
YPOG

The AI Act: Challenges and Opportunities

Dr. Benedikt Flöter

Objectives

- Single European Market
- Innovation and Economic Growth
- Fundamental Rights

Brain Drain?

Does the AI Act harm innovation?

Two thirds expect a negative impact of the AI Act on AI Innovation in Europe

Source: appliedAI, AI Impact Survey December 2022

Tight vote …

"*Favors Big Tech*"

DR. VOLKER WISSING

Interview October 27, 2023

'EU's AI act could kill our company,' says Mistral's Cédric O

"In the digital world, the leaders set the standard, and Europe has no leaders," says former French tech minister Cedric O

Zosia Wanat 3 min read

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	Definitions	Definitions	Definitions	
Article 3, first paragraph				
127	For the purpose of this Regulation, the following definitions apply:	For the purpose of this Regulation, the following definitions apply:	For the purpose of this Regulation, the following definitions apply:	
Article 3, first paragraph, point (1)				
128	(1) 'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;	(1) 'artificial intelligence system' (AI system) means ~~*software*~~***a machine-based system*** that is ~~*developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined*~~***designed to operate with varying levels of autonomy and that can, for explicit or implicit*** objectives, generate outputs such as ~~*content,*~~ predictions, recommendations, or decisions***, that influence physical or virtual environments*** ~~*influencing the environments they interact with*~~;	(1) 'artificial intelligence system' (AI system) means ~~*software*~~***a system*** that is ~~*developed with one or more of the techniques and approaches listed in Annex I and can, for*~~***designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve*** a given set of ~~*human-defined objectives, generate*~~***objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated*** outputs such as content ***(generative AI systems)***, predictions, recommendations~~,~~ or decisions***,*** influencing the environments ~~*they interact with*~~***with which the AI system interacts***;	(1) ~~*'artificial intelligence*~~***An AI*** system~~*' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives*~~ ***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 ~~*content, predictions*~~***predictions, content***, recommendations, or decisions ~~*influencing the*~~***that can influence physical or virtual*** environments***. .*** ~~*they interact with;*~~

Scope of Application

Providers of AI systems

No AI Outsourcing

No off-shore Training

stability.ai

Implementation

1. August 2024

Entry into force

9 months

Codes of Conduct

May, 2025

24 months

High Risk AI (Annex III)

August, 2026

6 months

Prohibited AI Systems

February, 2025

12 months

GPAI-Systems

August, 2025

36 months

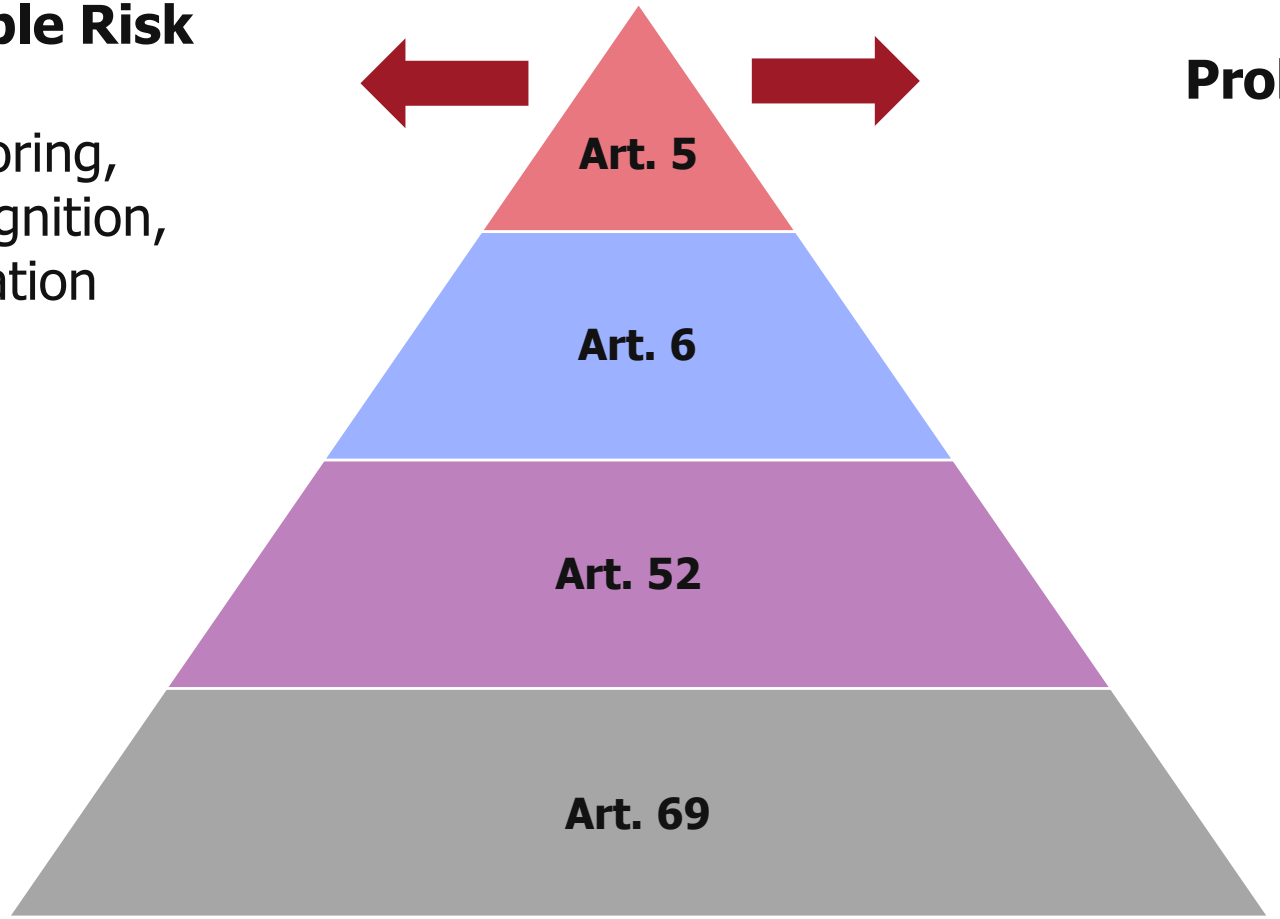
High Risk AI (Annex I)

