

WEBINAR

Deep-dive into artificial intelligence and data ecosystems: the regulatory approach of the European Union

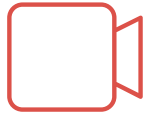
The logo for Data Europa Academy is located in the bottom left corner. It consists of the text "data.", "europa", and "academy" stacked vertically in a white, sans-serif font. The text is set against a dark blue circular background. To the right of this circle is a white circle, and both are partially enclosed by a larger, light grey circle that overlaps the bottom left edge of the slide.

data.
europa
academy

02 February 2024

10.00 — 11.30 CET

Rules of the game



The webinar will be recorded



For questions, please use the ClickMeeting chat.



Please reserve 3 min after the webinar to help us improve by filling in our feedback form

Introduction



Hans Graux

Lawyer IP, IT and data protection
law, Partner at Timelex



Eleni Kosta

Professor of Technology Law and Human
Rights at the Tilburg Institute for Law



Pieter Gryffroy

Lawyer, data protection and
privacy at Timelex

Agenda

10.00 – 10.10	Opening and introduction – <i>Hans Graux</i>
10.10 – 10.40	An introduction to the AI Act – <i>Eleni Kosta</i>
10.40 – 11.10	Risk management & the draft AI act – <i>Pieter Gryffroy</i>
11.10 – 11.25	Q&A session
11.25 – 11.30	Closing statements

An introduction to the AI Act

Eleni Kosta



AN INTRODUCTION TO THE AI ACT

WEBINAR DEEP-DIVE INTO AI AND DATAECOSYSTEMS: THE REGULATORY APPROACH OF THE EU

Prof. dr. Eleni Kosta

02.02.2024

Political deal achieved

Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI

Press Releases IMCO LIBE 09-12-2023 - 00:04

- Safeguards agreed on general purpose artificial intelligence
- Limitation for the use of biometric identification systems by law enforcement
- Bans on social scoring and AI used to manipulate or exploit user vulnerabilities
- Right of consumers to launch complaints and receive meaningful explanations
- Fines ranging from 35 million euro or 7% of global turnover to 7.5 million or 1.5% of turnover

MEPs reached a political deal with the Council on a bill to ensure AI in Europe is safe, respects fundamental rights and democracy, while businesses can thrive and expand.

On Friday, Parliament and Council negotiators reached a provisional agreement on the Artificial Intelligence Act. This regulation aims to ensure that fundamental rights, democracy, the rule of law and environmental sustainability are protected from high risk AI, while boosting innovation and making Europe a leader in the field. The rules establish obligations for AI based on its potential risks and level of impact.

AI Act

2021/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE

(ARTIFICIAL INTELLIGENCE ACT) AND AMENDING DIRECTIVE 2008/48/EC OF THE

LEGISLATIVE PROCEDURE

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee¹,

Having regard to the opinion of the European Central Bank²,

Having regard to the joint opinion of the European Data Protection Board and the European Data Protection Supervisor,

Having regard to the opinion of the Committee of the Regions³,

Acting in accordance with the ordinary legislative procedure,

Leaked

Subject matter

The purpose of this Regulation is to **improve the functioning of the internal market** and promoting the **uptake of human centric and trustworthy artificial intelligence**, while ensuring a **high level of protection of health, safety, fundamental rights** enshrined in the Charter, including democracy, rule of law and environmental protection against harmful effects of artificial intelligence systems in the Union and supporting innovation.

This Regulation lays down:

- (a) harmonised rules for the **placing on the market, the putting into service and the use of artificial intelligence systems** ('AI systems') in the Union;
- (b) **prohibitions of certain artificial intelligence practices**;
- (c) specific **requirements for high-risk AI systems** and **obligations** for operators of such systems;
- (d) harmonised **transparency rules** for certain AI systems;
- (da) harmonised rules for the placing on the market of **general-purpose AI models**;
- (e) rules on **market monitoring, market surveillance governance and enforcement**;
- (ea) measures to **support innovation**, with a particular focus on SMEs, including start-ups;

Scope

This Regulation applies to:

- (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 who are located within the Union or in a third country;
- (b) **deployers** of AI systems that have their place of establishment or who are located within the Union;
- (c) **providers and deployers** of AI systems that have their place of establishment or who are located **in a third country**, where the output produced by the system is used in the Union;
- (ca) **importers and distributors** of AI systems;
- (cb) **product manufacturers** placing on the market or putting into service an AI system together with their product and under their own name or trademark;
- (cc) **authorised representatives of providers**, which are not established in the Union.
- (cc) **affected persons** that are located in the Union.

