public actors.
- Costs of regulatory burden are considerable:
- *Not applicable to private users!*



What is an AI system?

"**AI system**" is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

⇒ An AI System is always software, but not every software is an AI System

⇒ Embedded or stand-alone

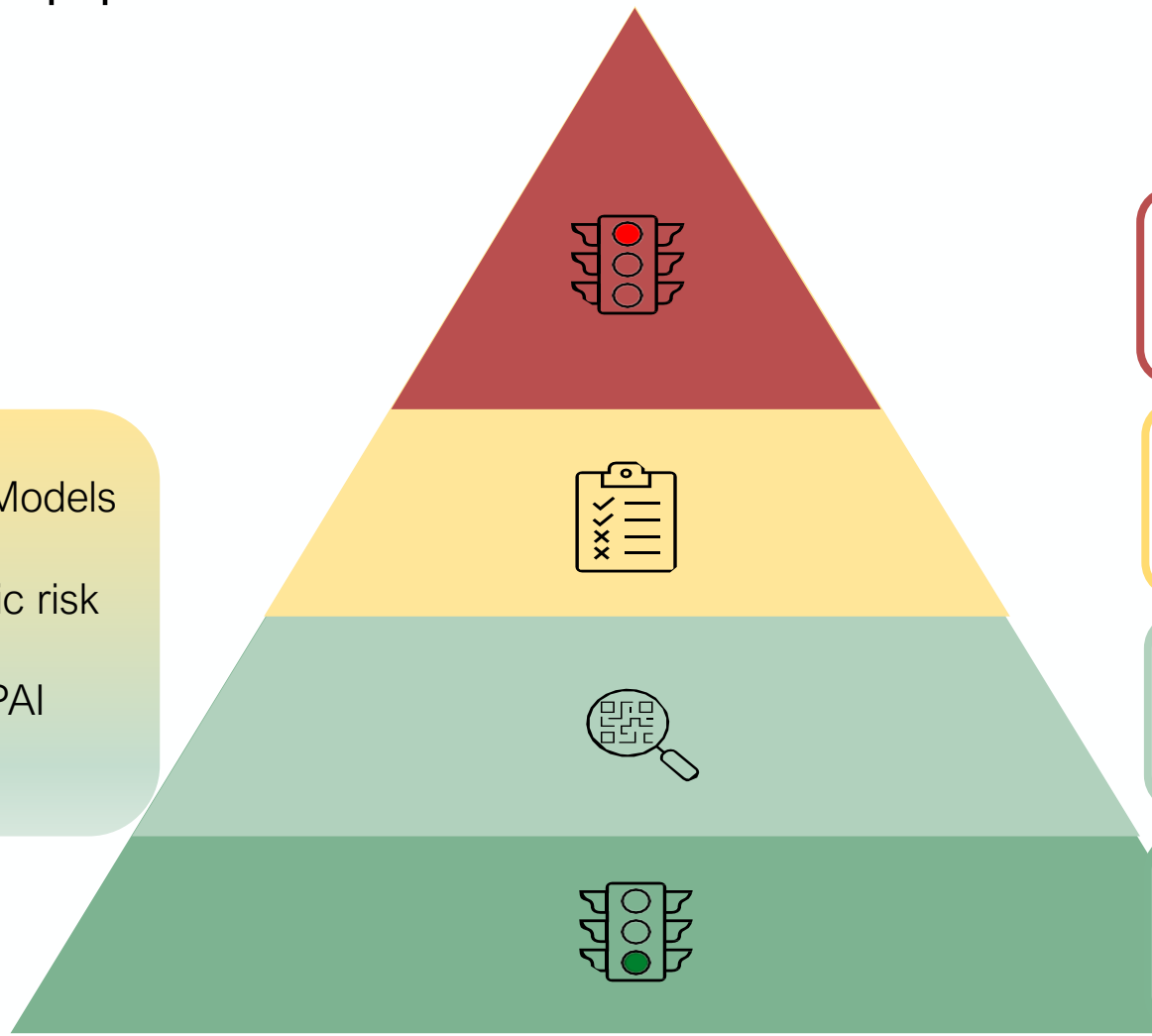
⇒ *Anything* can be an AI System, even if just partially automated (apart from very simple statistical or text editing tools), will (most likely) be an "AI system".

