L2B PARTNERS STUDIO LEGALE

- THE EUROPEAN AI ACT -

LAW & DATA – Università degli Studi di Padova

Padua, 15° January 2025

Cosetta Masi
Avvocato, LL.M. – Partner L2B Studio Legale

L2B PARTNERS STUDIO LEGALE

AGENDA

- Reasons that brought to the AI Act?
- Subject matter and scope of application
- Prohibited AI practices
- High-Risk AI systems: definition
- High-Risk AI systems: requirements
- Next steps
- Take-aways

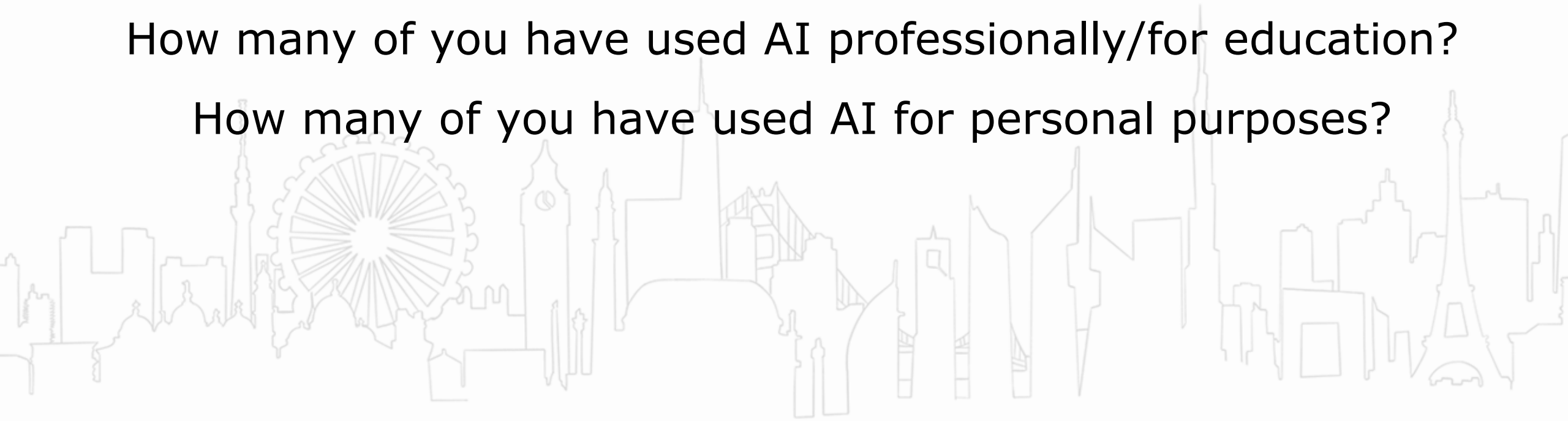
L2B PARTNERS STUDIO LEGALE

AGENDA

How many of you have heard of the AI Act before?

How many of you have used AI professionally/for education?

How many of you have used AI for personal purposes?

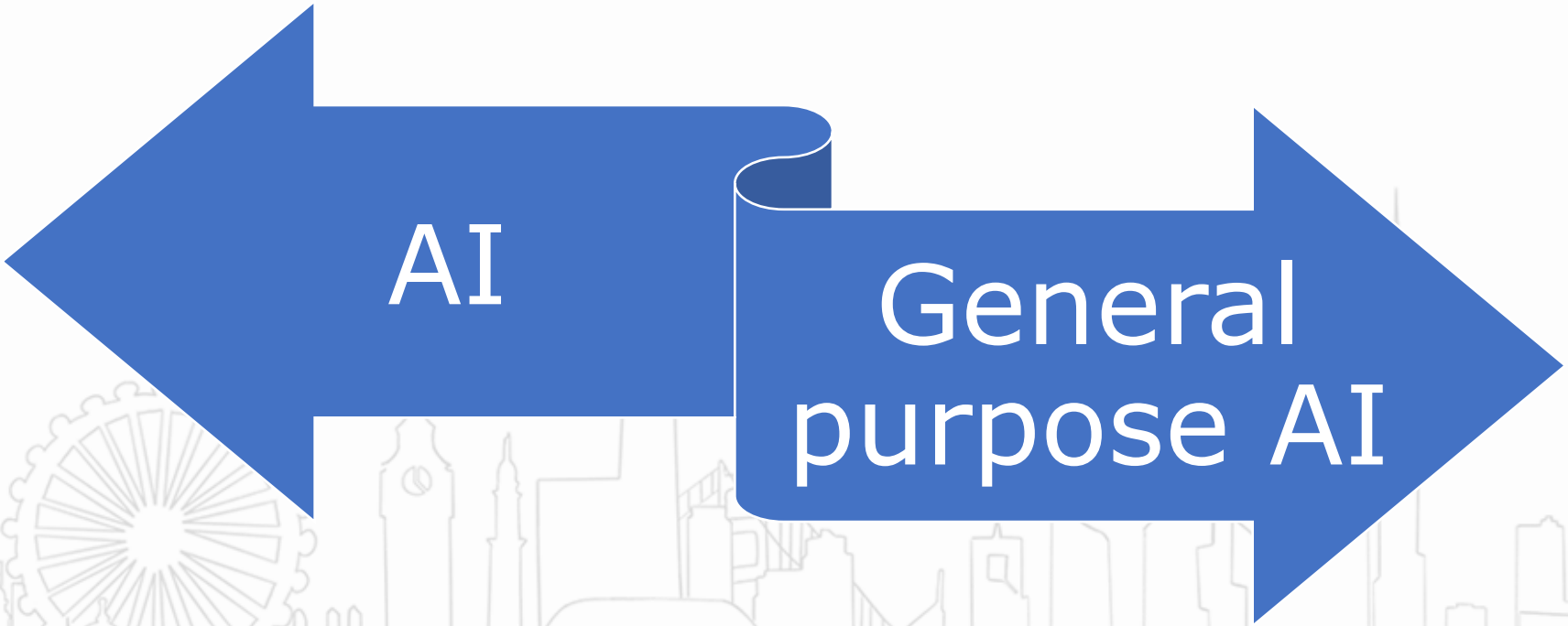


L2B PARTNERS STUDIO LEGALE

MAIN CHALLENGES OF AI

- ✓ compliance with regulations that safeguard *fundamental rights and privacy*
- ✓ addressing *biases* in AI systems, and maintaining transparency and accountability in decision-making processes
- ✓ the *rapid pace* of AI development often outstrips the creation of regulatory frameworks, leading to potential gaps in oversight
- ✓ balancing innovation with *ethical considerations*
- ✓ *international harmonization* of AI governance
- ✓ protecting *intellectual property rights* related to AI-generated content and AI learning