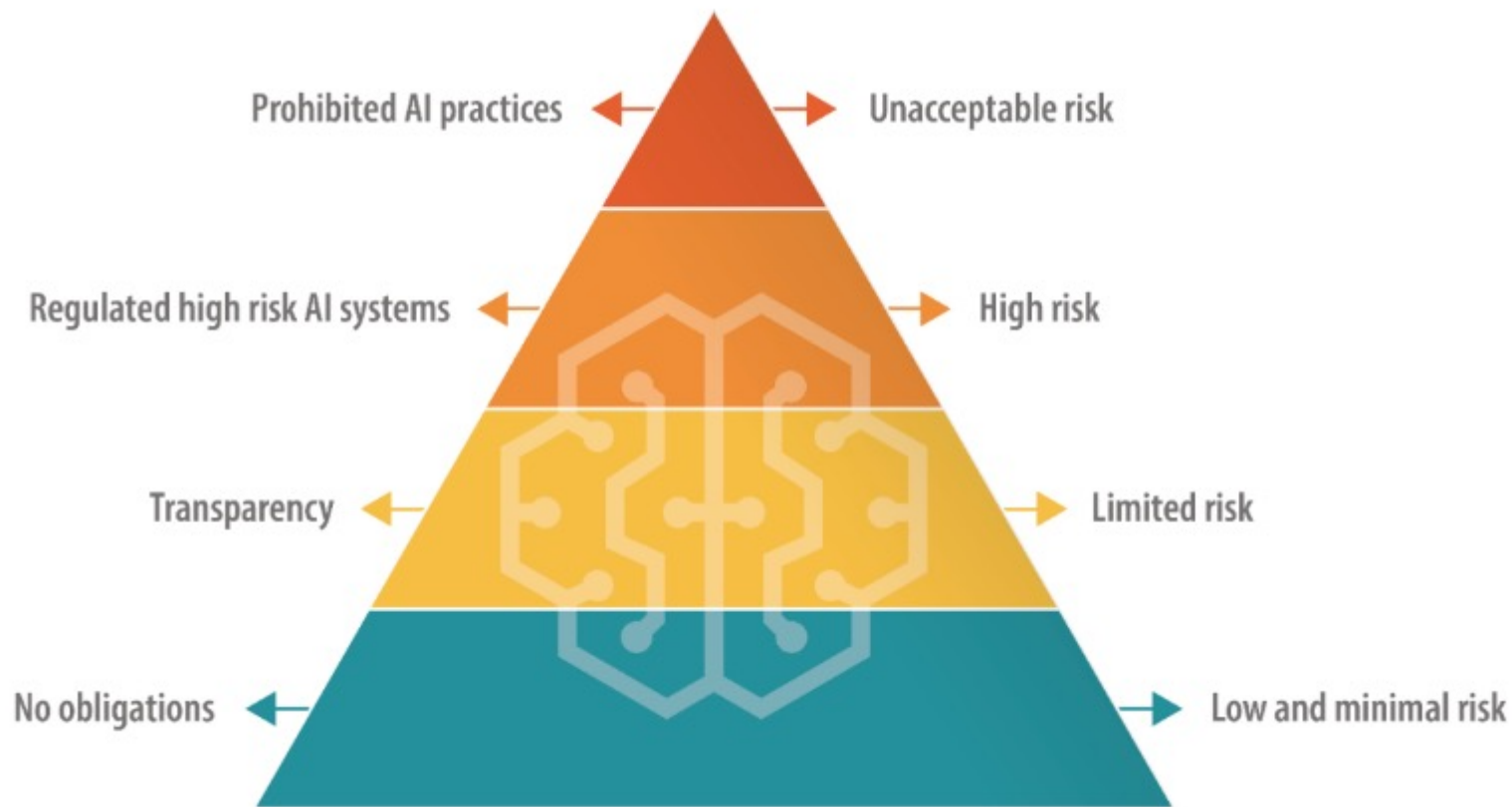
AI Regulation

Risk based regulation

High-risk AI systems and non-high risk

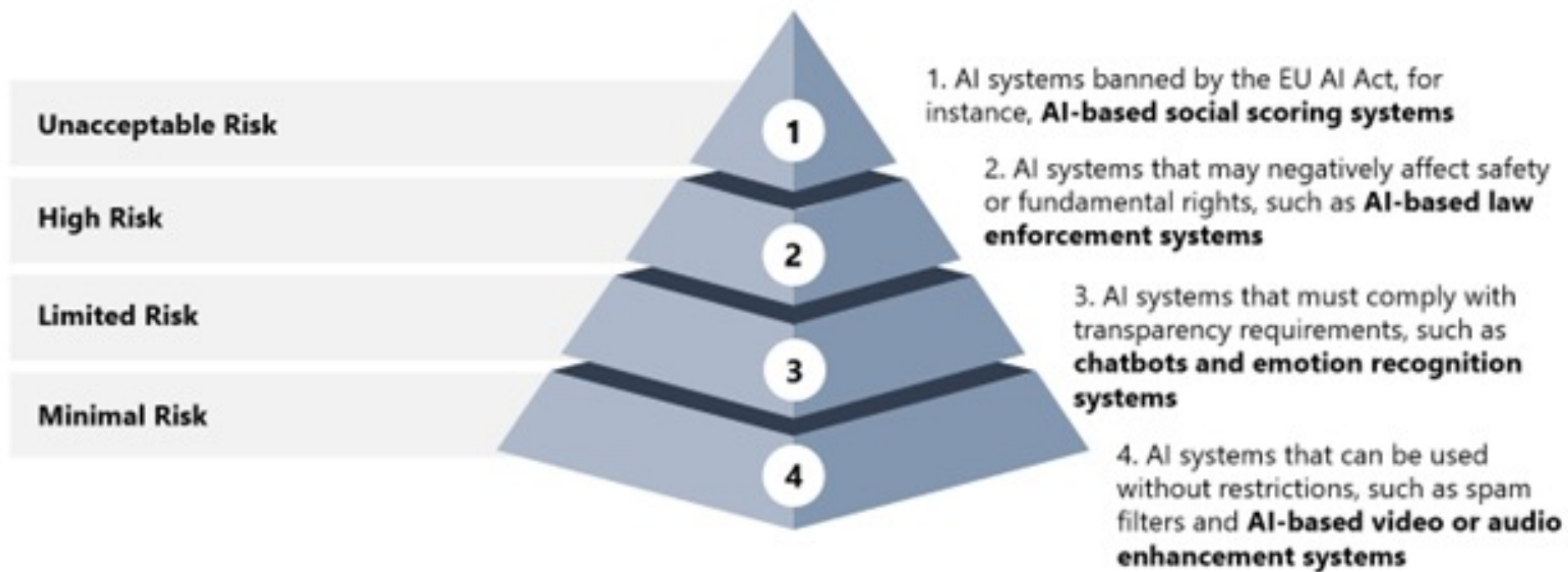


different requirements depending on the level of risk



Data source: [European Commission](#).

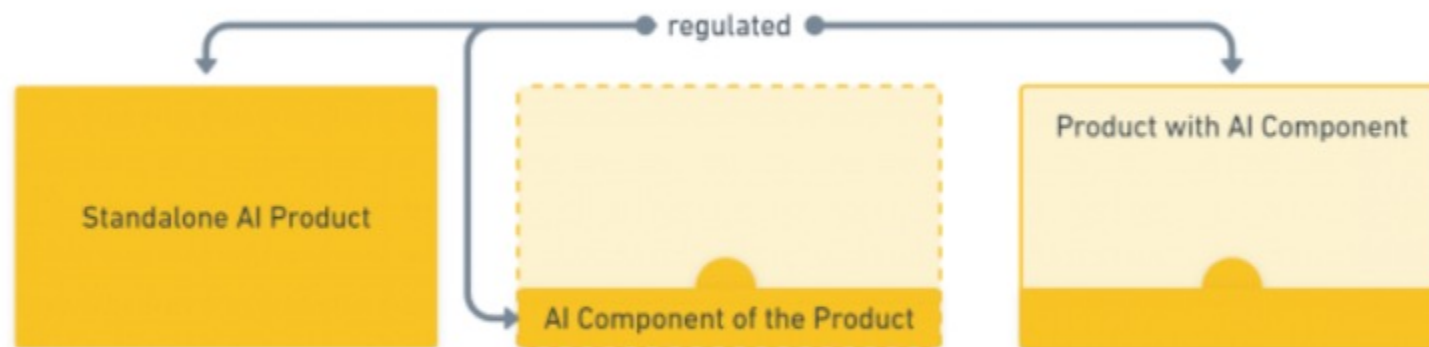
AI Act Risk Levels



What is high risk

AI system could be considered “high-risk” irrespectively of whether it is a **component** of another system or whether it is put into service independently as a **standalone product**.

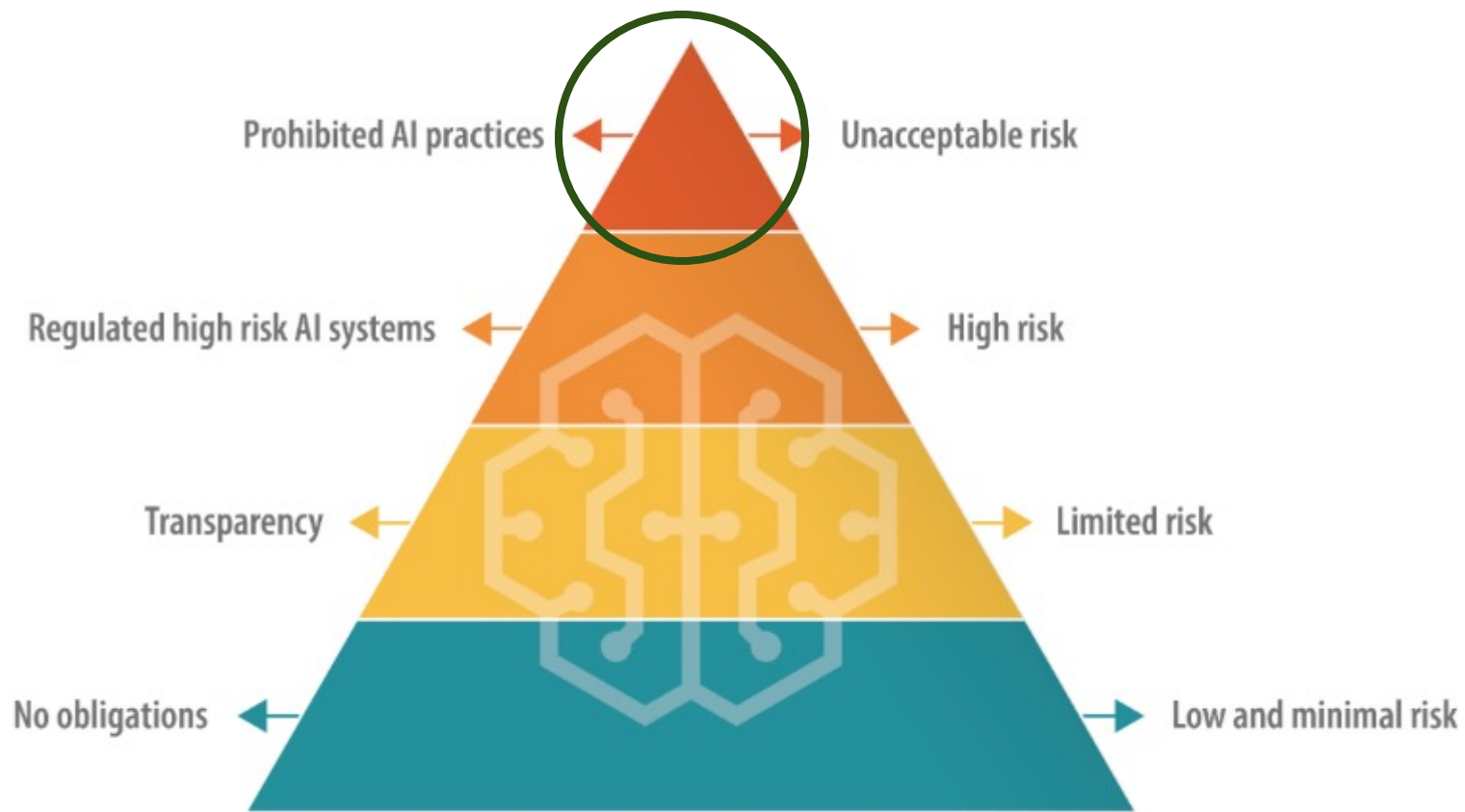
What is regulated



Nikita Lukianets, <https://futurium.ec.europa.eu/en/european-ai-alliance/open-discussion/more-visual-guide-proposed-eu-artificial-intelligence-act>

AI system

An 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.