⇒ The EU Commission will issue Guidelines

Risk-Based Approach to the AI Act

General Purpose AI Models

- GPAI with systemic risk
- Standard GPAI
- Open licensed GPAI



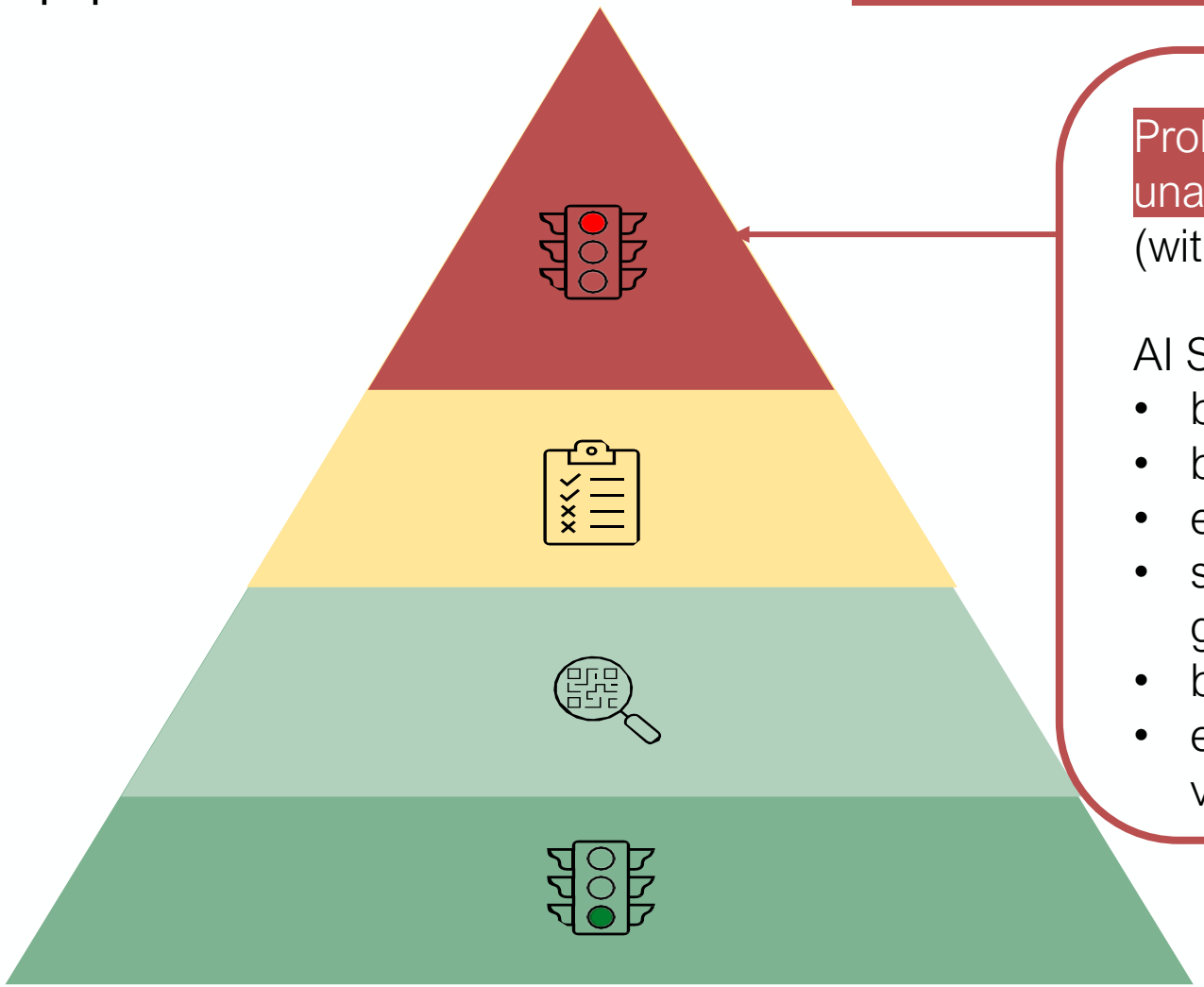
UNACCEPTABLE RISK:
Prohibited (with exceptions)