L2B PARTNERS STUDIO LEGALE



L2B PARTNERS STUDIO LEGALE

The Need for a Harmonised AI Framework

1

Fragmentation

Without a harmonized AI framework, fragmentation across different EU member states could create barriers to innovation and hinder the development of a single market for AI.

2

Level Playing Field

A unified regulatory approach ensures a level playing field for businesses and promotes fair competition in the AI market.

3

Trust and Confidence

A harmonized framework fosters trust and confidence in AI technologies, encouraging wider adoption and societal acceptance.

L2B PARTNERS STUDIO LEGALE

SUBJECT MATTER OF AI ACT – Art. 1

a) *harmonised rules* for the placing on the market the putting into service, and the use of AI systems;

b) *prohibitions* of certain AI practices;

c) specific *requirements for high-risk AI systems* and obligations for operators of such systems;

d) harmonised *transparency* rules for certain AI systems;

e) harmonised rules for the placing on the market of *general-purpose AI models*;

f) rules on market monitoring, market surveillance, governance and enforcement;

g) measures to *support innovation*, with a particular focus on SMEs, including start-ups.

L2B PARTNERS STUDIO LEGALE

SCOPE OF APPLICATION OF THE AI ACT – art. 2

1. The AI Act applies to (**subjects** and **territory**):

a) *providers* placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, *irrespective of whether those providers are established or located within the Union or in a third country*;

b) *deployers* of AI systems that have their place of establishment or are located within the Union;

c) providers and deployers of AI systems that have their place of establishment or are located in a third country, *where the output produced by the AI system is used in the Union*;

d) importers and distributors of AI systems;

e) product manufacturers placing on the market or *putting into service an AI system together with their product* and under their own name or trademark;

f) authorised representatives of providers, which are not established in the Union;

g) affected persons that are located in the Union.

L2B PARTNERS STUDIO LEGALE

RELEVANT DEFINITIONS – Art. 3

‘**provider**’ means 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**’ means a natural or legal person, public authority, agency or other body *using an AI system under its authority* except where the AI system is used in the course of a personal non-professional activity;
‘**authorised representative**’ means a natural or legal person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation;
‘**importer**’ means a natural or legal person located or established in the Union that *places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country*;
‘**distributor**’ means a natural or legal person in the supply chain, *other than the provider or the importer, that makes an AI system available on the Union market*;
‘**operator**’ means a provider, product manufacturer, deployer, authorised representative, importer or distributor.

L2B PARTNERS STUDIO LEGALE

SCOPE OF APPLICATION OF THE AI ACT – art. 2

The AI Act applies to (**subject matter**):

'**AI system**' means a machine-based system that is 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;

'**General-purpose AI model**' means an AI model, including where such an AI model is *trained with a large amount of data using self-supervision* at scale, that displays significant generality and is capable of competently *performing 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, except AI models that are used for research, development or prototyping activities before they are placed on the market.

L2B PARTNERS STUDIO LEGALE

SCOPE OF APPLICATION OF THE AI ACT – art. 2

The AI Act **DOES NOT apply to**:

AI systems distributed under a *FOSS license*.

AI models, including their output, specifically developed and put into service *for the sole purpose of scientific research and development*.

Household exception: deployers who are natural persons using AI systems in the course of a purely personal non-professional activity.

AI systems where and in so far they are placed on the market, put into service, or used with or without modification *exclusively for military, defence or national security purposes*, regardless of the type of entity carrying out those activities.

Public authorities in a third country nor to international organisations falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organisations use AI systems in the framework of *international cooperation or agreements for law enforcement and judicial cooperation*.

L2B PARTNERS STUDIO LEGALE

FUNDAMENTAL PRINCIPLES OF THE AI ACT

1 Data Ownership

Preserves data ownership rights while promoting access for AI development and innovation.

2 Data Access

Establishes frameworks for accessing and sharing data for AI purposes, ensuring fair and transparent access.

3 Non-discrimination

Guaranteeing that AI systems do not discriminate against individuals or groups based on factors such as race, gender, or religion.

4 Data Security and Privacy

Prioritizes data security and privacy, implementing measures to protect sensitive information and personal data.

5 Transparency and Explainability

Promotes transparency in AI systems, providing clear explanations of how data is used and how decisions are made.

6 Human Oversight

Ensuring human control over AI systems to prevent unintended consequences and protect human autonomy.

L2B PARTNERS STUDIO LEGALE

PURPOSES OF THE AI ACT

✓ promote data sharing
✓ enhance access to data for AI development
✓ ensure fair competition
✓ *protect fundamental rights*

L2B PARTNERS STUDIO LEGALE

Meta stops EU roll-out of AI model due to regulatory concerns

By **Cynthia Kroet**

Published on 18/07/2024 - 18:17 GMT+2

https://www.euronews.com/next/2024/07/18/meta-stops-eu-roll-out-of-ai-model-due-to-regulatory-concerns

L2B PARTNERS STUDIO LEGALE

TECH

Apple Intelligence won't launch in EU in 2024 due to antitrust regulation, company says

PUBLISHED FRI, JUN 21 2024•2:01 PM EDT | UPDATED FRI, JUN 21 2024•3:01 PM EDT

Rohan Goswami
@IN/ROHANGOSWAMICNBC/
@ROGOSWAMI

SHARE

https://www.cnbc.com/2024/06/21/apple-ai-europe-dma-macos.html

L2B PARTNERS STUDIO LEGALE

Now, how does it achieve these goals?
At its core, the AI Act is a **risk-based framework**

AI systems are categorized into four levels of risk:

- ✓ **Minimal risk**, such as spam filters.
- ✓ **Limited risk**, which might include chatbots.
- ✓ **High risk**, like AI used in recruitment or medical devices.
- ✓ **Unacceptable risk**, such as social scoring by governments, *which is outright prohibited*.