August, 2027

Risk Classification

Unacceptable Risk

Social Scoring,
Facial Recognition,
Manipulation

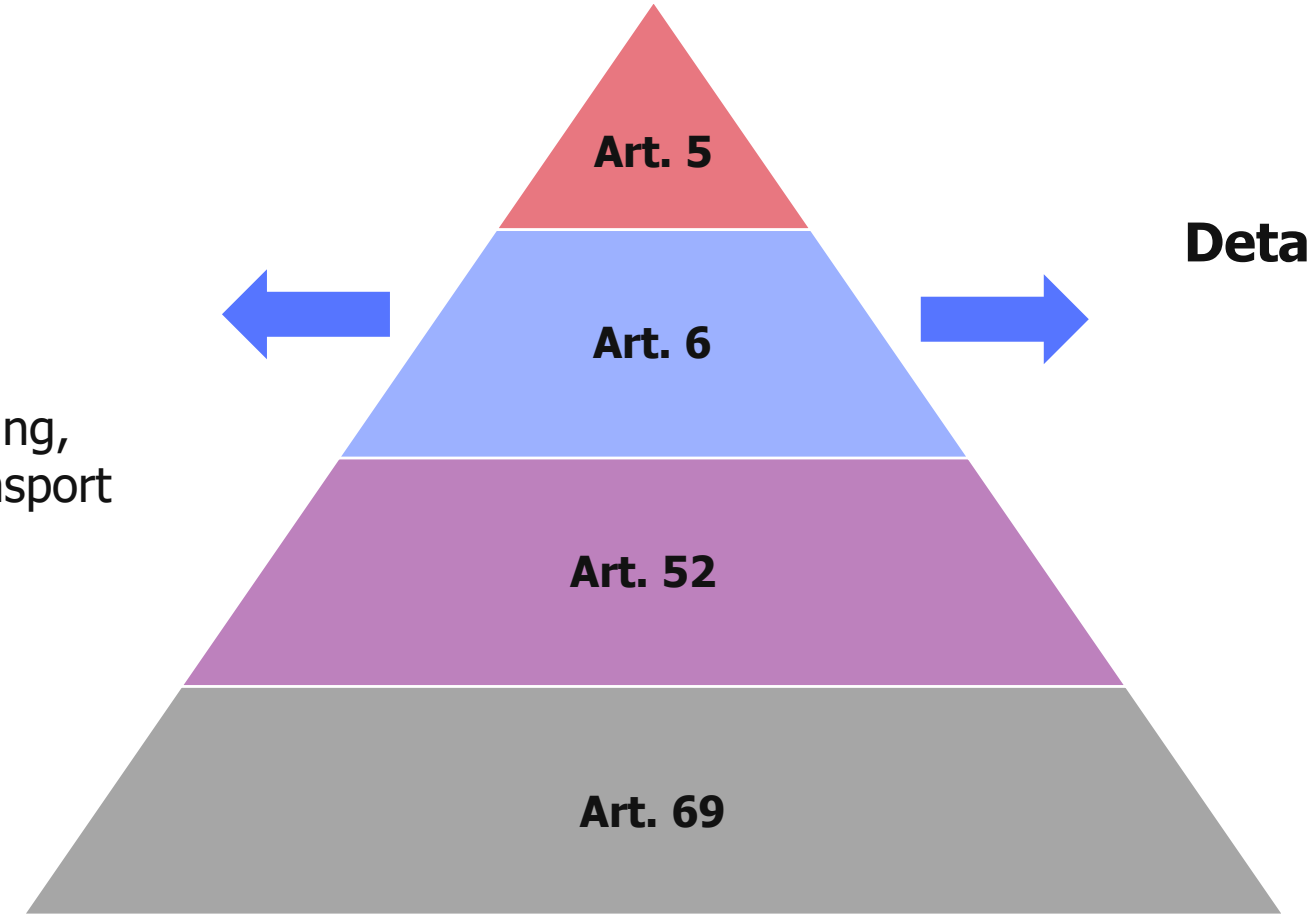


Prohibited

Risk Classification

High Risk

Judiciary
HR-Tools,
Education & Training,
Infrastructure & Tansport



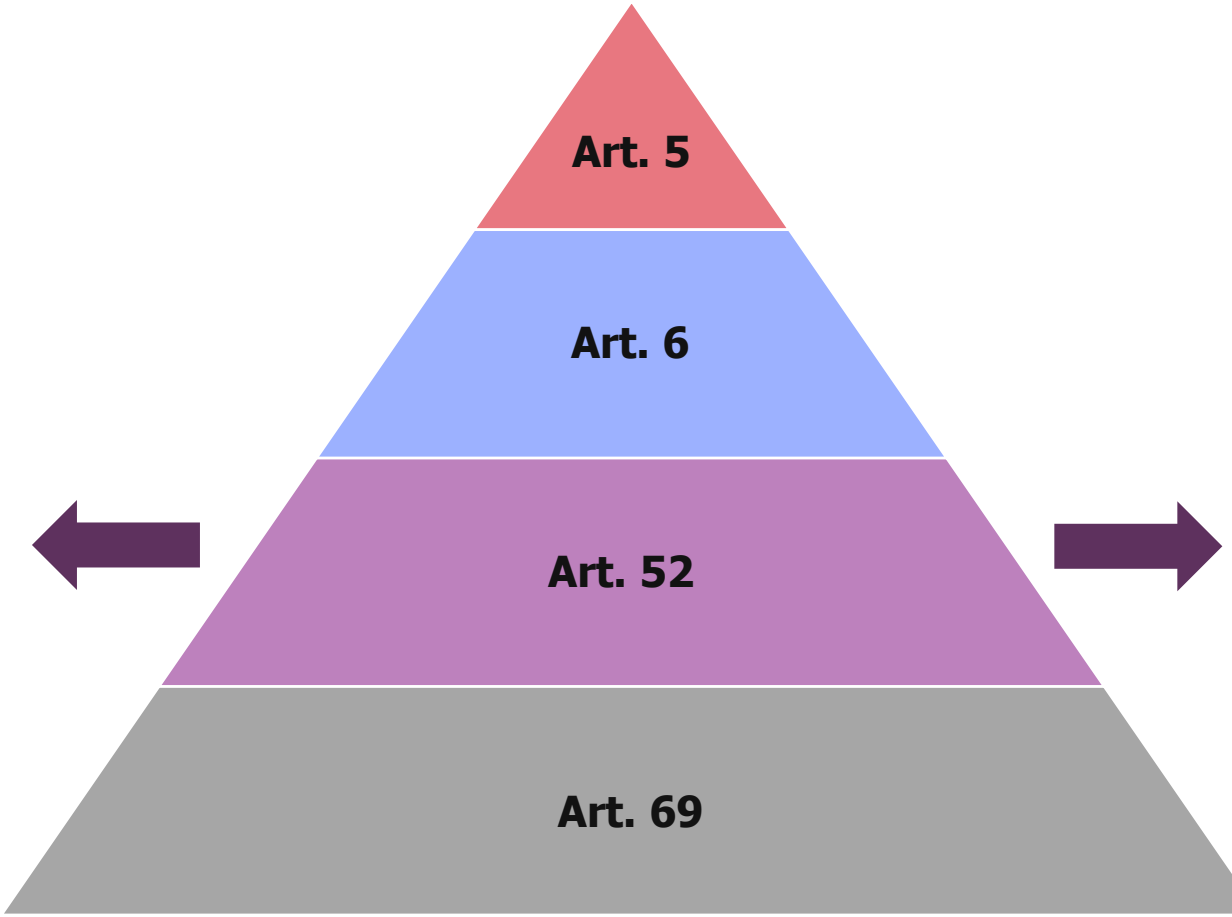
Detailed Compliance

Obligations

Risk Classification

Interactive AI

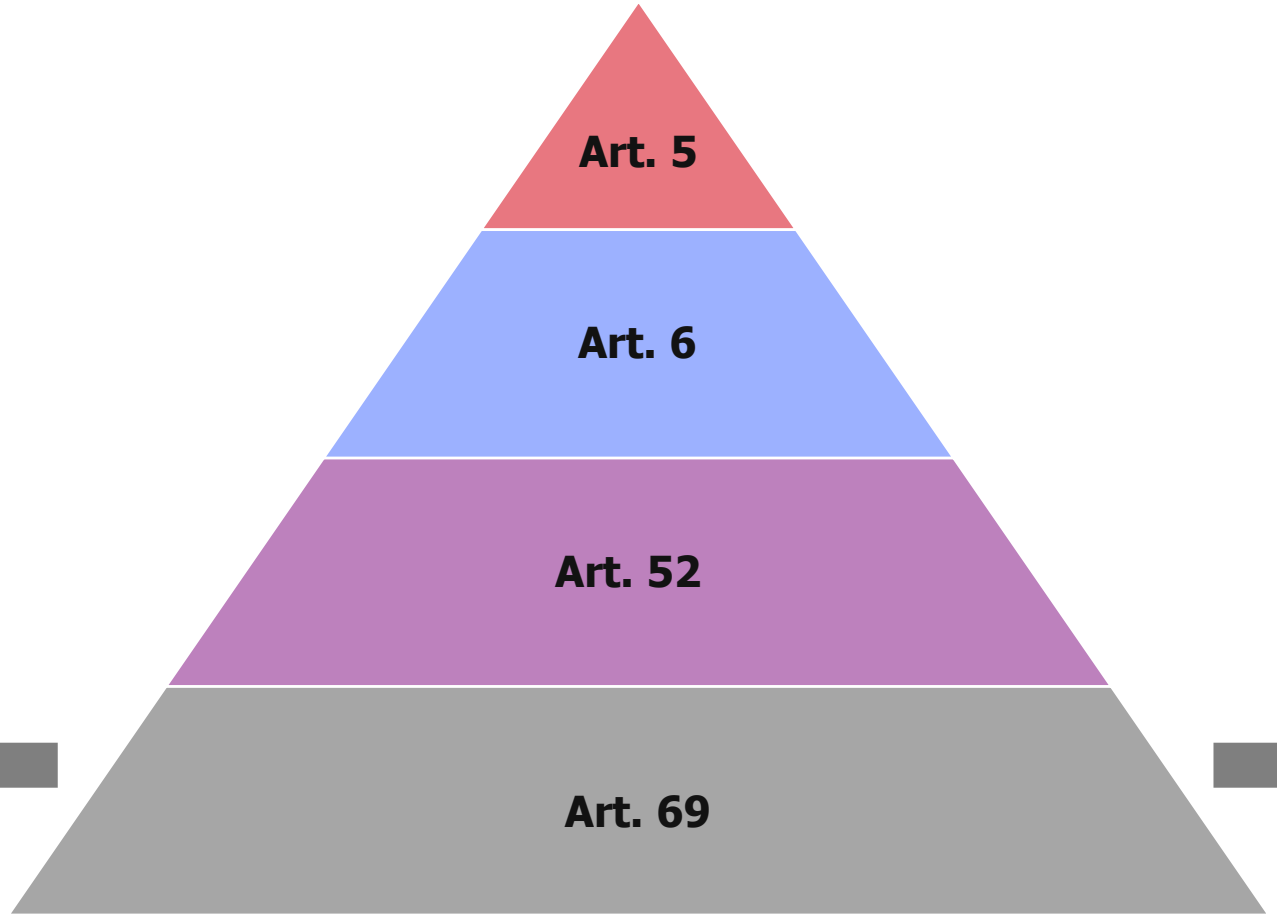
GenAI,
Chatbots,
Videogames



Transparency

Obligations

Risk Classification



Other AI Systems

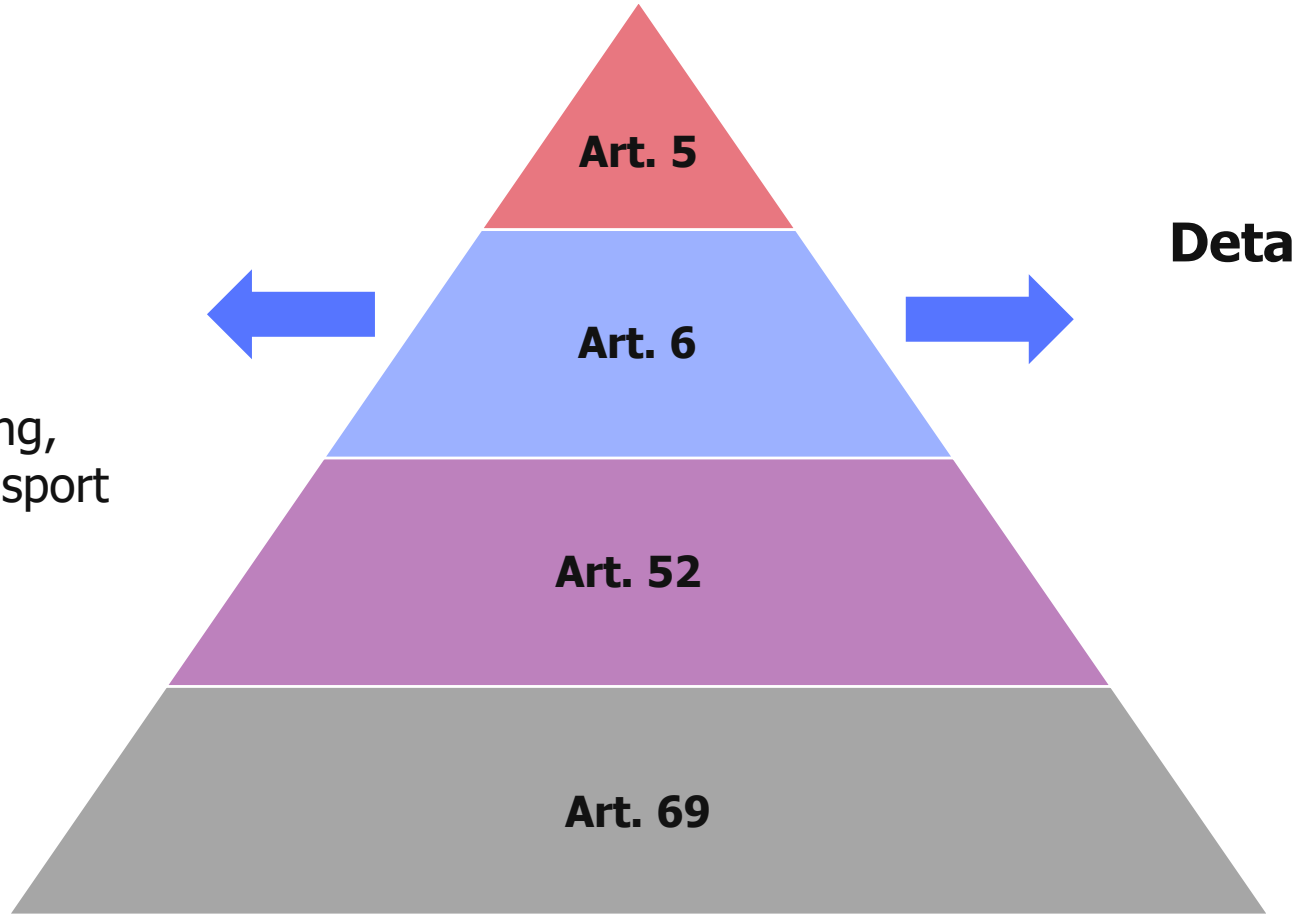
Spam Filter,
Dynamic Pricing

Code of Conduct

Risk Classification

High Risk

Judiciary
HR-Tools,
Education & Training,
Infrastructure & Transport



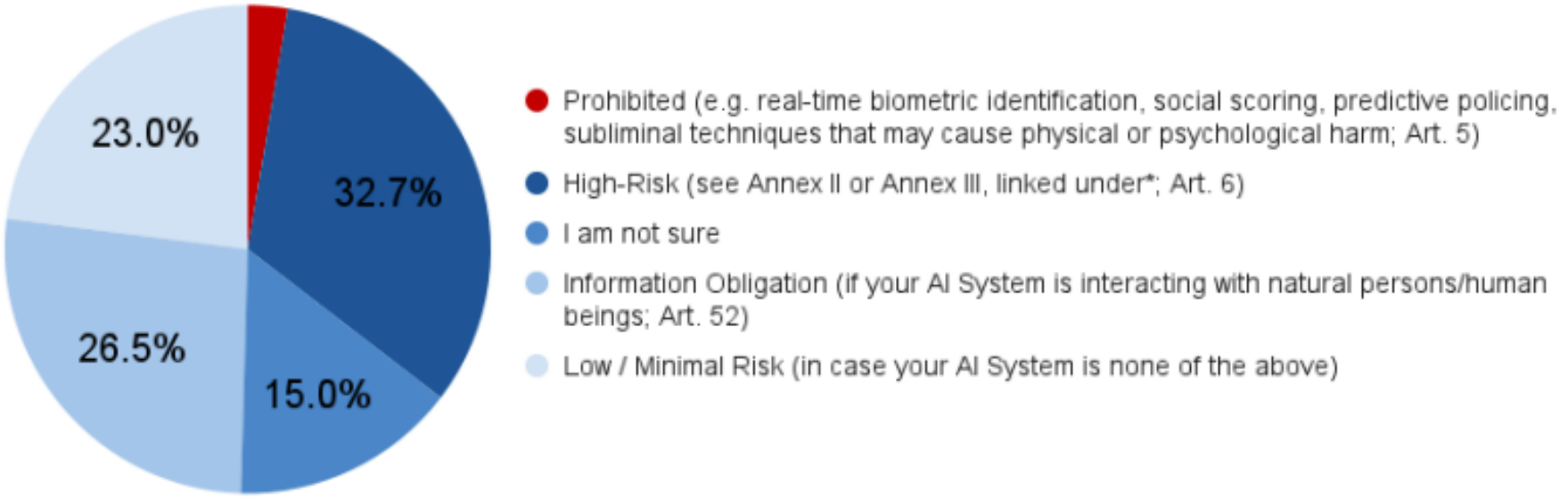
Detailed Compliance

Obligations

Risk Classification

EU Assumption: **15 % High Risk**

appliedAI: **50 %**

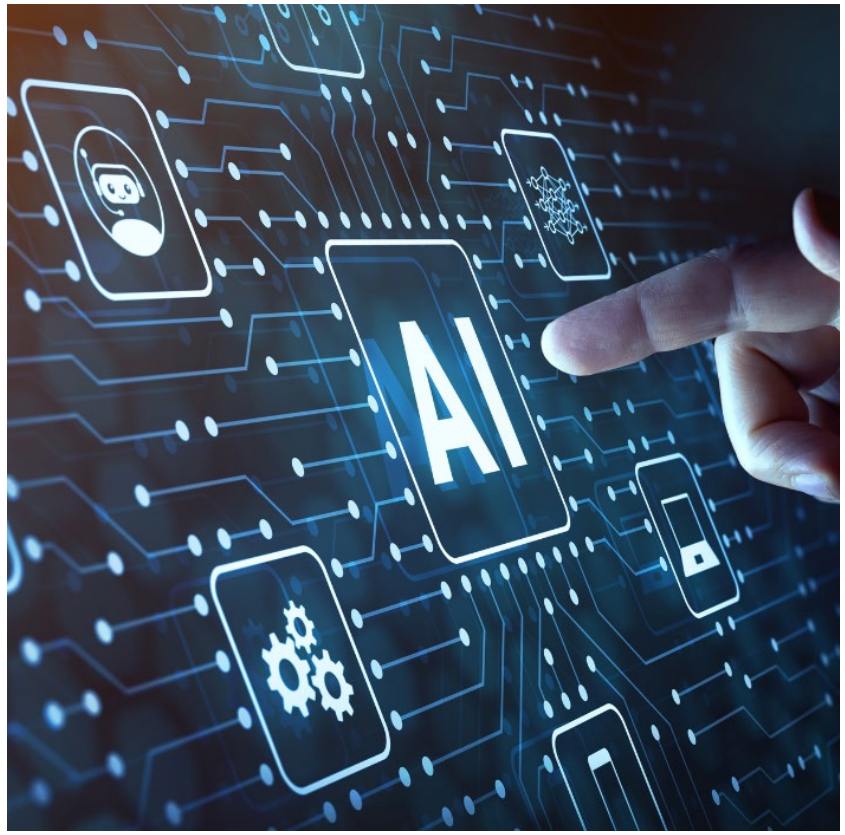


Source: appliedAI, AI Impact Survey December 2022

Risk Classification

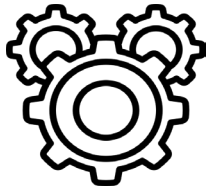
Art. 6 AI Act

1. Products or security system for products listed in Annex I
2. Products listed in Annex III



Risk Classification

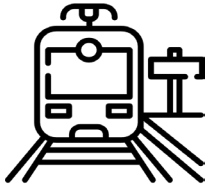
Annex I



Machinery

Toys

Medical devices



Rail system

Vehicles

Appliances burning gaseous fuels

Risk Classification

Annex III