HIGH RISK:
Comprehensive compliance requirements

LIMITED RISK:
Limited obligations: transparency towards end users, Code of Conduct

MINIMAL RISK:
Minimal obligations, Code of Conduct

Risk-Based Approach of the AI Act: Prohibited AI

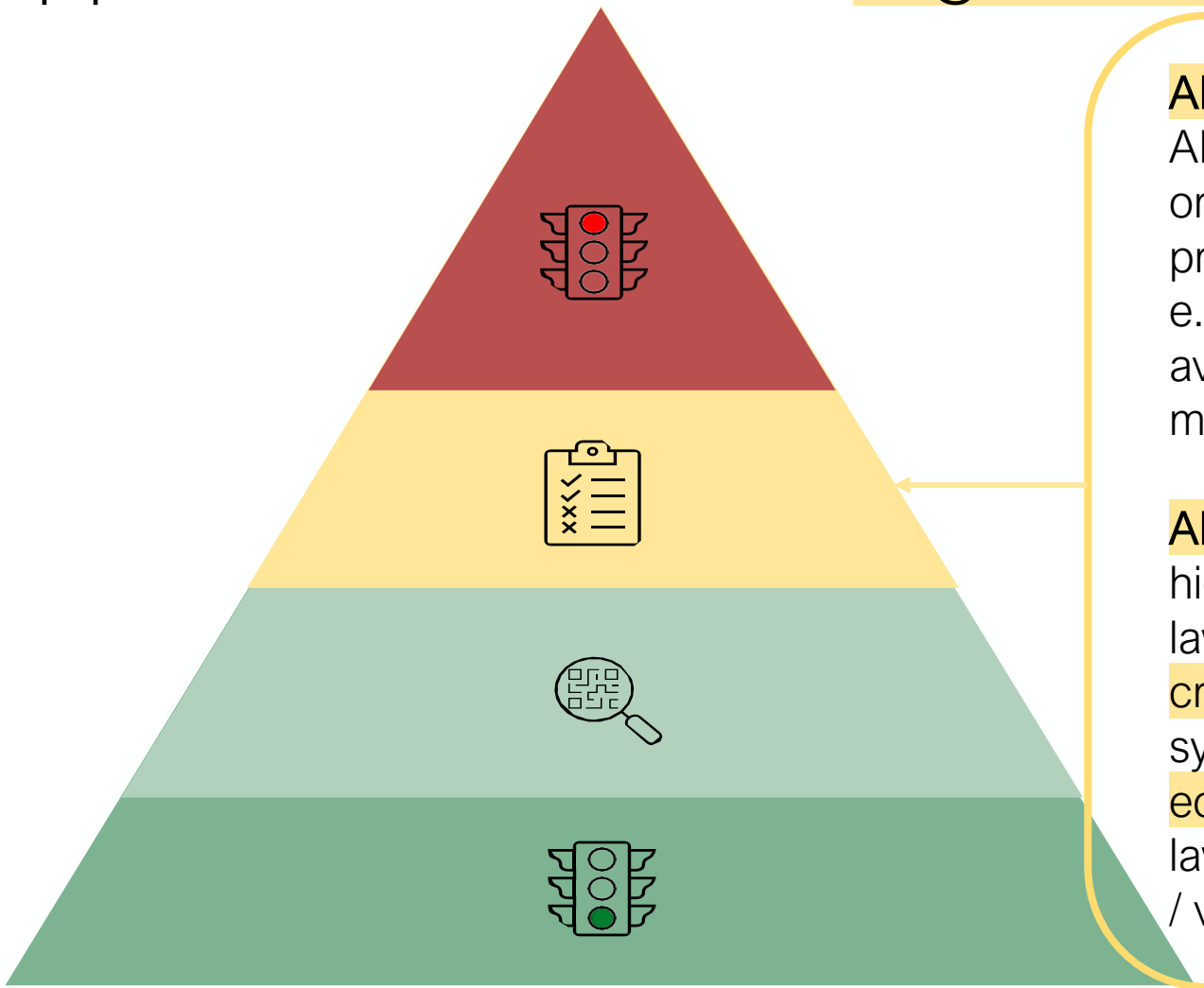


Prohibited due to unacceptable risk
(with exceptions)

AI Systems used for:

- biometric identifications
- biometric categorization
- emotion recognition
- social scoring by governments
- behavioural manipulation
- exploitation of vulnerabilities of children

Risk-Based Approach of the AI Act: High-Risk AI



ANNEX II:
AI systems used as a product or security component of a product **in regulated industries**: e.g. medical devices, civil aviation, vehicle security, marine equipment

ANNEX III:
high-risk areas of application: law enforcement, employment, credit scoring, other biometric systems, critical infrastructure, education, justice, immigration, law enforcement and elections / voting.

Provider - Deployer

Provider = "a natural or legal person public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge..."

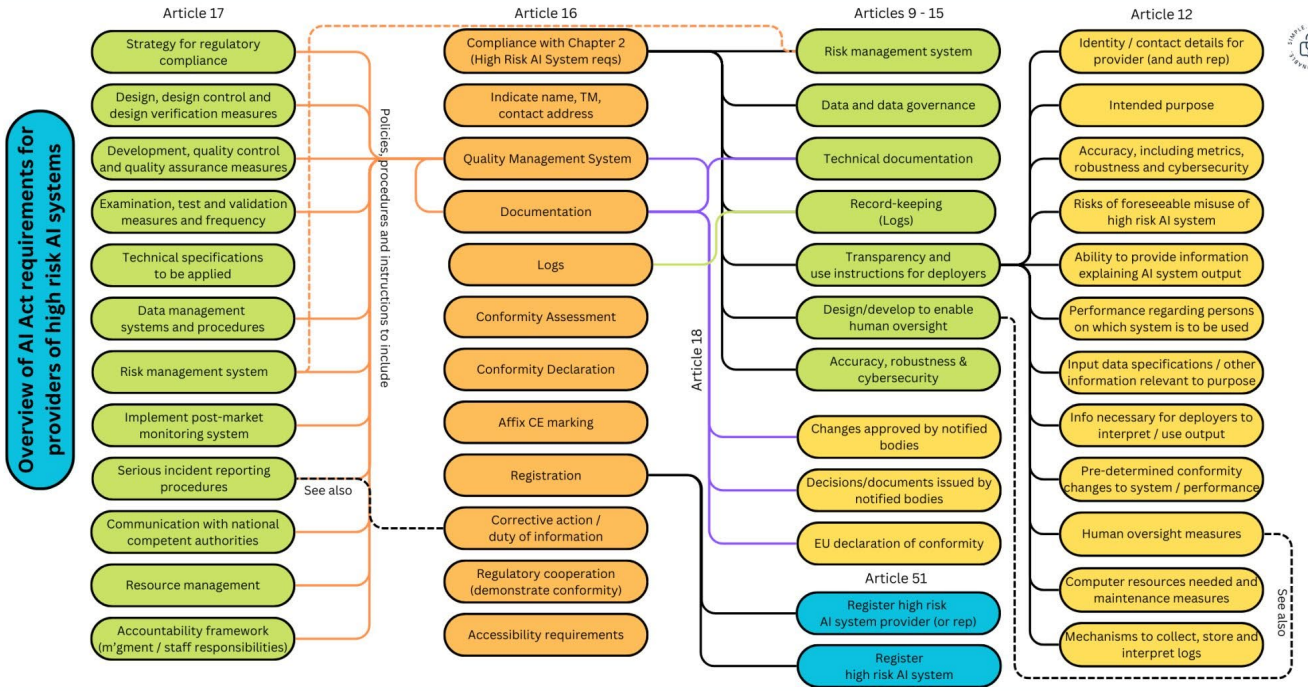
Deployer = "a natural or legal person, public authority, agency or other body using an AI system *except where the AI system is used in the course of a personal non-professional activity.*"

