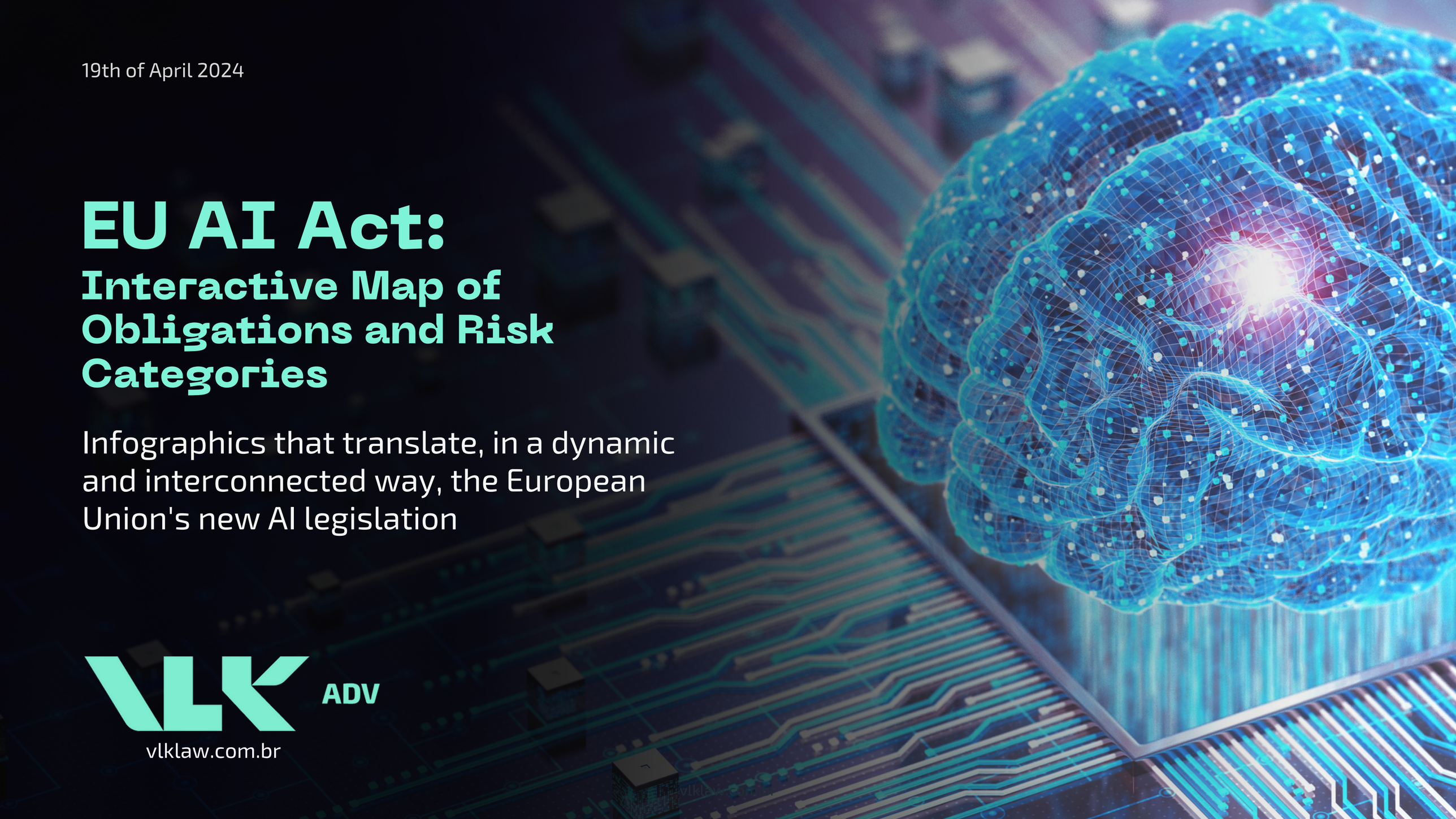
19th of April 2024

EU AI Act:
Interactive Map of Obligations and Risk Categories

Infographics that translate, in a dynamic and interconnected way, the European Union's new AI legislation



VLK ADV

vlklaw.com.br

Summary

Instructions: This is an interactive document. **Click** on the items on the side to **access the page you would like to see**.