Biometric identification


Critical infrastructure


Employment and workers management


Law enforcement


Essential private and public services

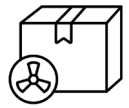

Migration and border control


Education and training


Judiciary


Public administration


Healthcare


Dangerous and substandard products

Risk Classification

Annex III


Biometric identification


Critical infrastructure


Employment and workers management


Law enforcement


Essential private and public services

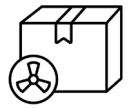

Migration and border control


Education and training


Judiciary


Public administration


Healthcare


Dangerous and substandard products


Military use out of scope

Risk Classification

How to assess a product's field of application?

(52) As regards stand-alone AI systems, namely high-risk AI systems other than those that are safety components of products, or that are themselves products, it is appropriate to classify them as high-risk if, in light of their intended purpose, they pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence and they are used in a number of specifically pre-defined areas specified in this Regulation. The identification of those

Risk Classification

How to assess a product's field of application?

(52) As regards stand-alone AI systems, namely high-risk AI systems other than those that are safety components of products, or that are themselves products, it is appropriate to classify them as high-risk if, in light of their intended purpose, they pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence and they are used in a number of specifically pre-defined areas specified in this Regulation. The identification of those

Risk Classification

How to assess a product's field of application?

Article 3

Definitions

For the purposes of this Regulation, the following definitions apply:

(12) 'intended purpose' means the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;

Risk Classification

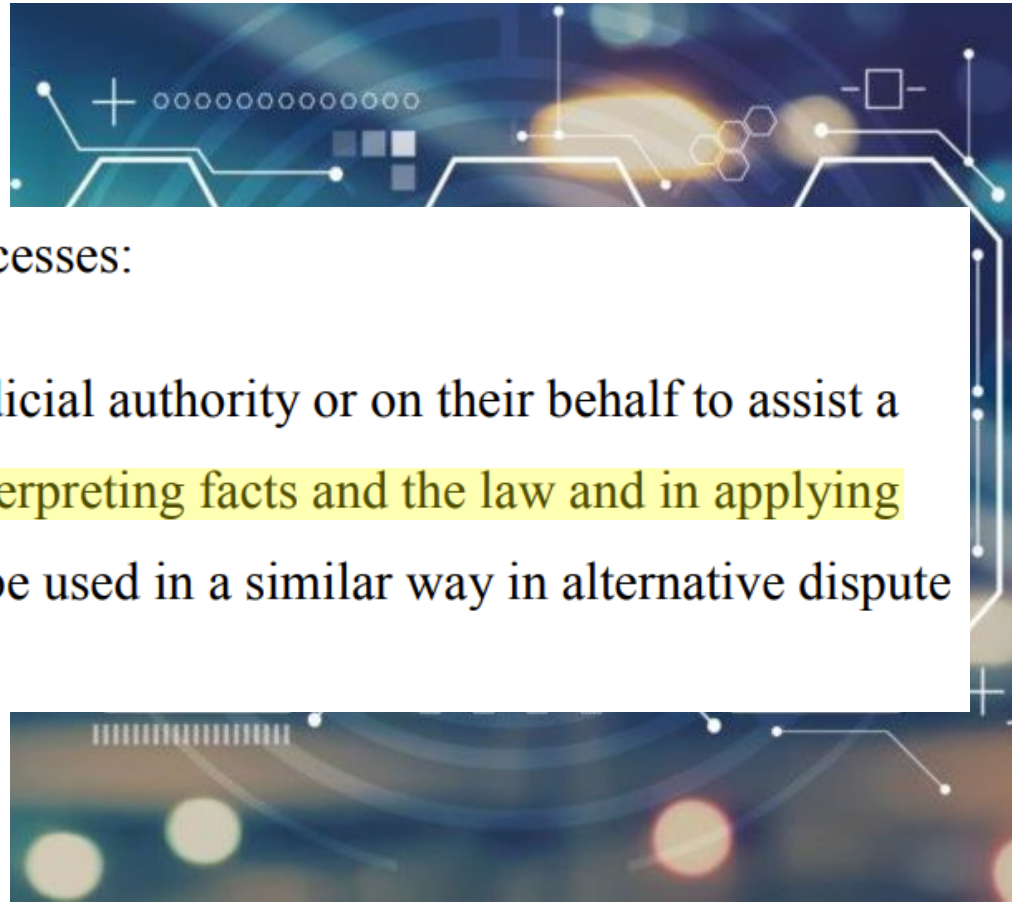
Use Case: Legal Tech

- Analyzes cases and indicates outcome
- Draft claims, motions etc.

Risk Classification

Use Case: Legal Tech

- Analyzes cases and indicates outcome
- Draft claims, motions etc.



8. Administration of justice and democratic processes:

(a) AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts, or to be used in a similar way in alternative dispute resolution;

Risk Classification

Use Case: Legal Tech

- Analyzes cases and indicates outcome
- Draft claims, motions etc.

⇨ Dual use
Judiciary **(+)**
Lawyers **(–)**

⇨ Market and advertise as AI for lawyers ?