L2B PARTNERS STUDIO LEGALE

Unacceptable risk: PROHIBITED AI PRATICES

Art. 5

L2B PARTNERS STUDIO LEGALE

Prohibited Practice 1: Subliminal Techniques

1

Unconscious

2

Influence

Using AI to manipulate individuals' behaviour through subliminal techniques, like hidden messages or unconscious triggers, without their awareness.

3

Ethical

Raises serious ethical concerns as it considerably undermines individuals' autonomy and decision-making processes, having such individual make a decision they would not otherwise have made, potentially leading to significantly harmful consequences.

L2B PARTNERS STUDIO LEGALE

Prohibited Practice 2: Exploiting Vulnerabilities

Protection

AI systems that exploit vulnerabilities due to age, disability or a specific social or economic situation

Risk

Distortion of such natural person behavior which could cause significant harm to that person or another person

L2B PARTNERS STUDIO LEGALE

Prohibited Practice 3: Social Scoring Systems

1 Ranking Individuals

AI systems that create social scores to rank individuals based on their behaviour, characteristics, or social connections.

2 Discrimination

These systems can lead to discrimination, profiling, and the creation of social hierarchies which are:

- in a context not connected to the context in which data has been gathered; and/or
- Disproportionate.

L2B PARTNERS STUDIO LEGALE

CHINA'S SOCIAL CREDIT SYSTEM

It's been dubbed the most ambitious experiment in digital social control ever undertaken. The Chinese government plans to launch its Social Credit System nationally by 2020.

WHAT'S THE AIM?

The system intends to monitor, rate and regulate the financial, social, moral and, possibly, political behavior of China's citizens – and also the country's companies – via a system of punishments and rewards. The stated aim is to "provide the trustworthy with benefits and discipline the untrustworthy."

The Chinese government considers the system an important tool to steer China's economy and to govern society. There is still much speculation about how the final system will actually function. Details in this chart are based on pilot schemes and plausible expert expectations.

REWARDS AND PUNISHMENTS

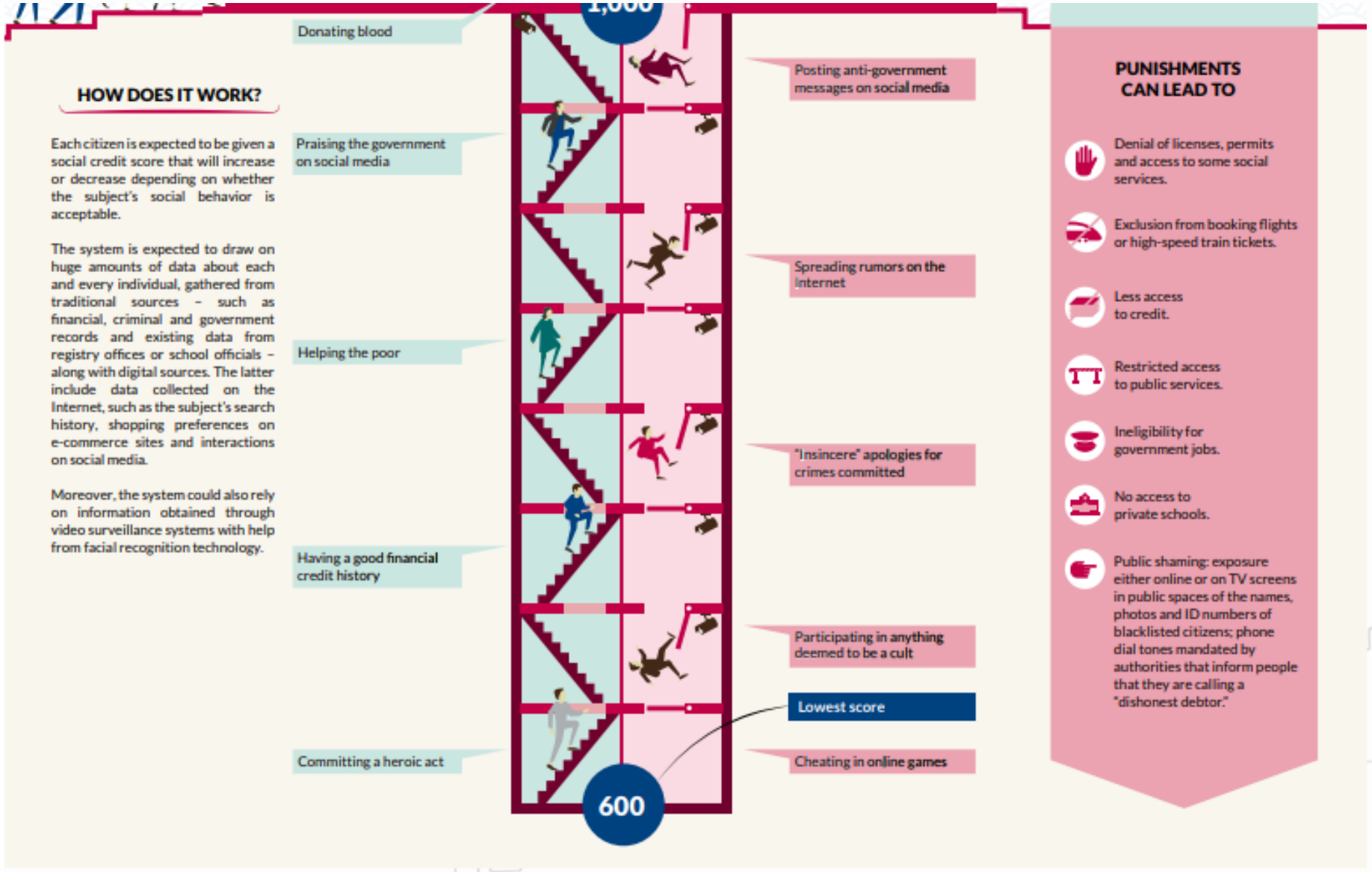
Citizens with high scores get to enjoy special "privileges" while those with low scores ultimately risk getting treated as second-class citizens.