Click on the texts in the infographics to understand the definitions, obligations and classifications of each risk category.

Disclaimer: Please note that the English version of these infographics utilizes British English to maintain consistency with the original text of the EU AI Act.

Direito, Inovação & Tecnologia

AI Act Map of Obligations

The EU AI Act prescribes a series of obligations, which vary according to the type of AI, its level of risk and the agent operating it. Learn more:

Direito,
Inovação
& Tecnologia

EU AI Act Map of Obligations

Public authority, agency or other EU body

Provider *(Art. 3 (1))*

Developing or having developed, and...

- Placing on the EU market
- Putting into service in the EU under its own name/trademark, for payment or free of charge
- Produce outputs that are used in the EU

→ General-Purpose AI Model
- Regardless of risk
  - Obligations of Providers of GPAI Models (Arts. 53-54)
  - Voluntary Codes of Practice (Art. 56)
- Systemic Risk
  - Obligations of Providers of GPAI Models with Systemic Risk (Art. 55)

→ AI System*
- Regardless of risk
  - Voluntary Codes of Practice (Art. 95)
  - AI Literacy (Art. 4)
- Limited Risk
  - Transparency Obligations of Providers of Limited Risk AI Systems (Art. 50)
- High Risk
  - Obligations of Providers of High Risk AI Systems (Art. 16)

*Has the system undergone downstream modifications or is it a safety component? Click here to understand.

Natural or Legal Person located or established within the EU or in a third country

Deployer *(Art. 3(4))*

Use, under its authority, wheter within the EU or a third country, provided that the outputs produced are used within the Union

→ AI System
- Regardless of risk
  - Voluntary Codes of Practice (Art. 95)
  - AI Literacy (Art. 4)
- Limited Risk
  - Transparency Obligations of Deployers of Limited Risk AI Systems (Art. 50)
- High Risk
  - Obligations of Deployers of High Risk AI Systems (Art. 26)

Natural or Legal Person located or established in the EU

Authorised Representative *(Art. 3(5))*

Receiving and accepting a written mandate from a provider of

→ General-Purpose AI Model
- Regardless of risk
  - Obligations of Authorised Representatives of Providers of GPAI Models (Art. 54)

→ AI System
- High Risk
  - Obligations for Authorised Representatives of Providers of High Risk AI Systems (Art. 22)

Importer *(Art. 3(6))*

Placing on the EU market

→ AI System
- High Risk
  - Obligations for Importers of High Risk AI Systems (Art. 23)