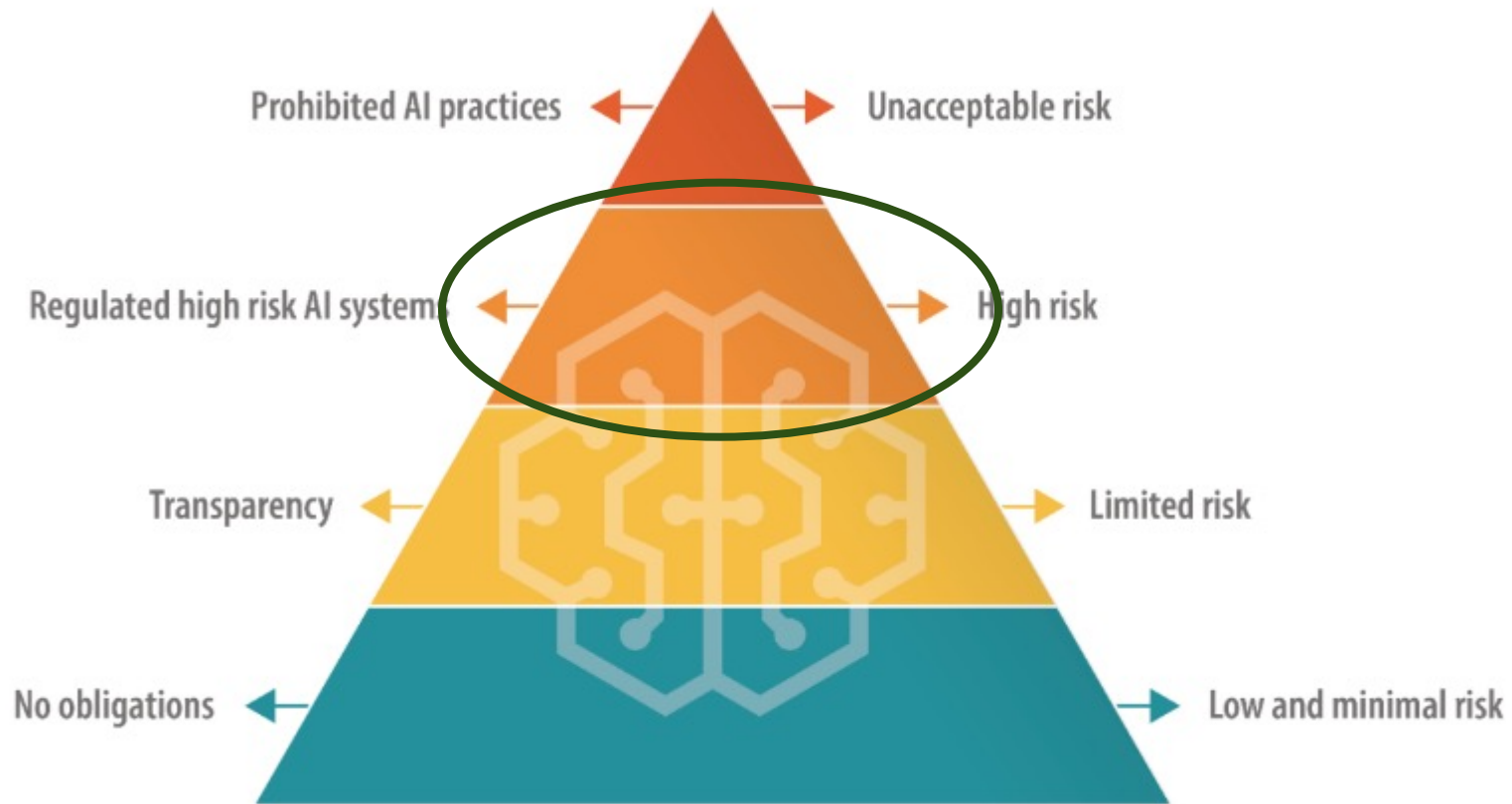
Data source: [European Commission](#).

Prohibited AI practices

- ❑ AI systems that **manipulate human behaviour** to circumvent their free will;
- ❑ **AI used to exploit the vulnerabilities of people** (due to their age, disability, social or economic situation)
- ❑ **biometric categorisation systems** that use **sensitive characteristics** (e.g. political, religious, philosophical beliefs, sexual orientation, race)
- ❑ **social scoring** based on social behaviour or personal characteristics

Prohibited AI practices

- ❑ **untargeted scraping of facial images** from the internet or CCTV footage to create facial recognition databases;
- ❑ **emotion recognition** in the **workplace** and **educational** institutions;
- ❑ **law-enforcement use of real-time biometric identification** in publicly accessible spaces, for
 - **targeted searches** of victims (abduction, trafficking, sexual exploitation, missing persons),
 - 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**, or
 - the localisation or identification of a person **suspected of having committed** one of the specific crimes mentioned in the regulation (e.g. terrorism, trafficking, sexual exploitation, murder, kidnapping, rape, armed robbery, participation in a criminal organisation, environmental crime) for the purposes of conducting a criminal investigation, prosecution or executing a criminal penalty for offences.



Data source: [European Commission](#).

High risk AI systems

6(1). Irrespective of whether an AI system is placed on the market or put into service independently from the products referred to in points (a) and (b), that AI system shall be considered 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 itself is a **product** subject to existing safety standards and assessments, such as toys, vehicles or medical devices (**Annex II**); or,
- (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 putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II;

High risk AI systems

Annex II

LIST OF UNION HARMONISATION LEGISLATION

Part I

Section A. List of Union harmonisation legislation based on the New Legislative Framework

1. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (OJ L 157, 9.6.2006, p. 24) [as repealed by the Machinery Regulation];
2. Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p. 1);
3. Directive 2013/53/EU of the European Parliament and of the Council of 20 November 2013 on recreational craft and personal watercraft and repealing Directive 94/25/EC (OJ L 354, 28.12.2013, p. 90);
4. Directive 2014/33/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to lifts and safety

High risk AI systems

6(2) AI systems referred to in Annex III shall also be considered high-risk

Annex III

HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:

1. Biometrics, insofar as their use is permitted under relevant Union or national law
 - (a) Remote biometric identification systems.

This shall not include AI systems intended to be used for biometric verification whose sole purpose is to confirm that a specific natural person is the person he or she claims to be;
 - (aa) AI systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics.
 - (ab) AI systems intended to be used for emotion recognition;
2. Critical infrastructure:
 - (a) AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic and the supply of water, gas, heating and electricity.
3. Education and vocational training:

High risk AI systems

Annex III

System is used for a specific **sensitive purpose**, falling within the following high-level areas :

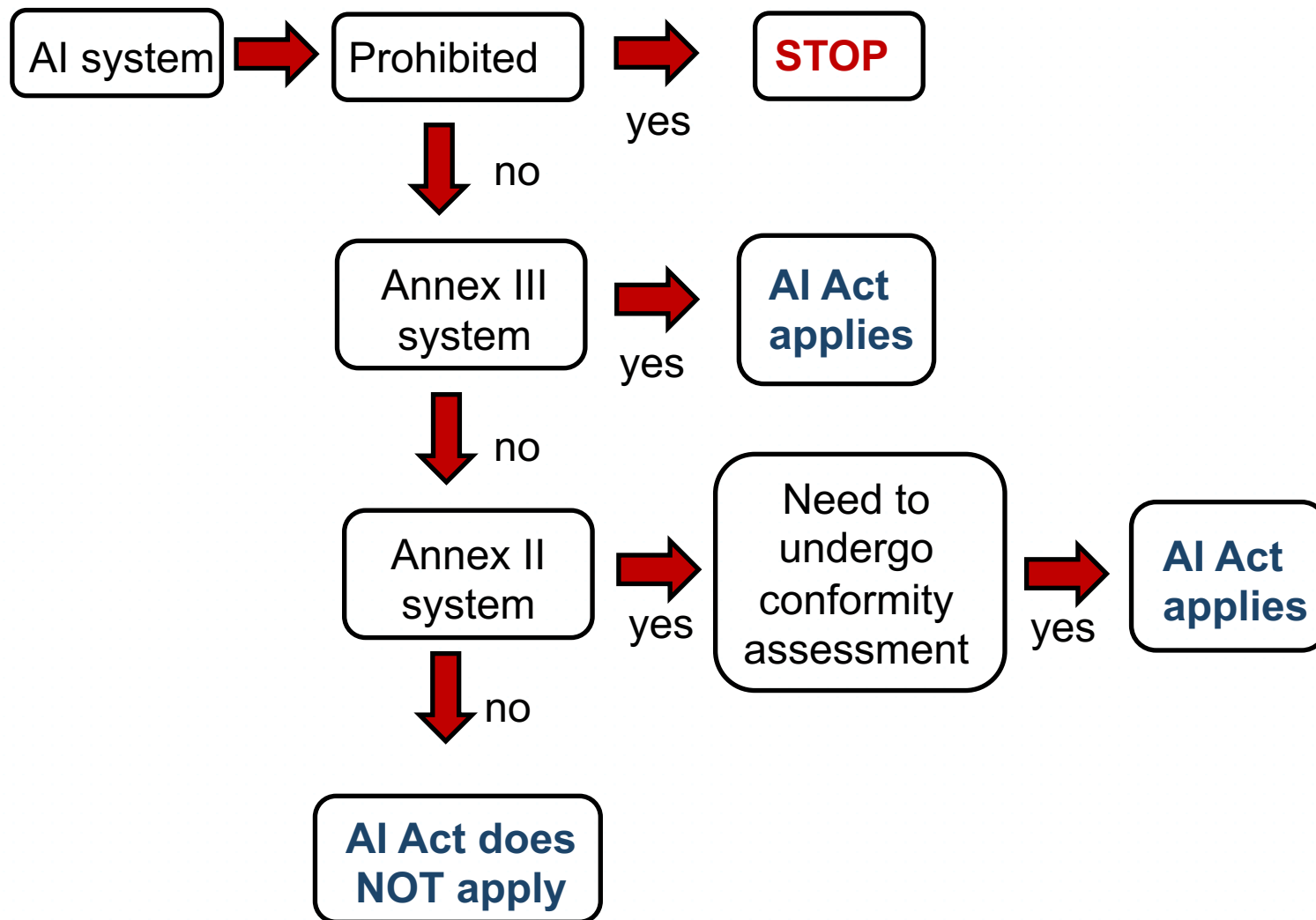
- Biometrics
- Critical infrastructure management (e.g. water, gas, electricity etc.)
- Education and vocational training
- Employment, workers management and access to self-employment
- Access to essential services (e.g. insurance, banking, credit, benefits etc.)
- Law enforcement
- Migration, asylum and border control management
- Administration of justice and democratic processes
- AI systems used to influence the outcome of elections and voter behaviour

General purpose AI systems

- **General-purpose AI (GPAI) systems**, and the GPAI models they are based on, will have to adhere to *transparency* requirements:
 - ✓ drawing up technical documentation,
 - ✓ drawing up documentation to providers of AI systems
 - ✓ complying with EU copyright law
 - ✓ disseminating detailed summaries about the content used for training...