HIGH SCORES CAN LEAD TO

- Priority for school admissions and employment.
- Easier access to cash loans and consumer credit.
- Deposit-free bicycle and car hire.
- Free gym facilities.
- Cheaper public transport.
- Shorter wait times in hospitals.
- Fast-track promotion at work.
- Jumping the queue for public housing.
- Tax breaks.

Source: https://www.bertelsmann-stiftung.de/fileadmin/files/aam/Asia-Book_A_03_China_Social_Credit_System.pdf

L2B PARTNERS STUDIO LEGALE



Source: https://www.bertelsmann-stiftung.de/fileadmin/files/aam/Asia-Book_A_03_China_Social_Credit_System.pdf

L2B PARTNERS STUDIO LEGALE

Prohibited Practice 4: Prediction of criminal offences

Such prediction is based *only* on the profiling based on the natural *person's personality traits and characteristics*

This prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity

L2B PARTNERS STUDIO LEGALE

Prohibited Practice 5:

AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage

L2B PARTNERS STUDIO LEGALE

Prohibited Practice 6:
AI systems that infer emotions of individuals on the workplace or education institutions

L2B PARTNERS STUDIO LEGALE

Prohibited Practice 7:

AI systems that categorise individually natural persons based on their *biometric data* to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation

L2B PARTNERS STUDIO LEGALE

Recital 15

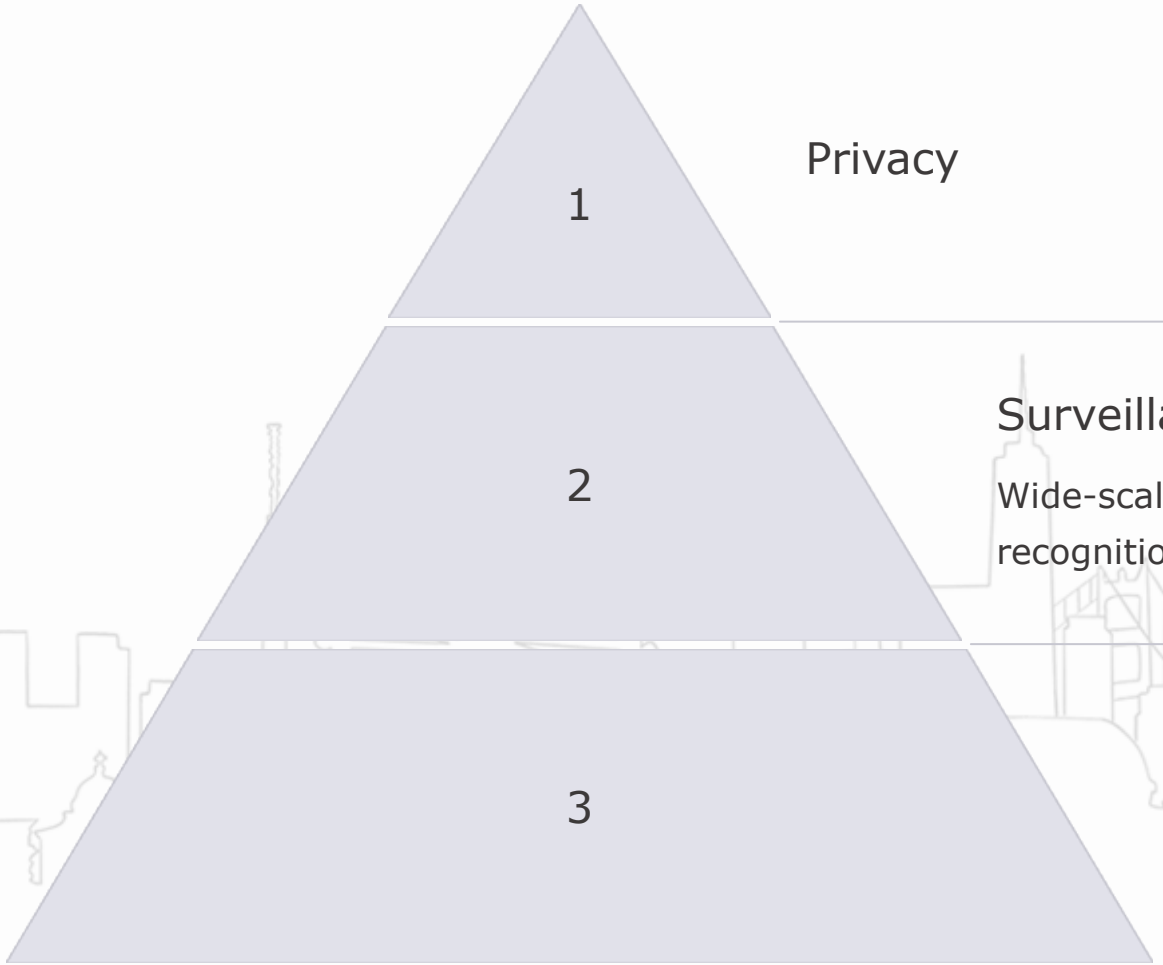
The notion of '*biometric identification*' referred to in this Regulation should be defined as the automated recognition of physical, physiological and behavioural human features such as the face, eye movement, body shape, voice, prosody, gait, posture, heart rate, blood pressure, odour, keystrokes characteristics, *for the purpose of establishing an individual's identity by comparing biometric data of that individual to stored biometric data of individuals in a reference database*, irrespective of whether the individual has given its consent or not. *This excludes AI systems intended to be used for biometric verification, which includes authentication, whose sole purpose is to confirm that a specific natural person is the person he or she claims to be* and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having security access to premises.