Distributor *(Art. 3(7))*

Making available on the EU market

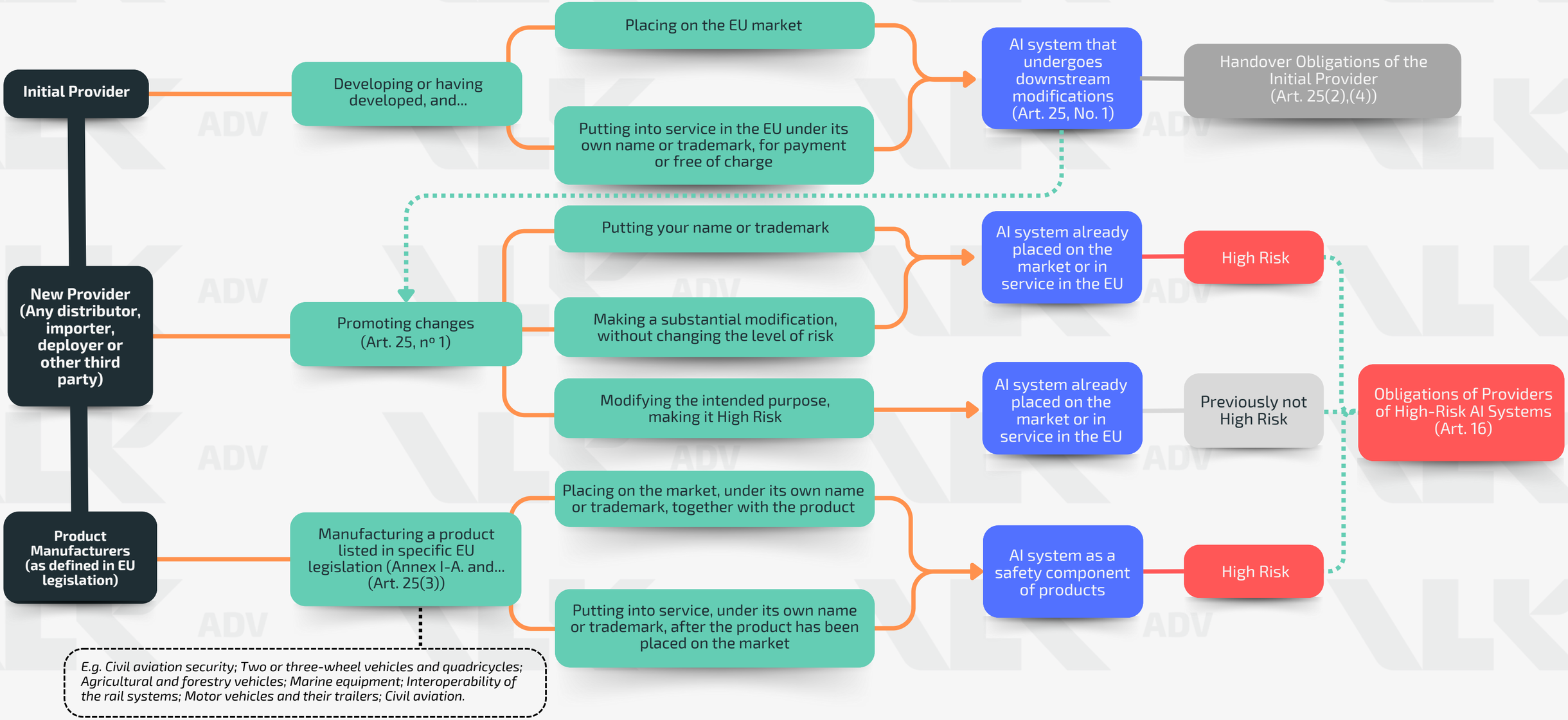
→ AI System
- High Risk
  - Obligations for Distributors of High Risk AI Systems (Art. 24)

Responsibilities Along the AI Value Chain

Learn which specific situations can make third parties subject to the same obligations as AI providers.

Direito,
Inovação
& Tecnologia

Responsibilities along the AI Value Chain



Lists of Obligations in the AI Act

Have you already identified which type of obligation you fall under? Find out which rules you are required to follow.

Direito,
Inovação
& Tecnologia

General-Purpose AI (GPAI) Models

Voluntary Codes of Practice (Art. 56)

- In accordance with the incentives and details given by the AI Service and the Committee, drawing up codes of practice for the correct application of the regulation, taking into account international approaches (Art. 56(1)) and covering specific obligations and essential elements, such as (Art. 56(2)):
  - Updating information in the light of technological and market developments;
  - Providing detailed summaries of the content used in the training;
  - Identifying and managing systemic risks
- Participating in the drafting of the codes, with the support of national authorities, civil society organisations, industry and academics (Art. 56(3)).

Authorised Representatives of Providers of GPAI Models (Art. 54)

- Performing the tasks assigned by the mandate, such as (Art. 54(3)):
  - Verifying the compliance of the GPAI model with the obligations of the regulation and keeping the technical documentation for 10 years after placing on the market;
  - Providing the necessary information and documentation to the AI Office to demonstrate compliance with the obligations prescribed;
  - Cooperating with the AI Office and competent authorities on measures related to the GPAI model;
- Upon request, providing the AI Office with a copy of the mandate in one of the official languages of the Union institutions (Art. 54(4)).
- Terminating the mandate if the provider acts contrary to the obligations of the regulation and inform the AI Office immediately (Art. 54(5)).
- The obligation does not apply to providers of GPAI models released under a free and open source license, unless they present systemic risks (Art. 54(6)).