General purpose AI systems

- **Stricter obligations** for [**high-impact**] **GPAI models with systemic risk** (*foundation models trained with large amount of data and with advanced complexity, capabilities, and performance well above the average, which can disseminate systemic risks along the value chain*) that will eventually be required to conduct model evaluations, assess and mitigate systemic risks, conduct adversarial testing, report to the Commission on serious incidents, ensure cybersecurity and report on their energy efficiency...
- **Generative AI:**
 - users must be informed when interacting with AI (e.g. chatbots)
 - Information about the operation of the system and processing of personal data
 - AI content must be labelled and detectable (e.g. deepfakes).



An oversimplified flow diagram on high risk systems

High-risk AI systems – requirements

- Fundamental Rights Impact Assessment
- Conformity Assessment
- Implementation of risk management and quality management system
- Data governance obligations (e.g. bias mitigation, representative training data etc.)
- Transparency obligations (e.g. instructions for use, technical documentation)
- Human oversight (e.g. explainability, auditable logs, human-in-the-loop etc.)
- Accuracy, robustness and cybersecurity obligations (e.g. testing and monitoring)

Conformity assessment

- Following the example of 'New Approach' legislation (e.g. medical devices): assessment by accredited third party or self-assessment and CE Marking.
- Harmonised European standards will be developed by the European standardisation organisations (CEN, CENELEC, ETSI) to cover the requirements of the Regulation.

Conformity assessment

New rules for providers of high-risk AI systems

Step 1



A high-risk AI system is developed

Step 2



It needs to undergo the conformity assessment

and comply with AI requirements

For some systems a notified body is involved

Step 3



Registration of stand-alone AI systems in an EU database

Step 4



A declaration of conformity

needs to be signed and the AI system should bear

the CE marking. The

system can be placed on the

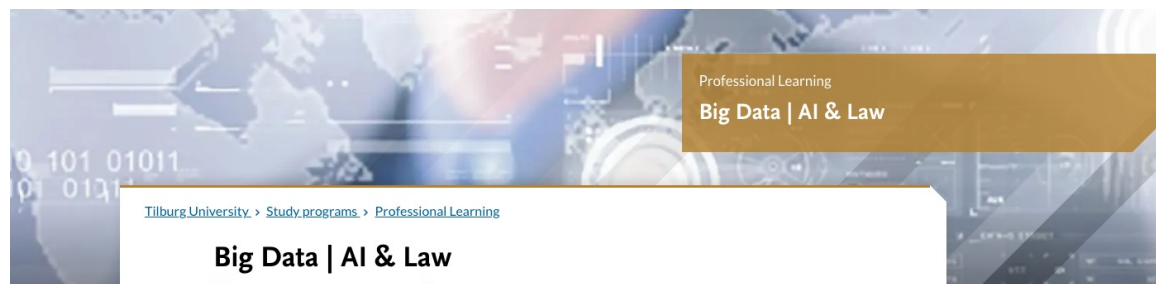
market

If substantial changes happen in the AI system's lifecycle, go

back to Step 2

Once the AI system is on the market, authorities are in charge of the market surveillance, users ensure human oversight and monitoring, while providers have a post-market monitoring system in place. Providers and users will also report serious incidents and malfunctioning.

Antonella Zara



Professional Learning
Big Data | AI & Law

[Tilburg University](#) > [Study programs](#) > [Professional Learning](#)

Big Data | AI & Law

📅 Date: 20th November 2023 📍 Location: Tilburg

The program Big Data | AI & Law offers you a broad spectrum on the legal, regulatory and ethical issues that arise with the development and use of Big Data and Artificial Intelligence.

During this program, you will get a comprehensive view on the latest developments in Big Data and Artificial Intelligence (AI) related to the law and legal practice, including how to apply GDPR in all phases of the development and deployment of AI systems, and what risk management tools are required to ensure Algorithmic Accountability.

We will fully cover the draft proposal for an EU Regulation laying down harmonized rules on artificial intelligence (draft Artificial Intelligence Act) that was presented by the European Commission in April 2021. Having followed this program, you have an up-to-date understanding of the privacy, data protection and ethical challenges of Big Data and Artificial Intelligence and you will be able to apply law and regulations when dealing with such technologies.

This program will be offered at the Faculty Club of Tilburg University.

[Register now for Big Data | AI & Law](#) →

Become an expert in the field of both big data and law

Having followed the Big Data | AI & Law program, you will be acquainted with the legal issues in relation to the data revolution including topics like the GDPR, Algorithmic Accountability and responding to ethical dilemmas. You will know exactly which role Big Data and AI are taking in today's legal landscape and know how to deal with Big Data and AI related legal and ethical issues in everyday practice. You will familiarize yourself with the EC proposal for an AI Regulation and be able to follow the relevant legislative developments.

Application form Big Data | AI & Law (June 3, 10, 17, and 24, 2024)

rilt

Tilburg Institute
for Law, Technology,
and Society



Thank you for your attention!

Prof. Dr. Eleni KOSTA
e.kosta@tilburguniversity.edu

Professor of Technology Law and Human Rights
Tilburg Institute for Law, Technology, and Society (TILT)
Tilburg University



ilt

Tilburg Institute
for Law, Technology,
and Society



Thank you for your attention!

Prof. Dr. Eleni KOSTA
e.kosta@tilburguniversity.edu

Professor of Technology Law and Human Rights
Tilburg Institute for Law, Technology, and Society (TILT)
Tilburg University



ilt

Tilburg Institute
for Law, Technology,
and Society

“Post-remote” biometric identification systems

- “**Post-remote**” biometric identification systems would be used strictly in the **targeted search** of a person **convicted or suspected** of having committed a serious crime.

Risk management & the draft AI

Pieter Gryffroy



RISK MANAGEMENT & THE DRAFT AI ACT

Pieter Gryffroy

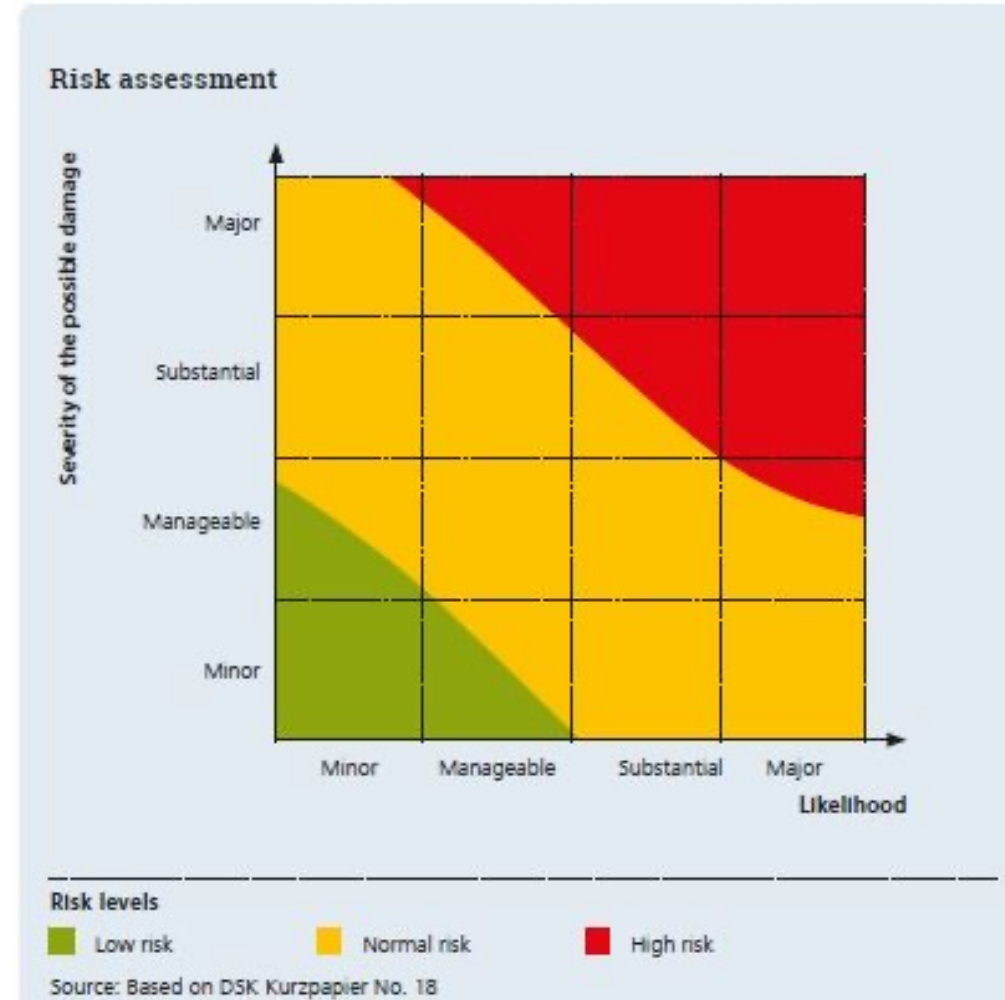
2 February 2023



Follow us on LinkedIn / www.linkedin.com/company/timelex

WHAT IS RISK?