L2B PARTNERS STUDIO LEGALE

Recital 16

The notion of '*biometric categorisation*' referred to in this Regulation should be defined as assigning natural persons to specific categories on the basis of their biometric data. Such specific categories can relate to aspects such as sex, age, hair colour, eye colour, tattoos, behavioural or personality traits, language, religion, membership of a national minority, sexual or political orientation. This does not include biometric categorisation systems that are a purely ancillary feature intrinsically linked to another commercial service, meaning that the feature cannot, for objective technical reasons, be used without the principal service, and the integration of that feature or functionality is not a means to circumvent the applicability of the rules of this Regulation. For example, filters categorising facial or body features used on online marketplaces could constitute such an ancillary feature as they can be used only in relation to the principal service which consists in selling a product by allowing the consumer to preview the display of the product on him or herself and help the consumer to make a purchase decision. Filters used on online social network services which categorise facial or body features to allow users to add or modify pictures or videos could also be considered to be ancillary feature as such filter cannot be used without the principal service of the social network services consisting in the sharing of content online.

Prohibited Practice 8: Real-Time Biometric Identification in Public Spaces for law-enforcement purposes



Privacy

Surveillance

Wide-scale surveillance using biometric identification, like facial recognition, in public spaces without individuals' consent or knowledge.

Freedom

Impacts freedom of movement, expression, and association, raising concerns about authoritarian control and the erosion of democratic values.

Prohibited Practice 8: Real-Time Biometric Identification in Public Spaces for law-enforcement purposes

Unless and in so far as such use is strictly necessary for one of the following objectives:

(i) the *targeted search for specific victims* of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons;

(ii) the prevention of a specific, *substantial and imminent threat to the life or physical safety* of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;

(iii) *the localisation or identification of a person suspected of having committed a criminal offence*, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

L2B PARTNERS STUDIO LEGALE

High risk
Chapter III

L2B PARTNERS STUDIO LEGALE

CLASSIFICATION AS HIGH-RISK - ART. 6

✓ An AI system shall be considered to be high-risk where *both* of the following conditions are fulfilled:

(a) the AI system is *intended to be used as a safety component of a product*, or the AI system is itself a product, covered by the Union harmonisation legislation listed in Annex I;

(b) the product whose safety component pursuant to point (a) is the AI system, or the AI system itself as a product, is required to undergo a *third-party conformity assessment*, with a view to the placing on the market or the putting into service of that product pursuant to the Union harmonisation legislation listed in Annex I.

✓ In addition, *AI systems referred to in Annex III* shall be considered to be high-risk

By *derogation*, an AI system referred to in Annex III shall not be considered to be high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making.

L2B PARTNERS STUDIO LEGALE

THE SECTORS COVERED BY EU HARMONIZATION LEGISLATION LISTED IN ANNEX I

- safety of toys
- lifts and safety components for lifts
- equipment and protective systems intended for use in potentially explosive atmospheres
- radio equipment
- pressure equipment
- cableway installations
- personal protective equipment
- appliances burning gaseous fuels
- medical devices, *in vitro* diagnostic medical devices

L2B PARTNERS STUDIO LEGALE

THE SECTORS COVERED BY EU HARNOMIZATION LEGISLATION LISTED IN ANNEX I

- civil aviation security
- two- or three-wheel vehicles and quadricycles
- agricultural and forestry vehicles
- marine equipment
- rail systems
- motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles,
- unmanned aircraft and their engines, propellers, parts and equipment to control them remotely, are concerned.

L2B
PARTNERS
STUDIO
LEGALE

THE HIGH-RISK AI SYSTEMS LISTED IN ANNEX III

L2B PARTNERS STUDIO LEGALE

Biometric Systems

Remote Biometric Identification

Systems used for identifying individuals at a distance, excluding verification purposes.

Biometric Categorisation

AI that categorises people based on sensitive or protected attributes.

Emotion Recognition

Systems designed to detect and interpret human emotions.

L2B PARTNERS STUDIO LEGALE

Critical Infrastructure and Safety

AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of essential utilities such as water, gas, heating, and electricity.

Road Traffic

AI managing traffic flow and safety

Utilities

AI controlling power grids

Water Supply

AI monitoring water distribution

L2B PARTNERS STUDIO LEGALE

Education and Vocational Training

1

Admissions

AI systems determining access or admission to educational institutions

2

Learning Evaluation

AI assessing learning outcomes and steering the learning process

3

Education Level Assessment

AI determining appropriate education levels that an individual will receive or will be able to access

4

Exam Monitoring

AI detecting prohibited behaviour during tests

L2B PARTNERS STUDIO LEGALE

Employment and Worker Management

Recruitment and Selection

AI systems used for job advertisements, application filtering, and candidate evaluation and selection

Work-Related Decisions

AI influencing used to make decisions affecting terms of work-related relationships, the promotion or termination of work-related contractual relationships, to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships

L2B PARTNERS STUDIO LEGALE

Access to Essential Services

Public Assistance

AI evaluating eligibility for essential public benefits, including healthcare services

Credit Scoring

AI assessing creditworthiness and establishing credit scores

Insurance Risk Assessment

AI systems for risk assessment and pricing in life and health insurance

Emergency Services

AI for evaluating emergency calls and dispatching first responders

L2B PARTNERS STUDIO LEGALE

Law Enforcement Applications

1. **Victim Risk Assessment**
   AI predicting the likelihood of a person becoming a crime victim

2. **Polygraph-like Tools**
   AI systems used as lie detectors or similar applications