Providers of GPAI Models (Arts. 53-54)

- Preparing and keeping updated the technical documentation of the GPAI model (Art. 53(1)(a)); and providing information for integrating the model into AI systems (Art. 52(1)(b)).
  - Exceptions: open source AI models, except those with systemic risks (Art. 53(2)).
- Putting in place copyright and related rights compliance policy (Art. 53(1((c)).
- Drawing up and making available a summary of the content used for training the model (Art. 53(1)(d)).
- Cooperating with authorities (Art. 53(3))
- If located in a third country, appointing an authorised representative in the EU and enable them to perform the tasks specified in the mandate given (Art. 54(1)(2)(3)).
  - Exceptions: open source AI models, except those with systemic risks (Art. 54(5)).

Providers of GPAI Models with Systemic Risk (Art. 55)

- Performing model evaluation in accordance with standardised protocols (Art. 55(1)(a)).
- Assessing and mitigating systemic risks in the EU (Art. 55(1)(b)).
- Monitoring, documenting and communicating relevant information on serious incidents and corrective measures (Art. 55(1)(c)).
- Ensure an adequate level of cybersecurity for the model and its physical structure (Art. 55(1)(d)).
- Treating information obtained in accordance with the confidentiality obligations of Art. 78 (Art. 55, no. 3).

Minimal Risk and Limited Risk AI Systems

AI Literacy (Art. 4)

- Taking measures to ensure, to the best extent, that persons involved in the operation and use of AI systems on their behalf have a sufficient level of literacy in the field of AI, taking into account their technical knowledge, experience, education and training and the context in which the AI systems are used, as well as the persons or groups of persons targeted by such use.

Voluntary Codes of Practice (Art. 95)

For Minimal or Limited Risk AI Systems:

- Drawing up codes of conduct, including related governance mechanisms, to voluntarily apply some or all of the requirements for High Risk AI Systems, taking into account available technical solutions and industry best practices (Art. 95(1)).

For any AI Systems:

- Drawing up voluntary codes of conduct, including elements such as (Art. 95(2)):
  - elements contained in the EU's "Ethical Guidelines for Trustworthy AI" document;
  - assessing and minimizing the impact of AI systems on environmental sustainability;
  - promoting AI literacy;
  - facilitating an inclusive and diverse design of AI systems, including through the creation of inclusive and diverse teams; and
  - assessing and preventing the negative repercussions of AI systems on vulnerable people.

Providers of Limited Risk AI Systems (Art. 50)

Ensuring that, no later than the first interaction, clear and distinguishable information is provided in the following terms (Art. 50(5)):

- For AI systems that interact directly with individuals: informing those individuals that they are interacting with an AI, unless contextually obvious or unless authorized by law for the purposes of detecting, preventing, investigating and prosecuting criminal offences (Art. 50(1)).
- For AI systems that generate synthetic content: marking the results as artificially generated, in a machine-readable and detectable format. These markings must be effective, interoperable, robust and reliable as far as is possible (Art. 50(2)).

Deployers of Limited Risk AI Systems (Art. 50)

Ensuring that, no later than the first interaction, clear and distinguishable information is provided in the following terms (Art. 50(5)):

- For emotion recognition or biometric categorisation systems: informing and processing personal data in accordance with EU law (Art. 50(3)).
- For systems that generate or manipulate deepfakes or texts intended to provide information of public interest: revealing their artificial origin (Art. 50(4)).

High Risk AI Systems: Deployers, Authorised Representatives, Importers and Distributors

Deployers of High Risk AI Systems (Art. 26)

- Ensuring the use of AI systems in accordance with the provider's instructions (Art. 26(1)).
- Assigning human oversight to individuals with technical competence, training, authority and necessary support (Art. 26(2))
- Exercising control over input data, ensuring relevance and representativeness, in view of the intended purpose (Art. 26(4)).
- Monitoring the operation of the system and, if they consider that it may pose a risk, suspending its use and informing the provider and the surveillance authority (Art. 26(5)).
- Reporting serious incidents to other operators and the authority (Art. 26(5)).
- Keeping logs for an appropriate period, the minimum being 6 months (Art. 26(6),(7)).
- For public authorities or EU entities, complying with registration obligations under Art. 49 and reporting on the use of AI systems (Art. 26(8)).
- Using information received for data protection impact assessment (Art. 26, para. 9).
- Requiring authorisation for the use of biometric identification systems and recording their use (Art. 26(10)).
- Informing: individuals about the use of AI systems for decision-making; and workers about the use of AI systems in the workplace; (Art. 26(5),(11))
- Cooperating with competent authorities (Art. 26(12)).