- “Risk means the combination of the probability of an occurrence of harm and the severity of that harm”
- So, risk = severity x likelihood of a certain harm
- ‘Harm might be material or immaterial, including physical, psychological, societal or economic harm.’



	Risk Impact			
	Negligible	Limited	Significant	Maximum
Likelihood	1	2	3	4
A (maximum)	M	H	E	E
B (significant)	M	H	H	E
C (limited)	L	M	H	E
D (negligible)	L	L	M	H

Key	Description
E	Extreme Risk: Immediate action required to mitigate the risk.
H	High Risk: Action should be taken to compensate for the risk.
M	Moderate Risk: Action should be taken to monitor the risk.
L	Low Risk: Routine acceptance of the risk.

HARM TO WHAT EXACTLY?

- **Health, safety and fundamental rights** (and freedoms) of natural persons
- But also mentioned in the act: to public interests (including not only public health and safety but also economic interests, social interest property, critical infrastructure, etc.)
- Hence: an impact assessment of AI might cover lots of aspects of risk:
 - Impact on fundamental/human rights
 - Ethical values (underlying legislation, policy & guidance, mission statement, funder requirements)
 - Social impact
 - Economic impact
 - Impact on compliance with sectoral legislation (health & safety), or legislation implementing fundamental rights (data protection law), or applicable standards

COMMON RISK SOURCES TO CONSIDER

- Internal vs. external
- Accidental vs. deliberate

Human factor (aka weak link)

- Management/organizational measures are missing
- Lack of knowledge/understanding/AI literacy
- Lack of governance
- Lack of oversight

Technical challenges

- Functionality/fit for purpose
- Data quality
- Issues with accuracy, robustness, consistency

Cybersecurity vulnerabilities

Other: e.g. natural disasters

AI ACT – A RISK-BASED APPROACH

- Predetermination of certain types of AI or uses of AI as having a certain inherent risk level
 - Forbidden uses of AI: risk too high, even with safeguards
 - Examples: emotion recognition in the workplace or education
 - High risk AI systems: high risk, but if safeguards of the AI act are observed (e.g. by the mandatory risk management system), risk can be mitigated, and the use allowed in that case
 - Examples: AI as safety components, critical infrastructure, law enforcement uses e.g. for remote biometric identification or profiling natural persons
 - Narrow exceptions from the list in Annex III under conditions that lower the impact, e.g. the system is intended to improve the result of a previously completed human activity or is meant for a preparatory task; provider must document such assessment

AI ACT – A RISK-BASED APPROACH (2)

- Limited risk: certain AI systems that pose a specific risk of not being recognized as such must disclose that the person is interacting with AI (transparency), but are otherwise not inherently high risk for this reason
 - Examples: AI that interacts with users directly, deep fakes
- General purpose AI systems: distinction between systemic risk and non-systemic risk
 - Transparency obligations on how the model works for all types
 - For systemic risks: additional obligations on cybersecurity, evaluation of the model, incident reporting and of course: assessing and mitigating the risk.
 - Examples: GPT-4 (ChatGPT), Llama-2
- Minimal or no risk (or more accurately “other”): residual category with no compliance obligations under the AI Act (but ethics etc. may apply)

RISK CAN PRESENT ITSELF AS PART OF

- The design of the AI system (providers), to mitigate this there are several obligations for high-risk AI systems:
 - The risk management system proper in Art. 9 of the draft (**more detail on this later**)
 - Data quality & governance
 - Technical documentation
 - Transparency
 - Human oversight
 - Accuracy, robustness and cybersecurity

RISK CAN PRESENT ITSELF AS PART OF (2)

- The deployment of the AI system (deployers), by putting the system in a given setting, obligations for high-risk AI systems focus on:
 - Correct use of AI in accordance with instructions + technical and organizational measures to ensure this
 - Human oversight with appropriate competence and training + support
 - If input data control: relevant and sufficiently representative
 - Monitoring, logging
 - Obligation to report
 - Issues related to post market-monitoring of the model by the provider (i.e. unknown risks)
 - Serious incidents
 - AI systems presenting risks at a national level (correction/withdrawal/recall procedure)
 - Explicit mention of DPIA.
 - This may also require indirectly a risk assessment to determine how to guarantee this internally

RISK CAN PRESENT ITSELF AS PART OF (3)

- The use of the AI system (especially relevant with GPAI)
 - Addressed by obligations for GPAI with systemic risk

AI ACT – RISK MANAGEMENT OBLIGATIONS

- Art. 9 risk management system, applicable to **providers** of high-risk AI systems:
 - Continuous iterative process
 - To identify **known and reasonably foreseeable risks** that the AI can pose to health, safety and fundamental rights
 - To identify **risks that may emerge from reasonably foreseeable misuse**
 - Testing to ensure that the AI performs consistently for the intended purpose and are compliance with high-risk requirements (data quality, governance, transparency, oversight, accuracy, robustness, cybersecurity)
 - Testing to identify appropriate and targeted risk management measures
 - **Goal: to make sure residual risk for hazards is at an acceptable level**
 - Focus on risks which may be reasonably mitigated or eliminated through the development or design of the high-risk AI system, or the provision of adequate technical information

AI ACT – RISK MANAGEMENT OBLIGATIONS (2)

- Also: Art. 61 of the draft: post-market monitoring by **providers** of the functioning of the high-risk AI system, compliance with high-risk requirements and of risk
 - “**Other possibly arising risks**” that are identified here must be part of art. 9 risk management system
 - Deployers must monitor and report risks as well
- For **providers** of GPAI with systemic risk: specific analysis of this risk to assess and mitigate the systemic risk + specific mention of cybersecurity risk and physical infrastructure
- Article 29a of current draft: fundamental rights impact assessment for high-risk systems to be conducted by certain **deployers** (public bodies, private bodies providing public services, essential services) **upon first use**
 - Explicit link made to DPIA (no duplication)
 - Explicit mention of questionnaire template to be developed by AI office

WHO MUST ASSESS RISK?

- Certainly:
 - Providers of high-risk AI
 - Providers of GPAI with systemic risk
 - Public deployers/public and essential services of high-risk AI system (Art. 29a)
- Deployers of high-risk systems: also a good idea to conduct an assessment, to ensure own obligations are met
- But also in other circumstances:
 - As good practice
 - As part of compliance with national rules, sectoral rules, other EU legislation (e.g., DPIA under data protection law)
 - For other reasons, e.g. when mandated by contract (e.g. acceptable use policies and requirements for risk/impact assessment), as part of a due diligence, as part of certification efforts, etc.
 - This may include AI systems that are not high risk as well, if the deployment is risky for other reasons

HOW TO GO ABOUT MANAGING RISK IN PRACTICE?

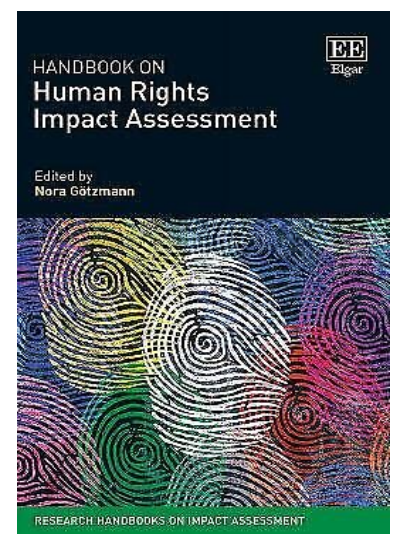
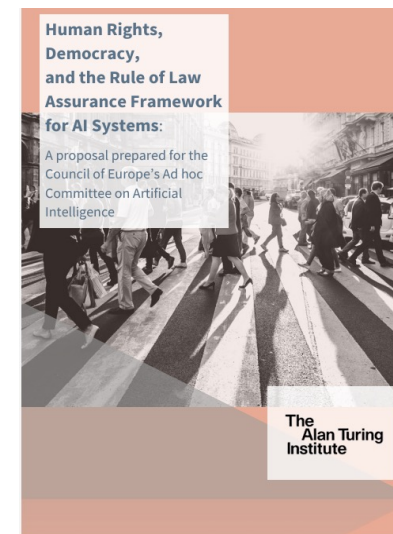
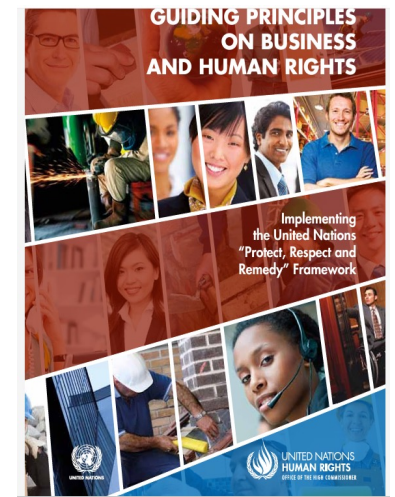
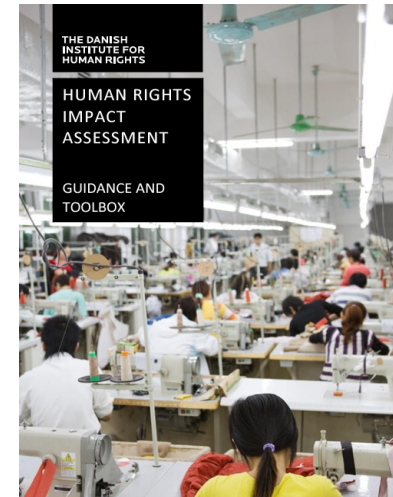
- Like a DPIA under the GDPR, risk assessment and management under the AI act **does not provide a concrete methodology, standard or template** that must be used, but the requirements for certain types of assessments
- There is **no one single type of AI Impact Assessment (AIIA)**, rather different methodologies and templates may be needed for e.g., fundamental rights impact assessment vs. risk management system vs. systemic risk assessment, but certain building blocks for different assessments may be common
 - Note that both fundamental rights impact assessment (art. 29a) and risk management system (art. 9) contain fundamental/human rights impact assessment
- Look at existing sources to define the approach for the assessment you need
- If a DPIA is needed under GDPR/LED, make sure to not overly duplicate certain parts of the assessment
- In the future:
 - The European Artificial Intelligence Board (AI Board) has as one its tasks to issue guidance (opinions, recommendations), including on risk assessment and for developing standards for high-risk AI requirements
 - Templates by the AI office: general mandate of the board to request AI office to create standardized templates for AI act compliance + explicit mention under art. 29a of template/questionnaire of fundamental rights IA questionnaire