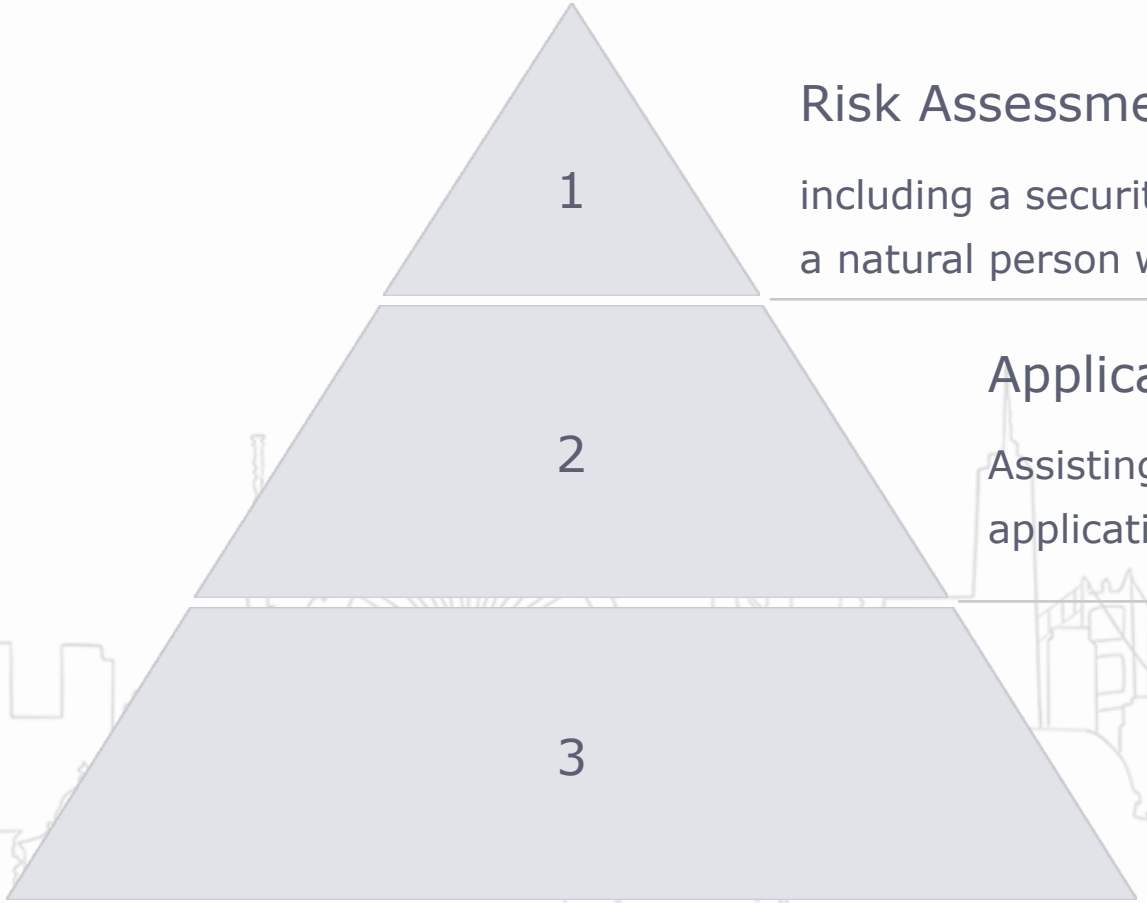
3. **Evidence Evaluation**
   AI assessing the reliability of evidence in criminal investigations

4. **Offender Risk Assessment**
   AI predicting the risk of a person offending or re-offending

5. **Criminal Profiling**
   AI systems used for profiling in criminal investigations

L2B PARTNERS STUDIO LEGALE

Migration, Asylum, and Border Control



Risk Assessment

including a security risk, a risk of irregular migration, or a health risk, posed by a natural person who intends to enter or who has entered into the territory

Application Processing

Assisting in examining asylum, visa, and residence permit applications with regard to the eligibility

Identity Verification

Detecting and identifying individuals at borders

L2B PARTNERS STUDIO LEGALE

Administration of Justice and Democratic Processes

Legal Assistance

AI systems assisting judicial authorities in researching, interpreting, and applying the law to specific cases

Electoral Influence

AI systems designed to influence election or referendum outcomes or voting behaviour

Exceptions

An AI system referred to in Annex III shall **not be considered to be high-risk** where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making.

The first subparagraph shall apply where any of the following conditions is fulfilled:
(a) the AI system is intended to perform a *narrow procedural task*;
(b) the AI system is intended to *improve the result of a previously completed human activity*;
(c) the AI system is intended to *detect decision-making patterns or deviations from prior decision-making patterns* and is not meant to replace or influence the previously completed human assessment, without proper human review; or
(d) the AI system is intended to *perform a preparatory task* to an assessment relevant for the purposes of the use cases listed in Annex III.

Notwithstanding the first subparagraph, an AI system referred to in Annex III shall always be considered to be high-risk where the AI system performs profiling of natural persons

L2B PARTNERS STUDIO LEGALE

Principles in the definition of High-Risk AI Systems

1 Comprehensive Scope

The EU's framework covers a wide range of AI applications across various sectors

2 Focus on Fundamental Rights

Regulations aim to protect individual rights and societal values

3 Balancing Innovation and Safety

The framework seeks to promote AI development while mitigating risks

4 Ongoing Adaptation

As AI evolves, regulations may need to be updated to address new challenges

L2B PARTNERS STUDIO LEGALE

High risk
Requirements for high-risk AI systems

What shall a provider do *before* distributing/making available an AI system on the market