Authorised Representatives of Providers of High Risk AI Systems (Art. 22)

- Providing a copy of the mandate to the Surveillance Authorities upon request (Art. 22(1))
- Assessing the conformity of the AI system documentation (EU Declaration of Conformity, technical documentation) and the conformity assessment (Art. 22(3))
- Keeping at the disposal of the competent authorities the contact details of the provider and the AI system documentation and, where applicable, the certificate issued by the notified body for ten years (Art. 22(3)).
- Cooperating with the competent authorities, including by providing them with the information and documentation requested by means of reasoned requests (Art. 22(3)).
- If registration in the EU database is required, ensure compliance of the information required by Annex VIII(A),(3) (Art. 22(3))

Importers of High-Risk AI Systems (Art. 23)

- Assessing the compliance of the AI system with the Regulation (carrying out conformity assessment, technical documentation, CE marking, EU Declaration of Conformity), the appointment of an Authorised Representative by the provider and not making non-compliant or falsified products available on the market (Art. 23(1),(2)).
- Indicating contact information on products and keeping records of the AI system for at least ten years after it has been placed on the market (Art. 23(3),(5)).
- Ensuring that storage or transport conditions do not jeopardise the compliance of the AI system (Art. 23(4)).
- Keeping for 10 years a copy of the certificate issued by the notified body, where applicable, the instructions for use and the EU Declaration of Conformity (Art. 23(5)).
- Providing information and documentation requested by the relevant competent authorities and cooperating in measures to minimise risks (Art. 23(6),(7)).

Distributors of High-Risk AI Systems (Art. 24)

- Assessing the compliance of the AI system with the regulation (presence of EU certification of conformity, Declaration of Conformity and instructions for use) and fulfilment of certain obligations by the provider and importer (Art. 24(1)).
- Not making irregular or falsified products available on the market (Art. 24(2)).
- Ensuring that storage and transport conditions do not jeopardise the system's conformity (Art. 24(3)).
- Adopting corrective actions or withdrawing from circulation AI systems that it has placed on the market and finds to be non-compliant (Art. 24(4)).
- Providing information and documentation requested by the competent authorities and cooperating in measures to minimise risks (Art. 24(5),(6)).

Providers of High-Risk AI Systems and Initial Suppliers in the AI Value Chain

Handover Obligations of Initial Providers (Art. 25(2), (4))

- Coooperating closely with new providers, providing information, technical access and assistance necessary to fulfil regulatory obligations, except if it has clearly specified any restrictions on changing the AI system to a high-risk AI system (Art. 25(2)).
- Specifying in writing the terms of the agreement between the provider of the high-risk AI system and third parties supplying tools, services, components or processes used or integrated into the system (Art. 25(4)).
- Developing and recommending models for voluntary contractual clauses between providers of high-risk AI systems and third parties, taking into account the contractual requirements applicable in specific sectors (Art. 25(4)).
- Respecting and protecting intellectual property rights, confidential business information and trade secrets, as required by EU and national law (Art. 25(5)).

Obligations of Providers of High-Risk AI Systems (Art. 16)

- Ensuring compliance with requirements for High Risk Systems (Arts. 8 - 21) and EU Directives, including but not limited to:
  - Clear identification of the system and its information;
  - Implementation of a quality management system (Art. 17), which must include, among other things:
    - Strategy for compliance with the AI Act
    - Techniques, procedures and actions for controlling the design, development and quality of the AI system;
    - Procedures for testing and validating the AI system.
    - Risk management (Art. 9)
    - Data governance (Art. 10)
    - Post-marketing monitoring system (Art. 72)
    - Serious incident reporting procedure (Art. 73)
    - Management of resources and communications with competent authorities.
    - Maintenance of documentation (Art. 18);
    - Automatic recording of systems (Art. 19);
    - Corrective actions (Art. 20).
- Carrying out the required assessments, declarations and registration (Arts. 40 - 49);
- Reporting Serious Incidents (Arts. 73 and 17);
- **If it considers that the AI system does not pose a significant risk,** the Provider must (Art. 6, no. 3):
  - Document its assessment before placing the system on the market or in service;
  - Register itself and the system in the EU database (Art. 49(2));
  - Provide the evaluation documentation to the competent national authorities upon request.
    - If a market surveillance authority identifies that the system has been incorrectly classified (Art. 80, no. 7), the system will be subject to the obligations for High Risk and the provider may be fined (Art. 99).