However, the deployer, distributor, importer *becomes* a provider of a high-risk AI system if:

- the use goes beyond the intended purpose
- Substantial changes are made
- the AI System is marketed under the deployers name.
- if you integrate a GPAI model with systemic risk through an API and make further modifications to it.

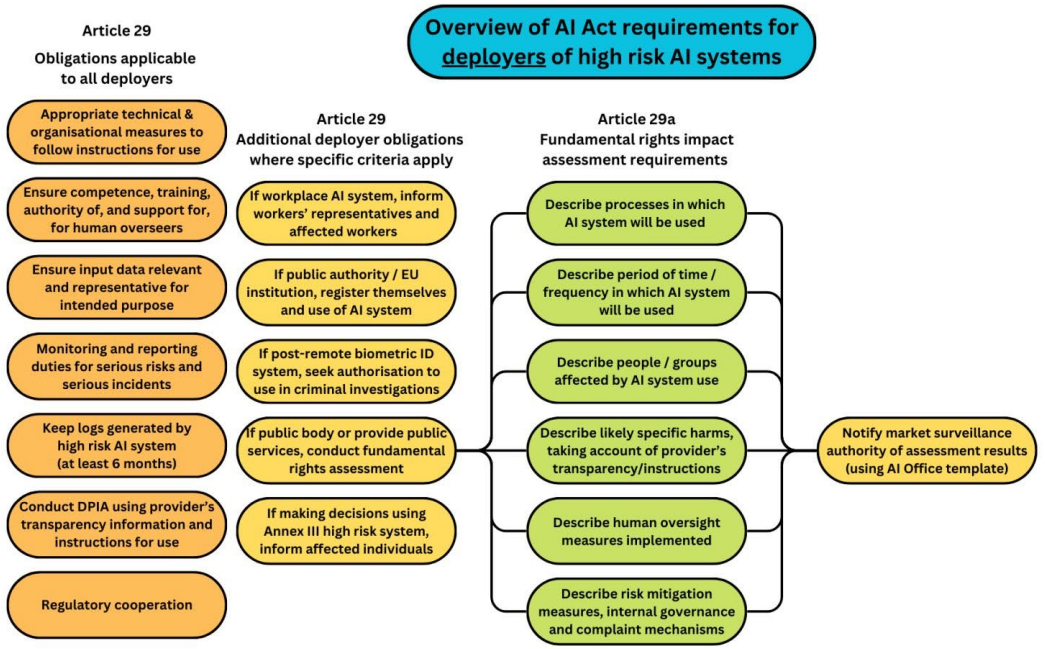
High-Risk AI System – Provider Obligations: an overview

- Risk management system + quality management system
- Quality of datasets
- Comprehensive technical documentation
- Automatic event recording
- Transparency
- Effective oversight by a natural person
- Accuracy, robustness, and cybersecurity
- Obtain conformity assessment and affix the CE mark
- Indicate provider's name and contact details on the AI system
- Maintain technical documentation and logs



High-Risk AI System – Deployer Obligations: an overview

- Ensure systems are used in accordance with accompanying instructions
- Assign human oversight
- Ensure input data is relevant and representative
- Monitor the AI system and reporting obligations
- Retain logs
- Transparency
- Conduct Data Protection Impact Assessment
- Conduct Fundamental Rights Impact Assessment



What is a General Purpose AI model?