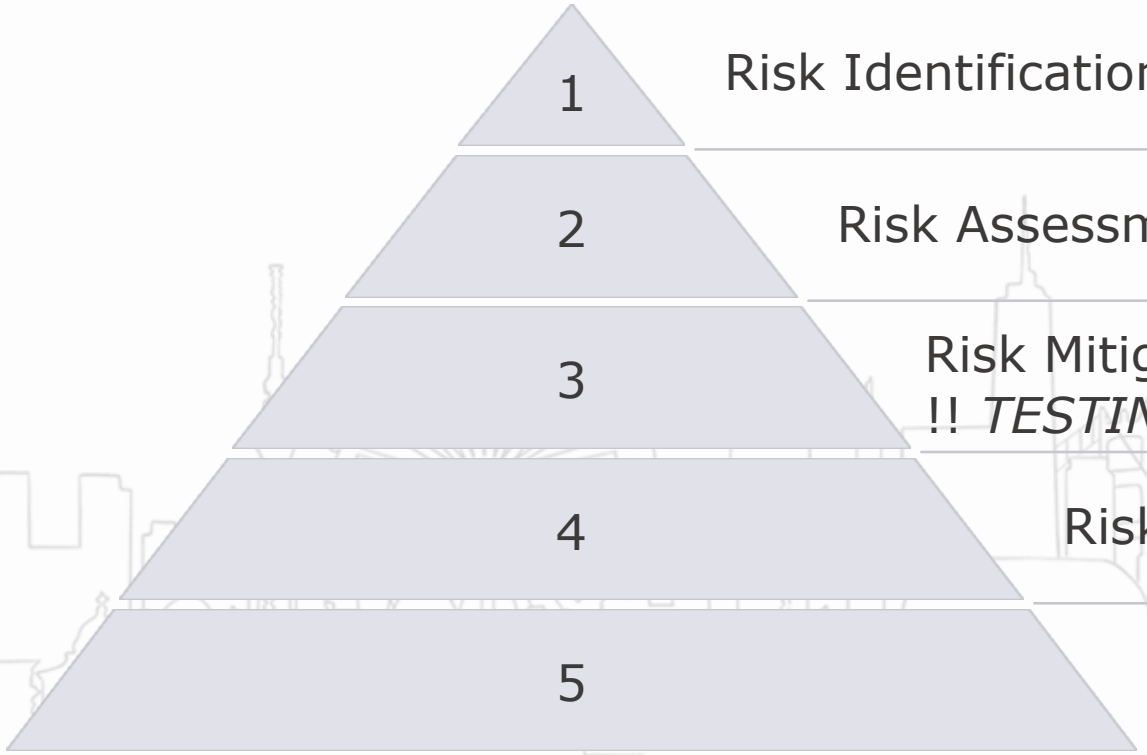
Compliance

High-risk AI systems must undergo conformity assessment by a notified body to ensure they comply with the AI Act's requirements. This involves a thorough evaluation of the system's design, development, and deployment.

Risk Management System

Organizations deploying high-risk AI systems need a robust risk management system to identify, analyze, mitigate, and monitor risks throughout the AI system's lifecycle. This involves a comprehensive framework for risk assessment and management.

Risk Management System – Art. 9



1. Risk Identification
2. Risk Assessment
3. Risk Mitigation: adoption of measures
   !! *TESTING*
4. Risk Monitoring
5. Risk Reporting

Data and Data Governance – Art. 10

!!
appropriate measures to detect, prevent and mitigate *possible biases*

1 Data Quality

High-risk AI systems require high-quality data for training and operation. This involves ensuring data accuracy, completeness, and relevance to the AI system's intended purpose.

2 Data Security

Organizations must implement robust data security measures to protect sensitive data used in high-risk AI systems. This includes measures to prevent unauthorized access, data breaches, and misuse of personal data.

3 Data Governance

Clear data governance frameworks are essential to ensure responsible data handling and compliance with regulations. This involves establishing clear data ownership, access control, and data retention policies.

L2B PARTNERS STUDIO LEGALE

Technical Documentation- Art. 11

System Description

Comprehensive technical documentation is required, detailing the AI system's design, algorithms, training data, and operational characteristics. This documentation should be easily accessible and understandable.

Software Code

The AI system's software code should be documented and accessible for review, allowing for analysis of the system's logic and potential biases or vulnerabilities.

Risk Assessment Results

Detailed risk assessment results, including identified risks, mitigation strategies, and residual risk levels, should be documented to demonstrate responsible risk management practices.

Specific contents of the documentation are listed in Annex IV to the AI Act

Record Keeping Art. 12

Logging system
which shall enable recording of following items, for the overall purposes of monitoring and individuation of risks

- ✓ recording of the period of each use of the system (start date and time and end date and time of each use)
- ✓ the reference database against which input data has been checked by the system
- ✓ the input data for which the search has led to a match
- ✓ the identification of the natural persons involved in the verification of the results

L2B PARTNERS STUDIO LEGALE

Transparency and Provision of Information – Art. 13

1

Transparency

High-risk AI systems must be transparent in their operation. Users should be informed about the AI system's capabilities, limitations, and potential biases. *Instructions* shall be provided.

2

Explainability

Organizations must provide clear explanations of how the AI system arrives at its decisions, allowing users to understand the reasoning behind the system's outputs.

3

Information Provision

Deployers should be provided with relevant information about the AI system's intended use, potential risks, and the availability of human oversight mechanisms.

Human Oversight – Art. 14

1

Human-in-the-Loop

Human oversight mechanisms should be integrated into the AI system's design, allowing for human intervention in critical situations and ensuring responsible decision-making. A *human-machine interface tool* is necessary.

2

Purpose

Human oversight shall aim to prevent or minimise the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse.

3

Monitoring and Evaluation

Ongoing monitoring and evaluation is possible in case the human is in a position to (i) to properly understand the relevant capacities and limitations of the high-risk AI system; (ii) correctly interpret the high-risk AI system’s output; (iii) to intervene in the operation of the high-risk AI system or interrupt the system.

Accuracy, Robustness, Cybersecurity –Art. 15

- ✓ The Commission shall encourage the development of benchmarks.
- ✓ Level of accuracy shall be included in the documentation
- ✓ Feedback loops shall be addressed in order to avoid biases
- ✓ Overall security measures to prevent un-authorized access

L2B PARTNERS STUDIO LEGALE

Obligations for AI System Providers

Ensure compliance with the requirements set forth above

Transparency

AI system providers must disclose information about their systems, including the data used and the decision-making processes.