Risk Categorisation

Learn about the EU AI Act's risk-based approach and the division between AI Systems and General Purpose AI Models.

Direito,
Inovação
& Tecnologia

Direito, Inovação & Tecnologia

Types of AI

AI Systems

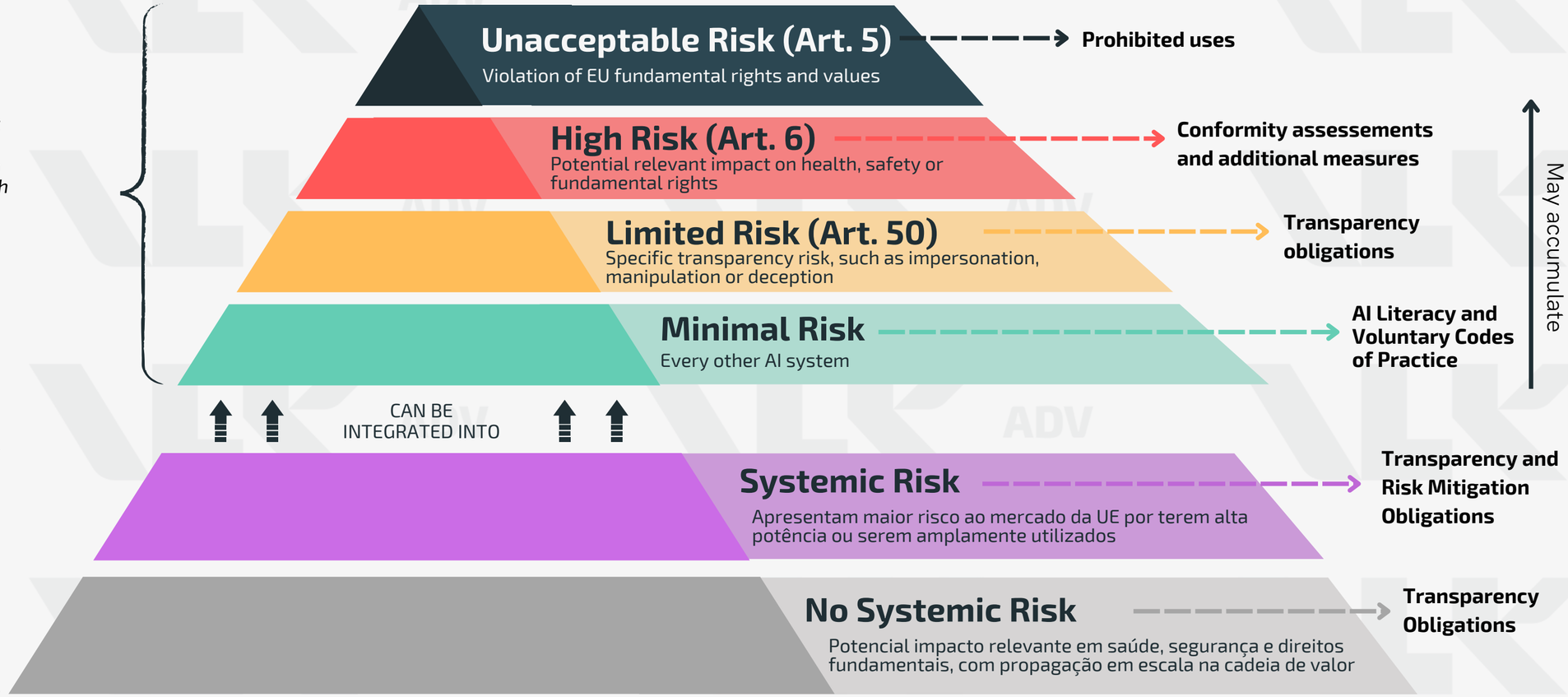
'(...) a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments' (Art. 3, No. 1)

General-Purpose AI Models (GPAI)

'(...) 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' (Art. 3, No. 63)

Level of Risk

Risk: *'(...) the combination of the probability of an occurrence of harm and the severity of that harm'* (Art. 3, No. 2)



Rules for Risk Classification

Understand how each level of risk is classified, what the exceptions are and who is entitled to change the classifications.