Risk Classification

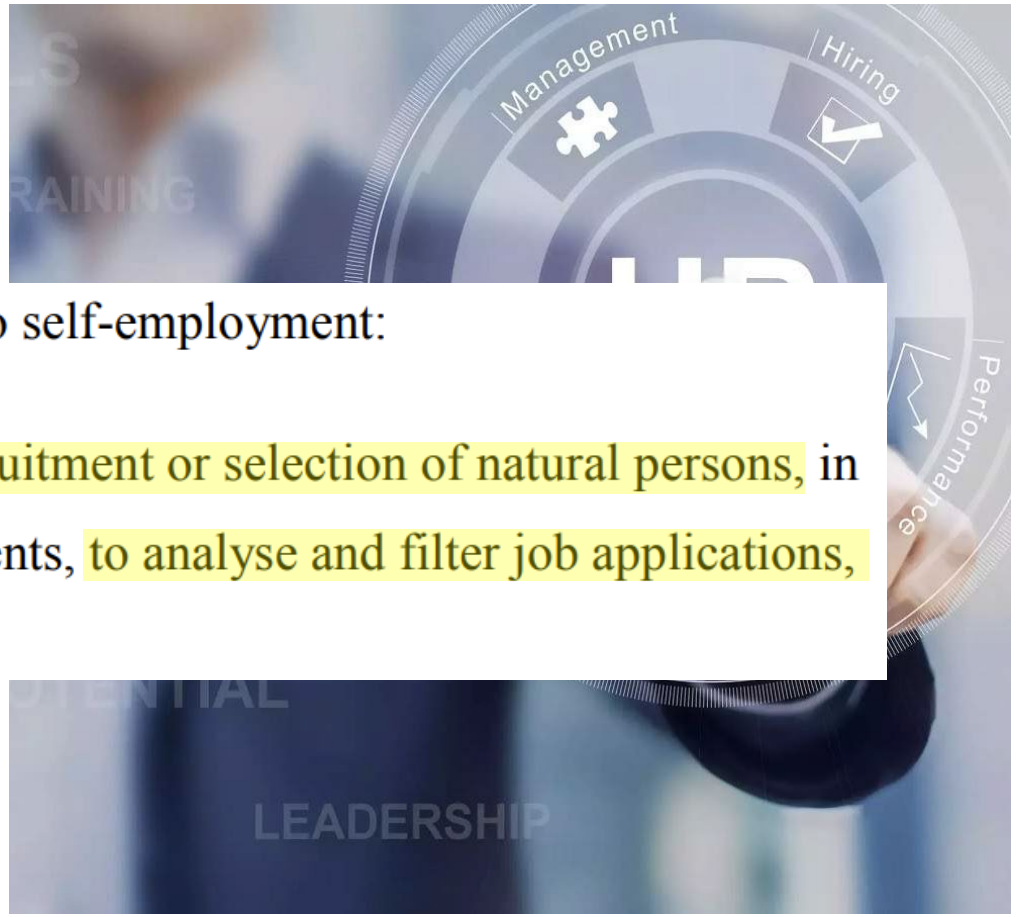
Use Case: Recruitment Tools

- Review CVs
- Check qualifications and keywords

Risk Classification

Use Case: Recruitment Tools

- Review CVs
- Check qualifications and keywords



4. Employment, workers management and access to self-employment:

(a) AI systems intended to be used for the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates;

Risk Classification

Use Case: Recruitment Tools

- Review CVs
- Check qualifications and keywords

⇨ Dual use
Recruitment **(+)**
Internal HR-Tool **(–)**

⇨ Market and advertise as HR-Tool?

Risk Classification

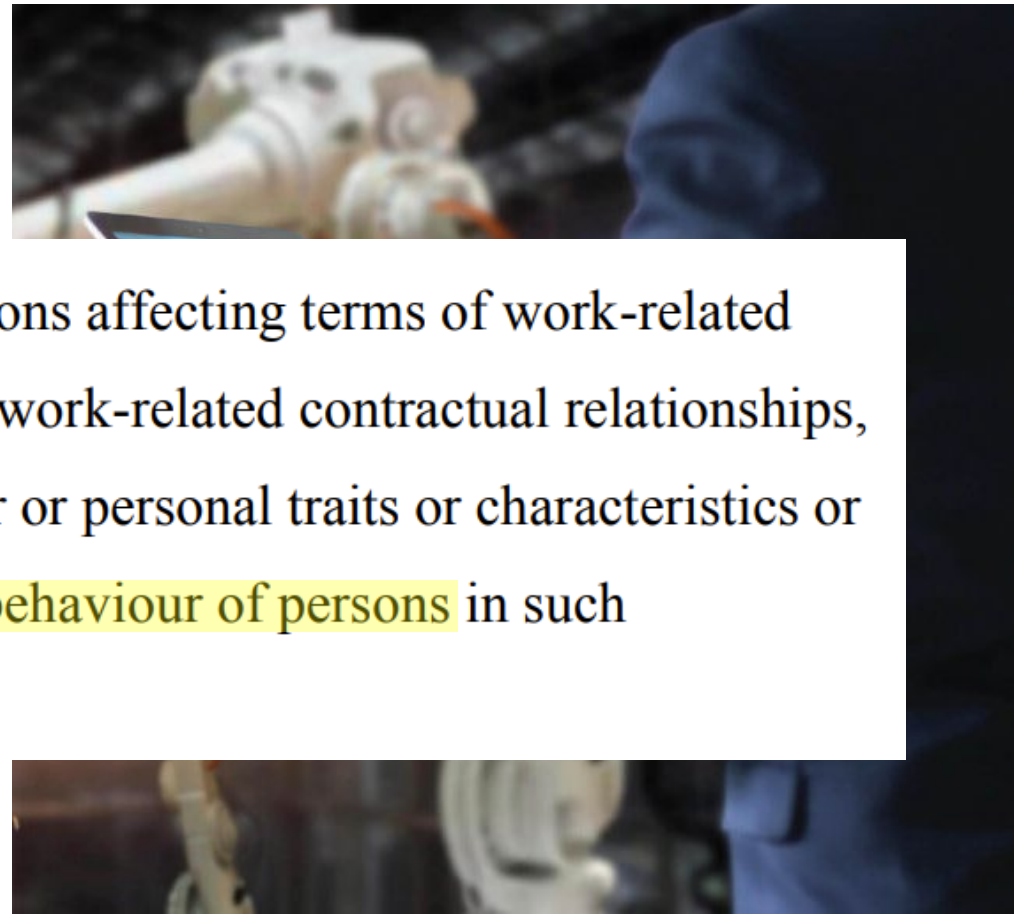
Use Case: Quality Control

- Computer vision for assembly lines
- Checks manufacturing process

Risk Classification

Use Case: Quality Control

- Computer vision for assembly lines
- Checks manufacturing process



(b) AI systems intended to be 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.