1

Accountability

AI system providers are held accountable for the performance and impact of their systems, ensuring ethical and responsible development.

3

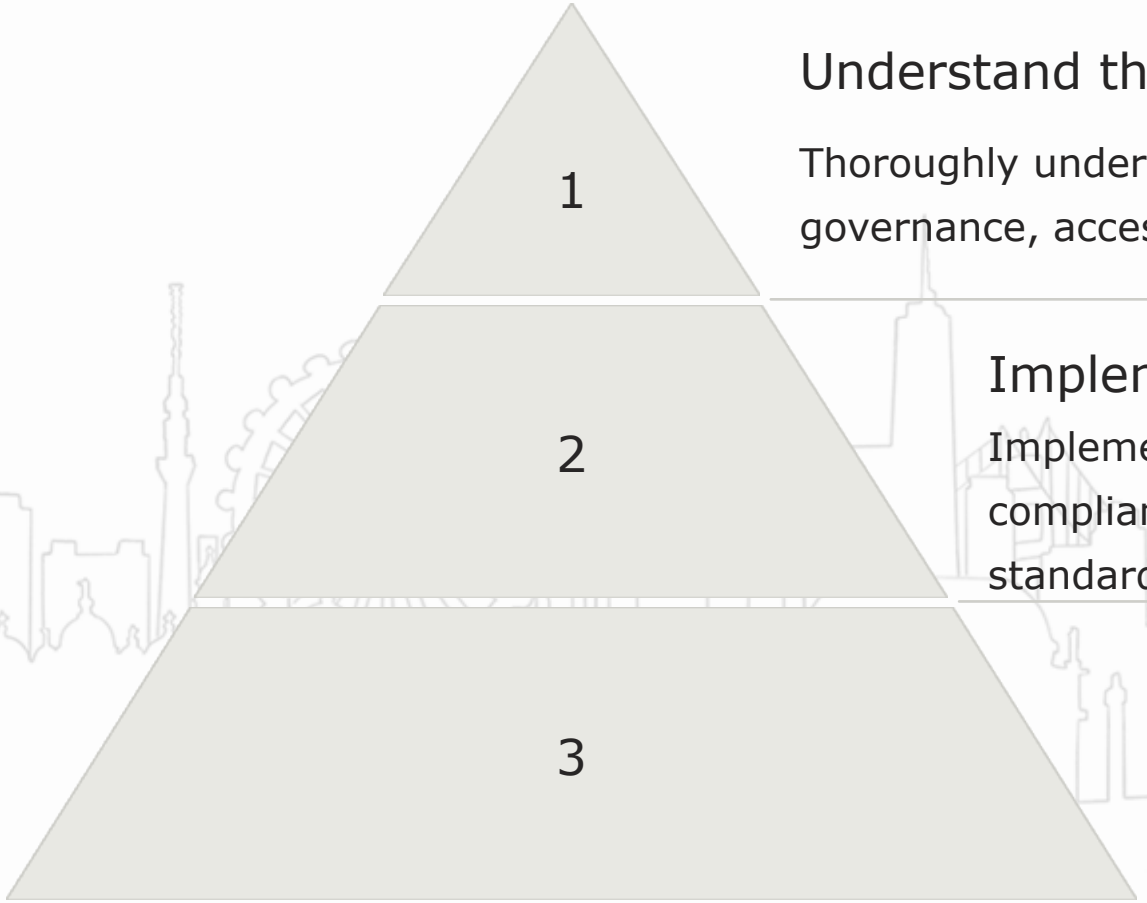
2

Fairness

The regulation requires AI systems to be fair and unbiased, avoiding discrimination and promoting equal opportunities.

L2B PARTNERS STUDIO LEGALE

Ensuring Compliance with the Regulation



Understand the Requirements

Thoroughly understand the provisions of the AI Data Act, including data governance, access, and security requirements.

Implement Data Protection Measures

Implement robust data protection measures to ensure compliance with privacy regulations and data security standards.

Document and Monitor Practices

Document data handling processes and monitor compliance with the regulation to ensure responsible AI development.

L2B PARTNERS STUDIO LEGALE

Challenges and Limitations of the AI Data Act

1

Data Availability

The regulation may encounter challenges in ensuring sufficient data availability for AI development, particularly for niche sectors.

2

Complexity and Interpretation

The regulation is complex and subject to interpretation, requiring careful consideration and legal advice to ensure compliance.

3

Enforcement and Oversight

Effective enforcement mechanisms and oversight are crucial for ensuring compliance and addressing potential violations.

L2B PARTNERS STUDIO LEGALE

Protecting Fundamental Rights and Values

Human Dignity

The AI Act emphasizes the protection of human dignity, prohibiting AI systems that could violate fundamental rights or lead to discriminatory outcomes.

Privacy

Safeguarding personal data and privacy, ensuring that AI systems respect individual autonomy and data protection regulations.

Freedom of Expression

Protecting freedom of expression and ensuring that AI systems do not restrict or censor individuals' rights to express themselves.

L2B PARTNERS STUDIO LEGALE

The AI Act's Entry into Force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.
It shall apply from 2 August 2026.

However:
(a) Chapters I (General Provisions) and II (Prohibited Practices) shall apply from **2 February 2025**;

(b) Chapter III Section 4 (notifying authorities), Chapter V (Standards, registration), Chapter VII (Governance) and Chapter XII (Penalties) and Article 78 (confidentiality) shall apply from **2 August 2025**, with the exception of Article 101;

(c)Article 6(1) (High-risk) and the corresponding obligations in this Regulation shall apply from 2 August 2027.

L2B
PARTNERS
STUDIO
LEGALE

L2B
PARTNERS
STUDIO
LEGALE

TAKE AWAYS

L2B
PARTNERS
STUDIO
LEGALE

THANK YOU
...and good luck!

cosetta.masi@L2Bpartners.com