Level of risk	Framing	Exceptions	Who can change the framing?	Normative reference
Unnacceptable Risk (1/3)	AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive, with the objective or the effect of substantially distorting behavior by impairing the ability to make informed decisions, posing a risk of significant harm.	N/A	**European Parliament, upon a proposal from the Commission**	**Art. 5 Art. 112**
	AI system that exploits vulnerabilities due to age, disability or socioeconomic situation with the objective or the effect of distorting behavior in a way that is reasonably likely to generate significant harm to that individual or third parties.			
	Social evaluation or classification systems (e.g. profiling) that generate unfavorable treatment of natural persons (i) in a context unrelated to that in which the data was collected; **and/or** (ii) that is unjustified or disproportionate to their social behavior or its respective gravity.			

Back to the map

Level of risk	Framing	Exceptions	Who can change the framing?	Normative reference
Unnacceptable Risk (2/3)	AI systems aimed at assessing the risk of a person committing a criminal offence based solely on profiling or assessing personality traits and characteristics.	The use of predictive systems to assist in the human assessment of a person's involvement in a criminal activity, provided that this assessment is based on objective, verifiable facts directly linked to the criminal activity.	**European Parliament, upon a proposal from the Commission**	**Art. 5 Art. 112**
	AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage.	N/A		
	AI systems to infer emotions of a natural person in the areas of workplace and education institutions.	When used for medical or safety reasons.		
	AI systems that, through biometric categorisation, infer sensitive personal data about an individual in the workplace and in educational institutions.	Labelling and filtering of lawfully acquired biometric datasets, such as images, based on biometric data or the categorizing of biometric data in the area of law enforcement.		

Back to the map

UE AI Act

Level of risk	Framing	Exceptions	Who can change the framing?	Normative reference
Unnacceptable Risk (3/3)	The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement	If, cumulatively: • The use is strictly necessary for (i) the targeted search for missing persons or specific victims of certain crimes (e.g. kidnapping); (ii) the prevention of a specific, substantial and imminent threat to life or physical safety or a genuine and present or genuine and foreseeable threat of a terrorist attack; (iii) the location or identification of a person suspected of committing a criminal offence, the initiation of a criminal prosecution or the execution of a criminal penalty for any of the offences referred to in Annex II. • The Law Enforcement Authority has completed a fundamental rights impact assessment. • It has been approved by a Judicial Authority or Independent Administrative Authority with binding powers. • It has been communicated to the Data Protection Authority and the Market Surveillance Authority.	**European Parliament, upon a proposal from the Commission**	**Art. 5 Art. 112**

Back to the map

Level of risk	Framing	Exceptions	Who can change the framing?	Normative reference
High Risk	The AI system is a product or a safety component of a product which, cumulatively: (i) is regulated by one of the harmonised legislation listed in Annex I; and (ii) the legislation in question requires the system to undergo a conformity assessment.	N/A	**The Commission, via delegated acts, either by amending Annex III or by amending the hypothetical exceptions.**	**Art. 6 Art. 7 Art. 97 Annex I Annex III**
	The AI system fits into one of the hypotheses described in Annex III. These hypotheses are specific use cases in the areas of: • Remote biometrics; • Critical infrastructures; • Educational and vocational training; • Employability and worker management; • Access to and enjoyment of essential private services and essential public services and benefits; • Law enforcement; • Migration and border control; • Administration of justice and the democratic process.	Even if it falls within one of the hypotheses in Annex III, the system shall not be considered high risk if, cumulatively ***(i)*** it is not intended for profiling natural persons; and ***(ii)*** it meets at least one of these requirements: • Performs a narrow procedural task; • It only improves the result of a previously completed human activity; • It only detects the patterns of previous decisions and any deviations, and is not intended to influence or replace previously completed human decisions, barring appropriate human review; • It is intended for preparatory tasks for an assessment relating to Annex III use cases.		