Risk Classification

Use Case: Quality Control

- Computer vision for assembly lines
- Checks manufacturing process

⇨ Dual use

Monitor workers **(+)**

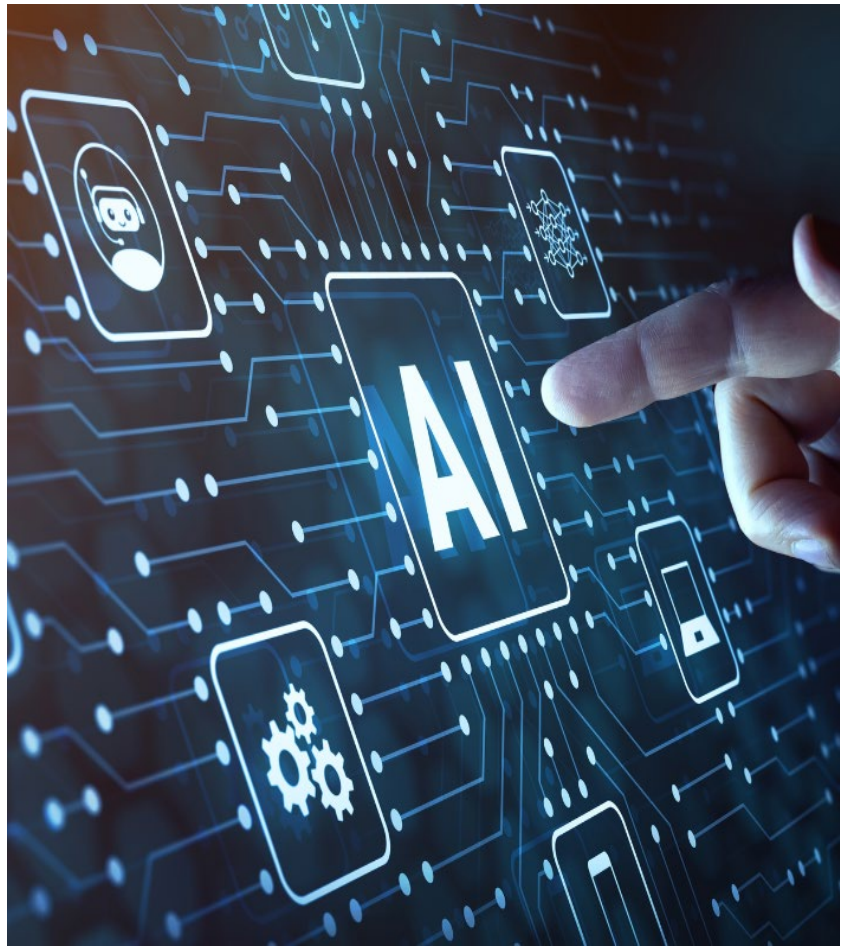
Quality control **(–)**

⇨ Market and advertise as quality control?

Risk Classification

Art. 6 AI Act

1. Products or security system for products listed in Annex I
2. Products listed in Annex III



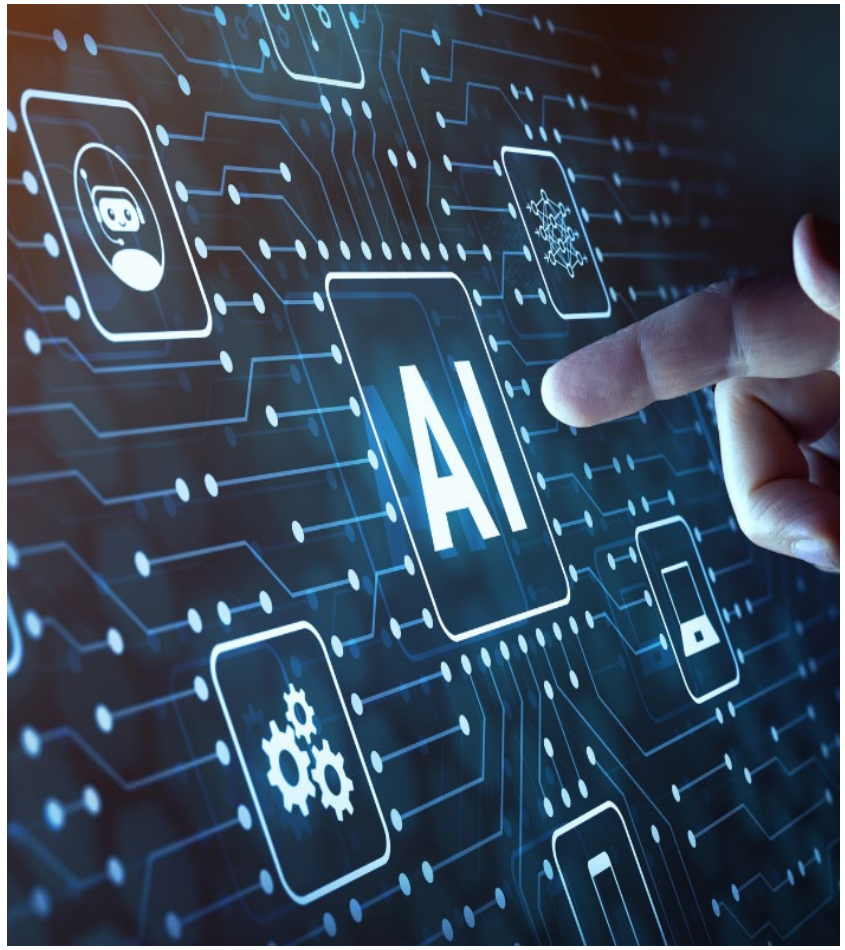
Risk Classification

Art. 6 AI Act

1. Products or security system for products listed in Annex I
2. Products listed in Annex III

Unless AI system only

- performs a narrow task
- improves human work results
- performs preparatory tasks



High Risk AI

Compliance with the AI Act

- Risk Management System
- Quality Management System
- Get CE-Certificate
- Registration in EU Database

Want to know more?

Watch the webinar

HIGH RISK AI

HUMAN CONTROL AS GUIDING PRINCIPLE

Risk Management System

Transparency / Explainability

Data Quality and Governance

Technical Documentation

Cyber Security

Record-keeping

High Risk AI

Risk Management System – **Transparency**

Use Case: Bank loan

- Software to assess the creditworthiness of individuals
- Gives recommendation on grant of loan

High Risk AI

Risk Management System – **Transparency**

Use Case: Bank loan

- Can user recognize dysfunctions ?
- Liability for oversight ?
- Trust bias ?

High Risk AI

Risk Management System – **Transparency**

Use Case: Bank loan

- Can user recog
- Liability for ove
- Trust bias ?

High Risk AI

Risk Management System – **Data Quality and Governance**

Article 10

Data and data governance

High-risk AI systems which make use of techniques involving the training of models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5 whenever such datasets are used.

- ⇨ Use relevant data
- ⇨ Sufficiently representative
- ⇨ Error free and complete (to the extent possible)
- ⇨ Non-biased
- **Publish summary of content**

High Risk AI

Risk Management System – **Data Quality and Governance**

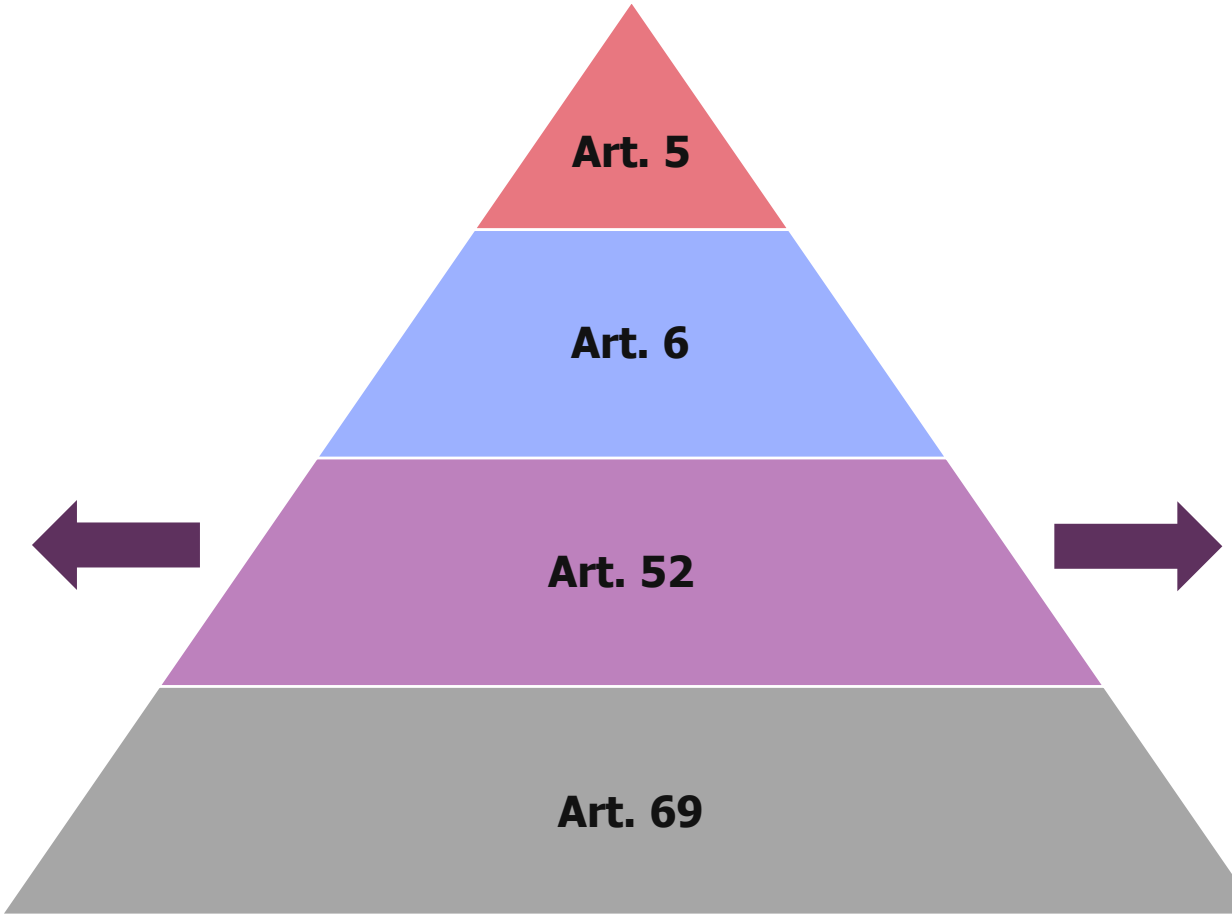
Dataset	Description	Percentage	Total Size (Tokenized)	Tokens
Web Crawls	Large web scrape corpora (e.g. Common Crawl) containing various styles and sources	71%	2,77TB	761,41B
Books	Fiction and non-fiction literature providing well-structured and coherent text on various topics	20%	0,79TB	217,15B
Political and Legal Sources	Data provided by the EU parliament, legislation and speeches	5%	0,18TB	49.47B