'**general purpose AI model**' means an **AI model**, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications. *This does not cover AI models that are used before release on the market for research, development and prototyping activities*

⇒ GPAI = Generative AI and LLM

General Purpose AI Models

1. **“Systemically risky” GPAI (**FLOP-Threshold of more than 10^25 based upon assumption that higher computational resources indicate more sophisticated models)
    1. fulfil **standard obligations**
    2. conduct model evaluations
    3. including adversarial testing (red teaming)
    4. assess and mitigate risks
    5. document and report incidents to the AI Office
    6. maintain adequate cybersecurity protection

2. **Standard GPAI:** detailed **technical and informational documentation** to enable downstream users to comprehend their capabilities and limitations, **intellectual property law adherence** (e.g., copyright Directive), and **transparency about training data**

3. **Open licensed GPAI with publicly accessible parameters and architecture**: technical documentation requirements

When will the AI Act take effect?

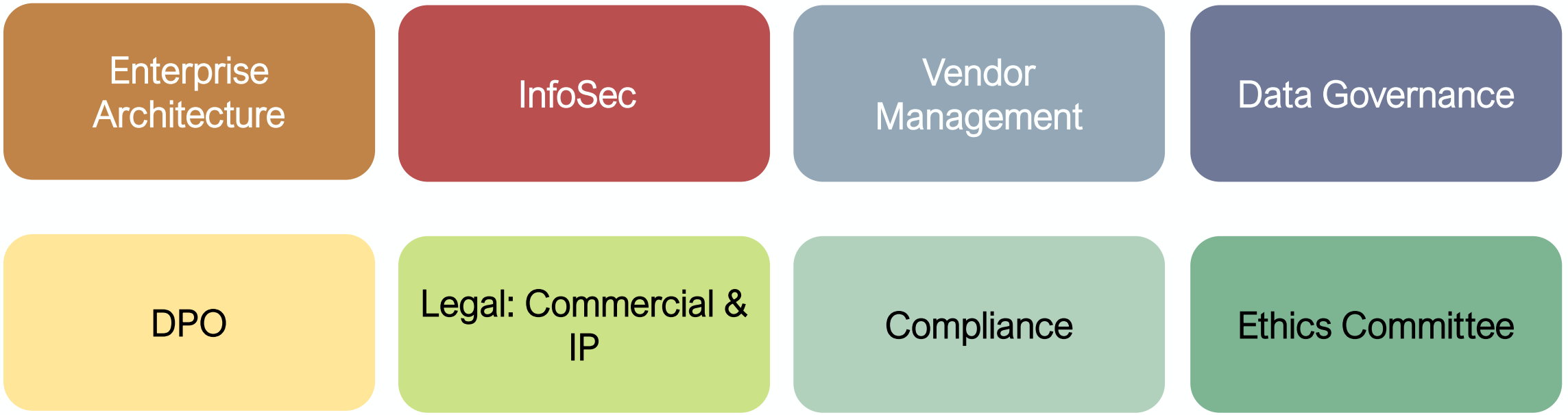
The AI Act shall apply from 24 months following the entry into force.

However:

1. the **general provisions** reflecting i.a. the EU Principles on AI apply within 6 months after entry into force
2. the **prohibition** on AI systems according to Titel II Art. 5 and Annex I apply within 6 months after entry into force
3. Title III Chapter 4 [**notifying authorities**], Title VI [**transparency obligations for providers and deployers of certain AI Systems**], Title VIIIa [**GPAI**], Title X [**Penalties**] apply within 12 months after entry into force
4. Article 6(1) [**high-risk AI systems**] and the corresponding obligations in this Regulation apply within 36 months after entry into force
5. Codes of practices shall be ready at the latest 9 months after the entry into force of this