EXISTING SOURCES - OVERVIEW

- Human rights impact assessment (HRIA) methods (general)
- Existing social and economic impact assessment methods (general)
- HRESIA: human rights, ethics, social IA for AI (specific)
- Ethical guidance and ethical compliance assessment methodologies for AI (specific)
- DPIA guidance and tools for AI (specific)
- General risk assessment methods, standards (general)
- Methods and standards for AI risk management (specific)

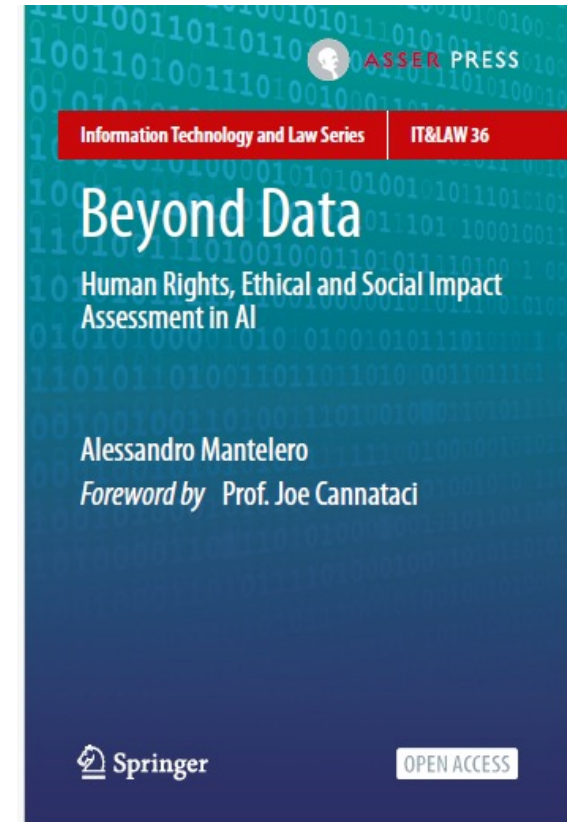
EXISTING SOURCES (1)

- Human rights impact assessment (HRIA) methods (general)
 - Methodology and toolbox by the Danish institute for human rights; based on the UN’s guiding principles on business and human rights (2011)
 - Handbook on human rights impact assessment, also refers to UN principles
 - Another example, and specific to AI, is the HUDERIA (Human Rights, Democracy and Rule of Law Impact Assessment) framework developed under the auspices of the Council of Europe
 - Note: AI Office to provide templates for Article 29a obligation in the future, but this is a good start; also for fundamental rights aspect of the risk management under Art. 9



EXISTING SOURCES (2)

- HRESIA: human rights, ethics, social IA (specific)
 - 2022
 - Open access book
 - Covers elements of:
 - Human/ fundamental rights
 - Existing ethics frameworks
 - Social impact assessment
 - Data protection



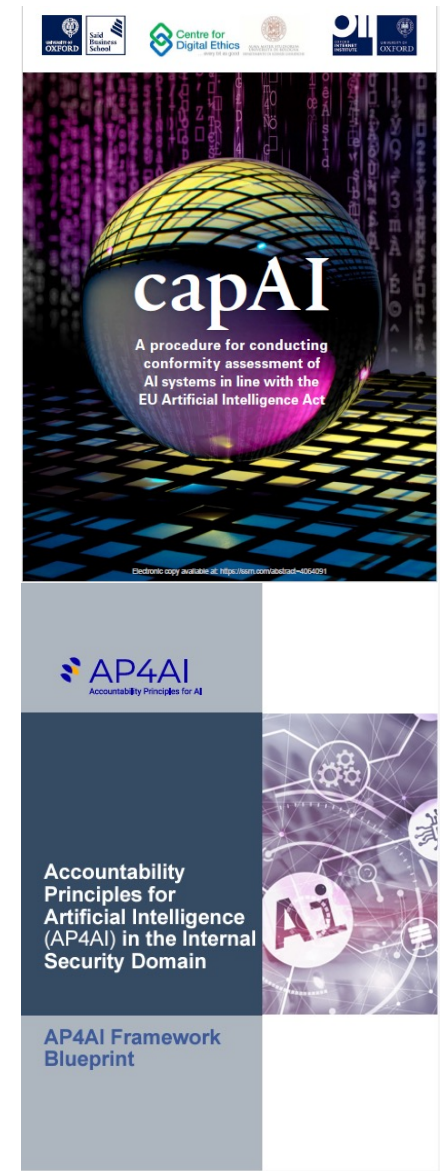
EXISTING SOURCES (3)

- Ethical guidance for AI (specific)
 - More guidance exists than can be listed here. AI could help in analyzing it
 - Most relevant is the HLEG AI ethics guidelines for trustworthy AI with 7 key principles (notice overlap with AI act)
 - Human Agency and Oversight
 - Technical Robustness and Safety
 - Privacy and Data Governance
 - Transparency
 - Diversity, Non-discrimination and Fairness
 - Environmental and Societal well-being; and
 - Accountability
 - And based on that, the Assessment List for Trustworthy Artificial Intelligence (ALTAI), a tool to dive deeper into the key principles/requirements



EXISTING SOURCES (4)

- Ethical compliance methodologies for AI (specific)
 - Similar comment, many methodologies exist, based on different ethical frameworks
 - Most relevant are methodologies focused on EU specifically, and based on HLEG AI guidance + AI act
 - Examples based on scientific research papers:
 - capAI (2022), sources include HLEG AI, OECD recommendations for AI, AIA draft
 - ECCOLA (2021), sources include HLEG AI guidance and IEEE work on ethics in AI
 - Different methodologies may apply for different sectors: e.g., Europol's AP4AI for LEAs (also CC4AI planned for AI act compliance)
 - These are relatively comprehensive methods for risk assessment, not just "light ethics"





Game Sheet – How to Play the Cards

Info: ECCOLA is easy to apply in practice. It is a sprint-oriented evolving process that empowers ethical thinking in the product development process. As a result, ethical development is embedded and Risk-Product-Shared (RPS) are achieved. The RPS help you establish the Transparency of the final result. ECCOLA is an evolving set of cards and you choose the cards that are most relevant for your work.

How to use ECCOLA is intended to be used during the system design and development process. It is used during 3 Phases – Choose the relevant cards for the current sprint. Choose cards and cards used for validation in RPS. Evaluate – Assess the selected cards on hand during single tasks. Write down if any actions are taken based on the cards. Evaluate – Review to ensure that all relevant actions are taken. Do this for each task, and if necessary, return back again.

Practical Tip: Repeat the process in every decision. Remember to do a retrospective afterwards. That should not end at what is set. Choose the cards that are the most relevant for your work in the end result.

#0 Stakeholder Analysis

Method: In order to understand the situation, it is important that stakeholders who the system will affect, and how they determine part of the situation, are taken into account in the analysis.

What to Do: Identify stakeholders.

- Who are the system's users, developers and customers?
- Are there any other stakeholders involved?
- Are there different stakeholders influencing the development of the system?
- Remember that a user is not an organization and avoid using organizational names. In addition, most people are subject to data collection.

Practical Example: Autonomous cars don't just affect their passengers, they also affect nearby cars, pedestrians, and other vehicles. It is important to consider the impact of all of these cars, what are the external impacts of the system? E.g., regulations arising from such external stakeholders.

#1 Types of Transparency

Method: What is the transparency? It is important that stakeholders who the system will affect, and who are affected by the system, are taken into account in the analysis.

What to Do: Consider the following:

- Are you trying to understand something? Internal transparency.
- Are you trying to understand something? External transparency.
- Are you trying to understand something? Internal transparency.
- Are you trying to understand something? External transparency.
- Are you trying to understand something? Internal transparency.
- Are you trying to understand something? External transparency.