Model Card Luminous | Aleph Alpha API (aleph-alpha.com)

Risk Classification

Interactive AI

GenAI,
Chatbots,
Videogames



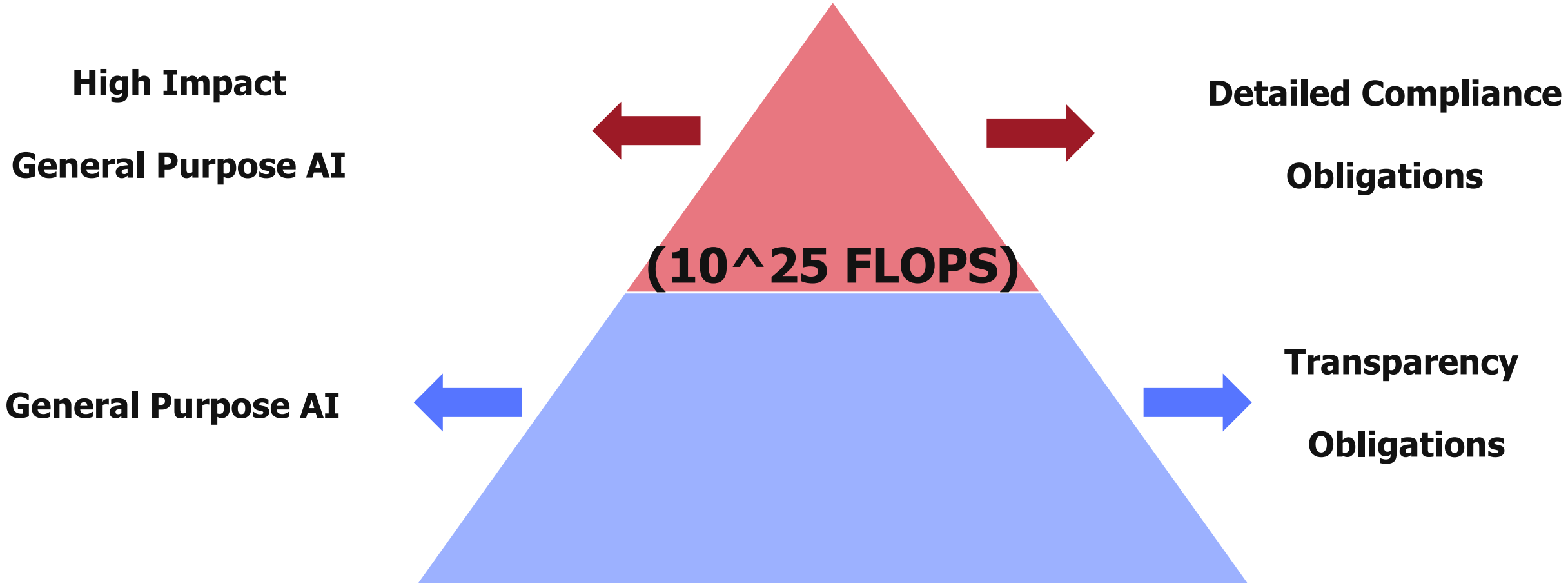
Transparency

Obligations

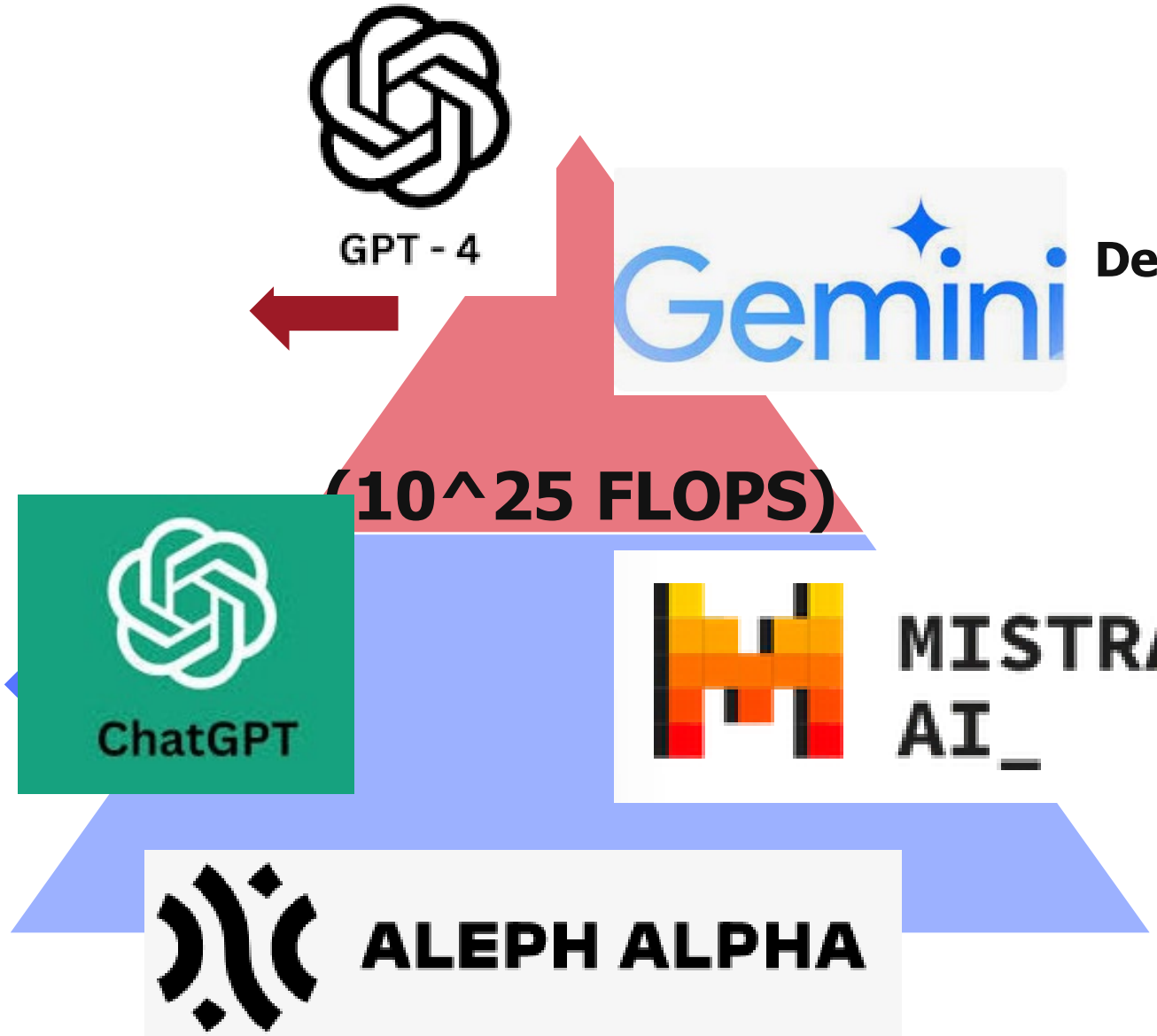
DEEP FAKES

CHATBOTS

General Purpose AI



General Purpose AI



High Impact General Purpose AI

Detailed Compliance Obligations

General Purpose AI

nsparency ligations

General Purpose AI

Transparency Obligations

- Disclose technical documentation to B2B customers
- Enable B2B customers to comply with AI Act