- For existing GPAIs on the market when the AI Act rules are applied, this transition period is extended to 24 months (Art. 83(3) AIA).
- And yes, there are of course sanctions in case of violation: depending on violation up to EUR 35m or 7% of global annual turnover

AI Compliance is a team effort



Digitization in the EU: a regulatory flood

More than 100 Regulations and Directives on EU level are related to digitization!

i.a.:

- Data Act
- Digital Services Act
- Digital Market Act
- AI Act
- DORA
- NIS 2 Directive
- Cyber Resilience Act

Legislation Tracker: https://apps.fliplet.com/taylor-wessing-digital-legislation-tracker/all-legislation-rgt5?

Table 1: Overview of EU Legislations in the Digital Sector

Applicable law	Published in the Official Journal of the European Union
In negotation	Proposal by the European Commission entered the legislative process.
Planed initiative	Mentioned by the European Commission as potential legislative initiative

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Media	Finance
Digital Europe Programme Regulation, (EU) 2021/694	Recovery and Resilience Facility Regulation, (EU) 2021/241	Frequency Bands Directive, (EEC) 1987/372	European Statistics, (EC) 2009/223, 2023/0237(COD)	Database Directive, (EC) 1996/9	Regulation for a Cybersecurity Act, (EU) 2019/881 2023/0108(COD)	Law Enforcement Directive, (EU) 2016/680	Product Liability Directive (PLD), (EEC) 1985/374, 2022/0302(COD)	Unfair Contract Terms Directive (UCTD), (EEC) 1993/13	EC Merger regulation, (EC) 2004/139, update soon	Satellite and Cable I Directive, (EEC) 1993/83	Common VAT system, (EC) 2006/112, 2022/0407(CNS)
Horizon Europe Regulation, (EU) 2021/695, (EU) 2021/764	InvestEU Programme Regulation, (EU) 2021/523	Radio Spectrum Decision, (EC) 2002/676	General Data Protection Regulation (GDPR), (EU) 2016/679	Community Design Directive, (EC) 2002/6, 2022/0391(COD)	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	Toys Regulation, (EC) 2009/48, 2023/0290(COD)	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 tech. market, (EU) 2022/858	Connecting Europe Facility Regulation, (EU) 2021/1153	Broadband Cost Reduction Directive, (EU) 2014/61, 2023/0046(COD)	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, (EU) 2018/1725	Enforcement Directive (IPR), (EC) 2004/48	NIS 2 Directive, (EU) 2022/2555	Regulation on interoperability between EU information systems in the field of borders and visa, (EU) 2019/817	European Standardization Regulation, (EU) 2012/1026	E-commerce Directive, (EC) 2000/31	Company Law Directive, (EU) 2017/1132, 2023/0089(COD)	Audio-visual Media Services Directive (AVMSD), (EU) 2010/13	Payment Service Directive 2 (PSD2), (EU) 2015/2366 2023/0209(COD)
	Regulation on High Performance Computing Joint Undertaking, (EU) 2021/1173	Open Internet Access Regulation, (EU) 2015/2120	Regulation on the free flow of non-personal data, (EU) 2018/1807	Directive on the protection of trade secrets, (EU) 2016/943	Information Security Regulation, 2022/0084(COD)	Regulation on terrorist content online, (EU) 2021/784	eIDAS Regulation, (EU) 2014/910, 2021/0136(COD)	Unfair Commercial Practices Directive (UCPD), (EC) 2005/29	Market Surveillance Regulation, (EU) 2019/1020	Portability Regulation, (EU) 2017/1128	Digital Operational Resilience Act (DORA Regulation), (EU) 2022/2554