Practical Example: Autonomous cars don't just affect their passengers, they also affect nearby cars, pedestrians, and other vehicles. It is important to consider the impact of all of these cars, what are the external impacts of the system? E.g., regulations arising from such external stakeholders.

#2 Explainability

Method: If we cannot understand the reasons behind the actions of the AI, it is difficult to trust it.

What to Do: Ask yourself:

- Is explainability a goal for your system? How do you plan to ensure it?
- How will you explain the actions of the system to the user? Do you have a plan for this? How will you explain the actions of the system to the user? Do you have a plan for this?
- How will you explain the actions of the system to the user? Do you have a plan for this? How will you explain the actions of the system to the user? Do you have a plan for this?
- How will you explain the actions of the system to the user? Do you have a plan for this? How will you explain the actions of the system to the user? Do you have a plan for this?

Practical Example: When interacting with a robot, users should be able to understand the reasons behind its actions and to explain its actions to others.

#3 Communication

Method: In practice, communication is a big part of the transparency with stakeholders. Being a member of a community or organization.

What to Do: Ask yourself:

- When the system is used, why is it important to communicate with stakeholders?
- When the system is used, why is it important to communicate with stakeholders?
- When the system is used, why is it important to communicate with stakeholders?
- When the system is used, why is it important to communicate with stakeholders?

Practical Example: Clearly stating what data you collect and how you use it is important for users to understand the system and to trust it.

#4 Documenting Trade-offs

Method: One important part of transparency is documenting trade-offs. When you make a decision, you choose one option over other alternatives. Documenting what you choose and why the alternative was not chosen is important.

What to Do: Ask yourself:

- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?

Practical Example: E.g., choosing machine learning algorithms over a rule-based system involves trade-offs in terms of accuracy, interpretability, and explainability.

#5 Traceability

Method: Traceability supports transparency. It helps to understand why the system works the way it does.

What to Do: Ask yourself:

- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?

Practical Example: When the system starts making decisions, it is important to be able to trace back the data and the logic that led to those decisions.

#6 System Reliability

Method: Transparency includes documenting development processes in the first place, to make it easier to understand how the system works and who is taking control.

What to Do: Ask yourself:

- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?

Practical Example: Documenting the development process helps to understand why the system works the way it does.

#7 Privacy and Data

Method: Privacy is a key concern in the design of any system. It is important to understand how the system handles user data.

What to Do: Ask yourself:

- How do you ensure that user data is protected?
- How do you ensure that user data is protected?
- How do you ensure that user data is protected?
- How do you ensure that user data is protected?

Practical Example: When collecting user data, it is important to be transparent about what data is collected and how it will be used.

#8 Data Quality

Method: In order to use data effectively, the data must be accurate, complete, and up-to-date. It is important to understand how the system handles user data.

What to Do: Ask yourself:

- How do you ensure that user data is accurate?
- How do you ensure that user data is accurate?
- How do you ensure that user data is accurate?
- How do you ensure that user data is accurate?

Practical Example: When collecting user data, it is important to be transparent about what data is collected and how it will be used.

#9 Access to Data

Method: Access to data is important for transparency. It helps to understand why the system works the way it does.

What to Do: Ask yourself:

- How do you ensure that user data is accessible?
- How do you ensure that user data is accessible?
- How do you ensure that user data is accessible?
- How do you ensure that user data is accessible?

Practical Example: When collecting user data, it is important to be transparent about what data is collected and how it will be used.

#10 Human Agency

Method: Transparency includes documenting development processes in the first place, to make it easier to understand how the system works and who is taking control.

What to Do: Ask yourself:

- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?

Practical Example: Documenting the development process helps to understand why the system works the way it does.

#11 Human Oversight

Method: Transparency includes documenting development processes in the first place, to make it easier to understand how the system works and who is taking control.

What to Do: Ask yourself:

- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?

Practical Example: Documenting the development process helps to understand why the system works the way it does.

#12 System Security

Method: Transparency includes documenting development processes in the first place, to make it easier to understand how the system works and who is taking control.

What to Do: Ask yourself:

- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?

Practical Example: Documenting the development process helps to understand why the system works the way it does.

#13 System Safety

Method: Transparency includes documenting development processes in the first place, to make it easier to understand how the system works and who is taking control.

What to Do: Ask yourself:

- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?

Practical Example: Documenting the development process helps to understand why the system works the way it does.

#14 Accessibility

Method: Transparency includes documenting development processes in the first place, to make it easier to understand how the system works and who is taking control.

What to Do: Ask yourself:

- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?

Practical Example: Documenting the development process helps to understand why the system works the way it does.

#15 Stakeholder Participation

Method: Transparency includes documenting development processes in the first place, to make it easier to understand how the system works and who is taking control.

What to Do: Ask yourself:

- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?

Practical Example: Documenting the development process helps to understand why the system works the way it does.

#16 Environmental Impact

Method: Transparency includes documenting development processes in the first place, to make it easier to understand how the system works and who is taking control.

What to Do: Ask yourself:

- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?

Practical Example: Documenting the development process helps to understand why the system works the way it does.

#17 Societal Effects

Method: Transparency includes documenting development processes in the first place, to make it easier to understand how the system works and who is taking control.

What to Do: Ask yourself:

- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?

Practical Example: Documenting the development process helps to understand why the system works the way it does.

#18 Auditability

Method: Transparency includes documenting development processes in the first place, to make it easier to understand how the system works and who is taking control.

What to Do: Ask yourself:

- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?

Practical Example: Documenting the development process helps to understand why the system works the way it does.

#19 Ability to Redress

Method: Transparency includes documenting development processes in the first place, to make it easier to understand how the system works and who is taking control.

What to Do: Ask yourself:

- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?

Practical Example: Documenting the development process helps to understand why the system works the way it does.

#20 Minimizing Negative Impacts

Method: Transparency includes documenting development processes in the first place, to make it easier to understand how the system works and who is taking control.

What to Do: Ask yourself:

- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?
- How have you documented the development of the system, both in terms of code and documentation?

Practical Example: Documenting the development process helps to understand why the system works the way it does.

Card Themes

Analyze
Transparency
Safety & Security
Fairness

Data
Agency & Oversight
Wellbeing
Accountability

Contents lists available at ScienceDirect

The Journal of Systems & Software

Journal homepage: www.elsevier.com/locate/jss

ECCOLA – A method for implementing ethically aligned AI systems^{*}

Ville Vakkuri^{*}, Kai-Kristian Kemell, Marianna Jantunen, Erika Halme, Pekka Abrahamsson

University of Jyväskylä, PO Box 35, FI 40014, Jyväskylä, Finland

EXISTING SOURCES (5)

- DPIA guidance and tools for AI (specific)
 - ICO AI and data protection risk toolkit (excel sheet)
 - ICO is still a good source
 - Lots of controls for AI-specific DPIA
 - Different phases of the AI lifecycle
 - CNIL data protection and AI toolkit
 - Fact sheet approach with different steps
 - Controls in different phases of the lifecycle

The screenshot displays a grid of seven AI lifecycle phases, each with a title, a brief description, and a 'Find out more' button. The phases are arranged in two columns: the left column contains four items, and the right column contains three items.

Phase	Description
Things to know before reading the guide	Introduction
Asking the right questions before using an artificial intelligence system	Fact sheet 1: Proportional integration of AI, specifying a clear objective
Collecting and qualifying training data	Fact sheet 2: Compliance with the GDPR when collecting and compiling a quality database.
Developing and training an algorithm	Fact sheet 3: Implementing best practices during this crucial phase.
Using an AI system in production	Fact sheet 4: Guaranteeing the quality and transparency of the system when in use.
Securing the processing	Fact sheet 5: Analysing risks and preventing flaws and attacks.
Ensuring individuals can fully exercise their rights	Fact sheet 6: Promoting transparency and rights for end-users.
Achieving compliance	Fact sheet 7: Assigning responsibilities and documenting the processing.