Texta.ai

Rytr

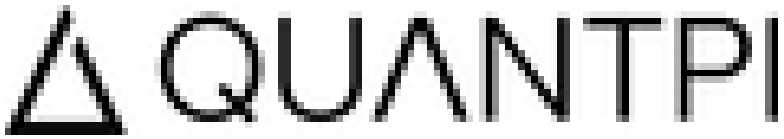
Jasper

copysmith

Writesonic

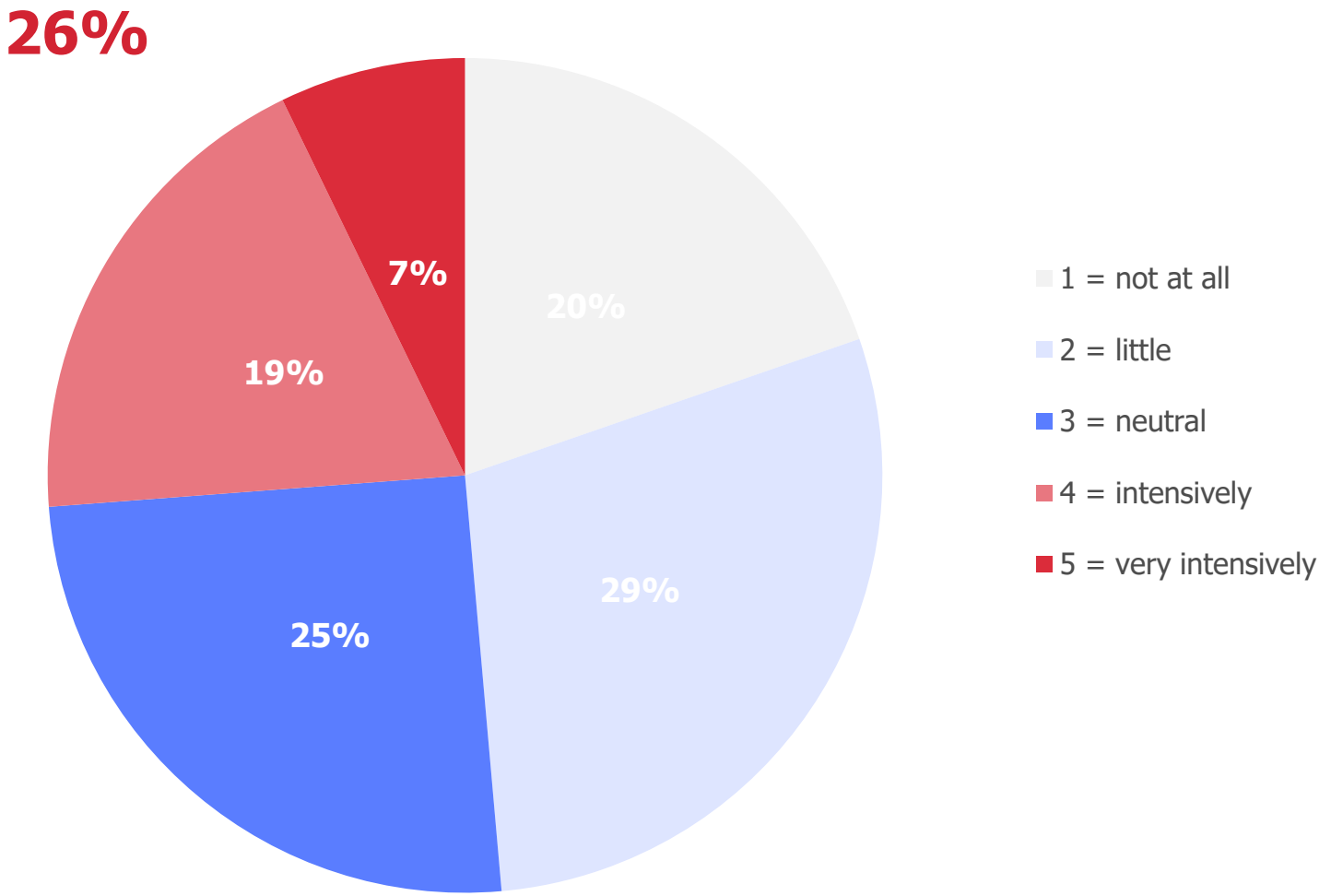
Brain Drain or …

… Steering Innovation to Explainable AI?



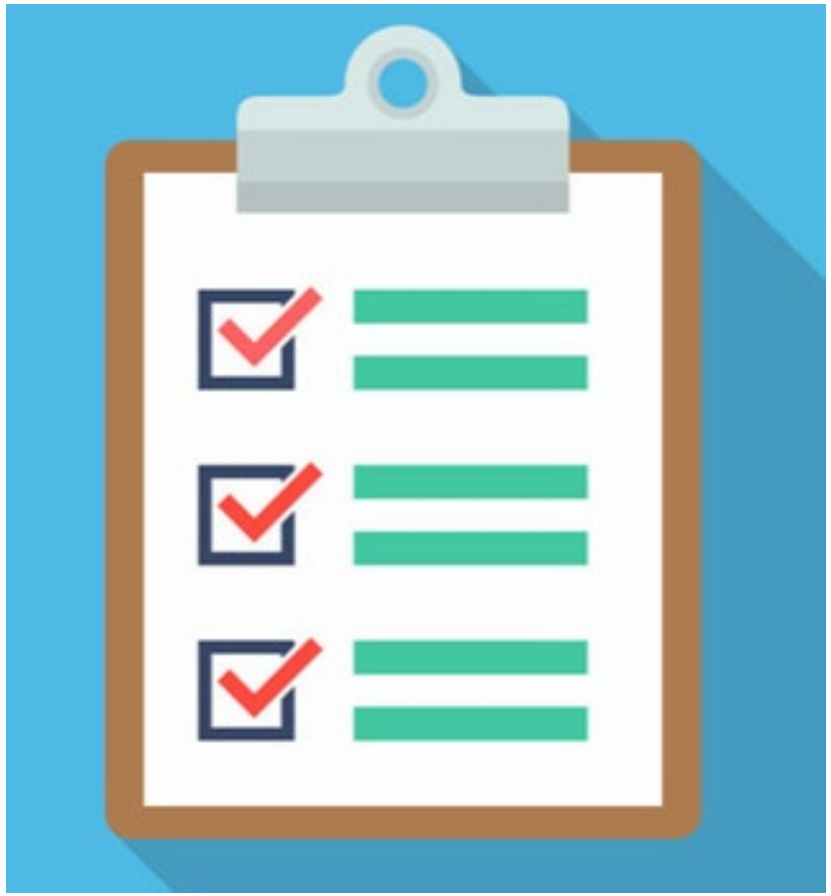
Survey AI Act

On a scale of 1 to 5, how intesively is your company engaging with the AI Act ?



SOURCE: Deloitte AI Act Survey 2024

Get ready now!



1. Create Responsibilities on C-Level
2. Educate Employees / Create Guidelines
3. Create Record of AI Systems
4. Conduct Risk Classification
5. Create Gap Analysis

Thanks for listening!

Dr. Benedikt Flöter
LinkedIn


YPOG