	Regulation on Joint Undertakings under Horizon Europe, (EU) 2021/2085, 2022/0033(NLE)	European Electronic Communications Code Directive (EECC), (EU) 2018/1972	Open Data Directive (PSI), (EU) 2019/1024	Design Directive, 2022/0392(COD)	Cybersecurity Regulation, 2022/0085(COD)	Temporary CSAM Regulation, (EU) 2021/1232, 2022/0155(COD)	Radio Equipment Directive (RED), (EU) 2014/53	Directive on Consumer Rights (CRD), (EU) 2011/83, 2022/0147(COD)	P2B Regulation, (EU) 2019/1150	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	.eu top-level domain Regulation, (EU) 2019/517	Data Governance Act (DGA Regulation), (EU) 2022/868	Compulsory licensing of patents, 2023/0129(COD)	Cyber Resilience Act, 2022/0272(COD)	E-evidence Regulation, (EU) 2023/1543	Regulation for a Single Digital Gateway, (EU) 2018/1724	e-invoicing Directive, (EU) 2014/55	Single Market Programme, (EU) 2021/690	Copyright Directive, (EU) 2019/790	Financial Data Access Regulation, 2023/0205 (COD)
	European Chips Act (Regulation), (EU) 2023/1781	Roaming Regulation, (EU) 2022/612	ePrivacy Regulation, 2017/0003(COD)	Standard essential patents, 2023/0133(COD)	Cyber Solidarity Act (Regulation), 2023/0109(COD)	Directive on combating violence gainst women, 2022/0066(COD)	General Product Safety Regulation, (EU) 2023/988	Geo-Blocking Regulation, (EU) 2018/302	Vertical Block Exemption Regulation (VBER), (EU) 2022/720	European Media Freedom Act, 2022/0277(COD)	Payment Services Regulation, 2023/0210(COD)
	European critical raw materials act (Regulation), 2023/0079(COD)	Regulation on the Union Secure Connectivity Programme, (EU) 2023/588	European Data Act (Regulation), 2022/0047(COD)			Digitalization of travel documents	Machinery Regulation, (EU) 2023/1230	Regulation on cooperation for the enforcement of consumer protection laws, (EU) 2017/2394	Digital Market Act (DMA Regulation), (EU) 2022/1925	Remuneration of musicians from third countries for recorded music played in the EU	Digital euro, 2023/0212 (COD)
	Net Zero Industry Act, 2023/0081(COD)	New radio spectrum policy programme (RSPP 2.0)	European Health Data Space (Regulation), 2022/0140(COD)				AI Act (Regulation), 2021/0106(COD)	Digital content Directive, (EU) 2019/770	Regulation on distortive foreign subsidies, (EU) 2022/2560		Regulation on combating late payment, 2023/0323(COD)
	Establishing the Strategic Technologies for Europe Platform (STEP), 2023/0199(COD)	Digital Networks Act	Regulation on data collection for short-term rental, 2022/0358(COD)				Eco-design Regulation, 2022/0095(COD)	Directive on certain aspects concerning contracts for the sale of goods, (EU) 2019/771	Horizontal Block Exemption Regulations (HBER), (EU) 2023/1066, (EU) 2022/1067		
	EU Space Law		Interoperable Europe Act, 2022/0379(COD)				AI Liability Directive, 2022/0303(COD)	Digital Services Act (DSA Regulation), (EU) 2022/2065	Platform Work Directive, 2021/0414(COD)		
	Initiative to open up European supercomputer capacity to AI start-ups		Harmonization of GDPR enforcement 2023/0202(COD)					Political Advertising Regulation, 2021/0381(COD)	Single Market Emergency Instrument (SMEI), 2022/0278(COD)		
			Access to vehicle data, functions and resources					Right to repair Directive, 2023/0083(COD)			
			GreenData4all					Multimodal digital mobility services (MDMS)			
								Consumer protection: strengthened enforcement cooperation			

kaizenner.eu

bruegel

https://www.kaizenner.eu/

ariolilaw

Hornbachstrasse 22, 8008 Zürich

+41 44 201 66 11

martina.arioli@arioli-law.ch | www.arioli-law.ch