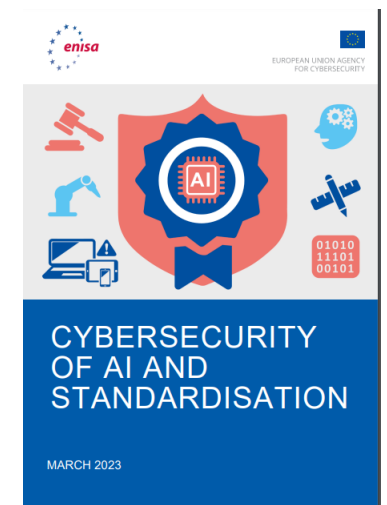
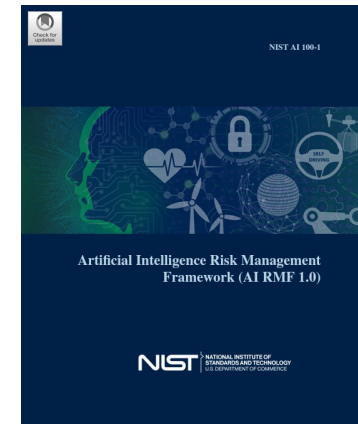
EXISTING SOURCES (6)

- Risk assessment methods and standards (general):
 - ENISA (cybersecurity) risk management standards (2022)
 - Contains overview of relevant standards for (cybersecurity) risk management
 - Not only cybersecurity and information security management (e.g., ISO/IEC 27000 family) but also general risk management (e.g., ISO/IEC 31000 family)
 - ENISA interoperable EU risk management toolbox (2023)
 - Rather comprehensive risk management toolbox to deal with various threats
 - Not specific to AI but relevant
 - ENISA interoperable risk management framework (2022)
 - Methodology for assessment of interoperability among risk management frameworks and methodologies



EXISTING SOURCES (7)

- Guidance and frameworks for AI risk management (specific):
 - ENISA - multilayer framework for good cybersecurity practices for AI
 - Description of different layers of good practices, cybersecurity focused
 - ENISA – cybersecurity of AI and standardization
 - Overview of existing standards for cybersecurity in AI
 - NIST – AI risk management framework
 - Risk management framework (US)

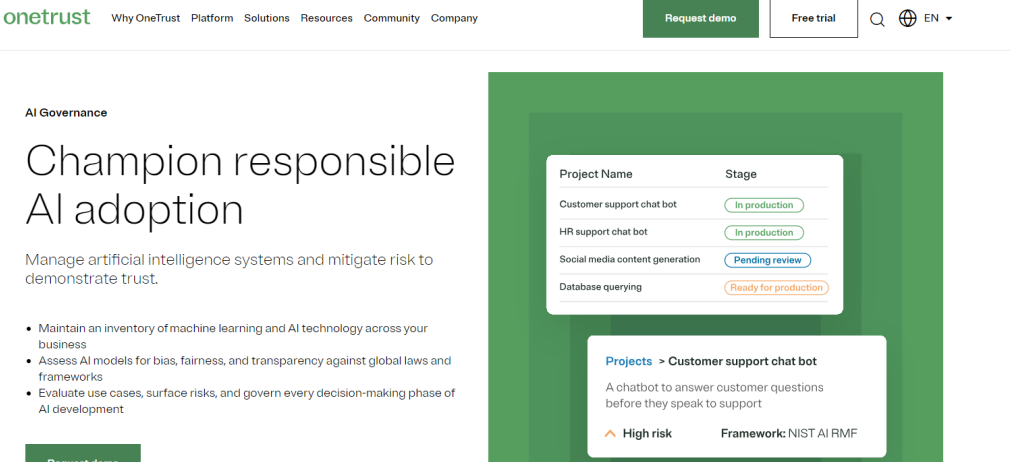


EXISTING SOURCES (8)

- ISO standards for AI risk management (specific):
 - ISO/IEC 42001:2023 - Artificial intelligence — Management system
 - Standard meant to manage AI-related risks and opportunities across an organization, putting in place policies and procedures
 - Includes risk assessment but from a different angle
 - ISO/IEC 23894:2023 - Information technology — Artificial intelligence — Guidance on risk management
 - Guidance for organizations that develop, produce, deploy or use products, systems and services that utilize artificial intelligence (AI) can manage risk specifically related to AI systems
 - Complements general standard for risk management (ISO 31000:2018)

FROM THE MARKET

- Onetrust AI governance solution



- IAPP training and certification for AI Governance Professional (AIGP)

Artificial Intelligence Governance Professional (AIGP)



With the expansion of AI technology, there is a need for professionals in all industries to understand and execute responsible AI governance. The AIGP credential demonstrates that an individual can ensure safety and trust in the development and deployment of ethical AI and ongoing management of AI systems.

Why pursue a AIGP designation?

- Establish foundational knowledge of AI systems and their use cases, the impacts of AI, and comprehension of responsible AI principles.
- Demonstrate an understanding of how current and emerging laws apply to AI systems, and how major frameworks are capable of being responsibly governed.
- Show comprehension of the AI life cycle, the context in which AI risks are managed, and the implementation of responsible AI governance.

SO, WHAT NOW? – NEXT STEPS

- Lots of existing guidance and sources, of varying relevance
- Lots of overlap, similar ideas of monitoring risk throughout the AI lifecycle, typically with continuous and iterative processes
- Time/knowledge intensive to review the whole corpus and to distill the optimal solution
- Different approaches will form/tailored methodologies for organizations/projects/sectors/settings
- Market will likely continue to provide more out-of-the box solutions
- Guidance and templates by AI Board and AI Office would be welcome to facilitate compliance

THANK YOU!

Pieter Gryffroy

pieter.gryffroy@timelex.eu

www.timelex.eu



Follow us on LinkedIn / www.linkedin.com/company/timelex

Questions & Answers

Hans Graux



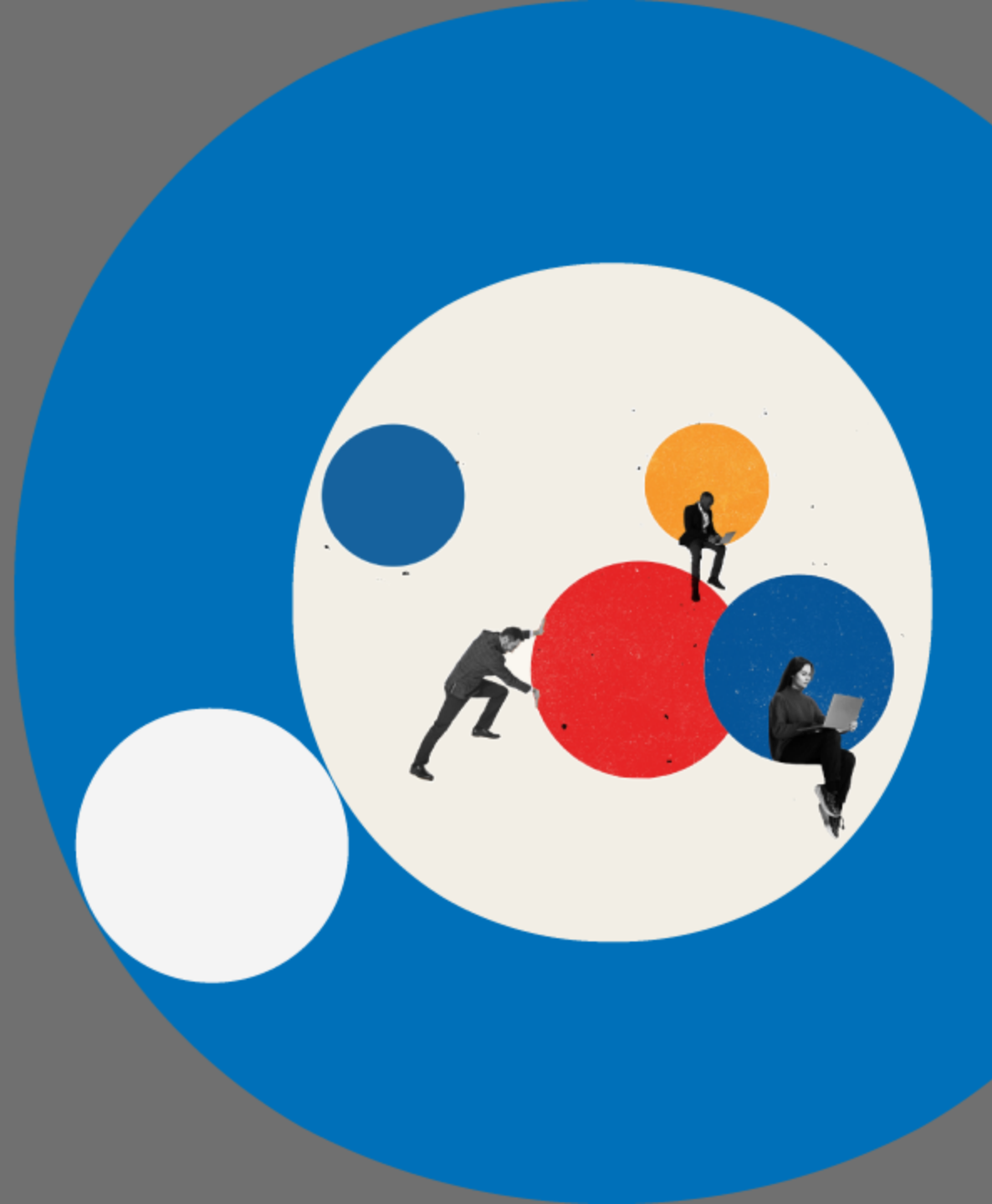
Eleni Kosta



Pieter Gryffroy



Please provide your
feedback!



Stay up-to-date on our
2024 activities!

The logo for Data Europa Academy is located in the bottom left corner. It consists of the words "data.", "europa", and "academy" stacked vertically in a white, lowercase, sans-serif font. The word "data." has a small orange dot above the 'a'. The word "europa" has a small orange dot above the 'o'. The word "academy" has a small orange dot above the 'a'. The logo is set against a dark blue circular background.

data.
europa
academy

Join our next webinars!

WEBINAR

Open data maturity
2023: best practices
across Europe



data.
europa
academy

16 February 2024
10.00 — 11.30 CET

WEBINAR

New business models
for data-driven
public services



data.
europa
academy

1 March 2024
10.00 — 11.00 CET



Thank you!

Sign up for the newsletter:
data.europa.eu/newsletter

Follow us on social media:



EU_opendata



Publications Office of the European Union



data.europa.eu

data.
europa
academy