Back to the map

UE AI Act

Level of risk	Framing	Exceptions	Who can change the framing?	Normative reference
Limited Risk (Specific Transparency Obligations)	The AI system is designed to interact directly with natural persons.	Contextualmente obvio **ou** legalmente autorizado para detectar, prevenir, investigar ou reprimir infrações penais, reservada as garantias dos direitos e liberdades de terceiros, salvo se os sistemas estiverem disponíveis ao público para denunciar uma infração penal.	**There is no specific provision, so it is assumed that the EU's ordinary legislative procedure will be followed.**	**Art. 50**
	The AI system, including the general-purpose AI systems, generates synthetic audio, image, video or text content.	The AI system performs a function in support of standard editing **or** does not substantially alter the input data provided by the deployer **or** its semantics, **or** when its use is authorised by law to detect, prevent, investigate and prosecute criminal offences.		
	Emotion recognition system or a biometric categorisation system.	If the AI system is legally authorised to detect, prevent or investigate criminal offences, subject to adequate guarantees of the rights and freedoms of third parties.		
	AI system that generates or manipulates image, audio or video content that constitutes a deep fake or generates or manipulates text for the purpose of disclosing information of public interest.	If the use is authorised by law to detect, prevent, investigate or prosecute criminal offences. In addition, if it has an artistic purpose, transparency obligations must be applied in such a way that they do not hamper the display or enjoyment of the work. If it is an informative text, it is not necessary if it is preceded by a process of human analysis or editorial control and there is an editorial responsible for the publication.		

Back to the map

Level of risk	Framing	Exceptions	Who can change the framing?	Normative reference
GPAI Model	AI Models that display significant generality and are 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. Without prejudice to other criteria, GPAI models will be those that cumulatively: ***(i)*** have at least one billion parameters; ***(ii)*** have been trained on a large volume of data using self-supervision at scale; and ***(iii)*** competently perform a wide range of tasks.	If the AI model is used for research, development or prototyping activities before being launched on the market.	**There is no specific provision, so it is assumed that the EU's ordinary legislative procedure will be followed.**	**Recital 98 Art. 3 (63) Art. 53**

Back to the map

Level of risk	Framing	Exceptions	Who can change the framing?	Normative reference
GPAI Model With Systemic Risk	The model has high-impact capabilities, with impact being presumed when the cumulative amount of computation used for its training measured in floating point operations per second (FLOPs), is greater than 10^25.	Even if this requirement is met, the provider, when notifying the Commission, can present, with its notification, sufficiently reasoned arguments to demonstrate that, exceptionally, it does not present systemic risks.	**The Commission may adopt delegated acts to amend the thresholds established for systemic risk models and the requirements of Annex XIII.**	**Art.3(65) Art. 51 Art. 52 Art. 97 Annex XIII**
	Having capabilities or an impact equivalent to those of high-impact models, having regard to the criteria set out in Annex XIII.	N/A		

Back to the map

Legal Definitions

Learn the key definitions to master the understanding of the EU AI Act, according to the wording of Article 3.

Direito,
Inovação
& Tecnologia

Art. 3: For the purposes of this Regulation, the following definitions apply: (...)

Operators

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;

68) '**Downstream provider**' means a provider of an AI system, including a general-purpose AI system, which integrates an AI model, regardless of whether the AI model is provided by themselves and vertically integrated or provided by another entity based on contractual relations.

4) '**Deployer**' mens 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;

5) '**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;

6) '**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;

7) '**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;

Actions

9) '**Placing on the market**' means the first making available of an AI system or a general purpose AI model on the Union market;

11) "**Colocação em serviço**", o fornecimento, diretamente ao implantador ou para utilização própria, de um sistema de IA para a primeira utilização na União com a finalidade prevista;

11) '**Putting into service**' means the supply of an AI system for first use directly to the deployer or for own use in the Union for its intended purpose;

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;

23) '**Substantial modification**' means a change to an AI system after its placing on the market or putting into service which is not foreseen or planned in the initial conformity assessment carried out by the provider and as a result of which the compliance of the AI system with the requirements set out in Chapter III, Section 2 is affected or results in a modification to the intended purpose for which the AI system has been assessed;

Types of AI

1) '**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;

66) '**General-purpose AI system**' means an AI system which is based on a general-purpose AI model and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems;

63) '**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;

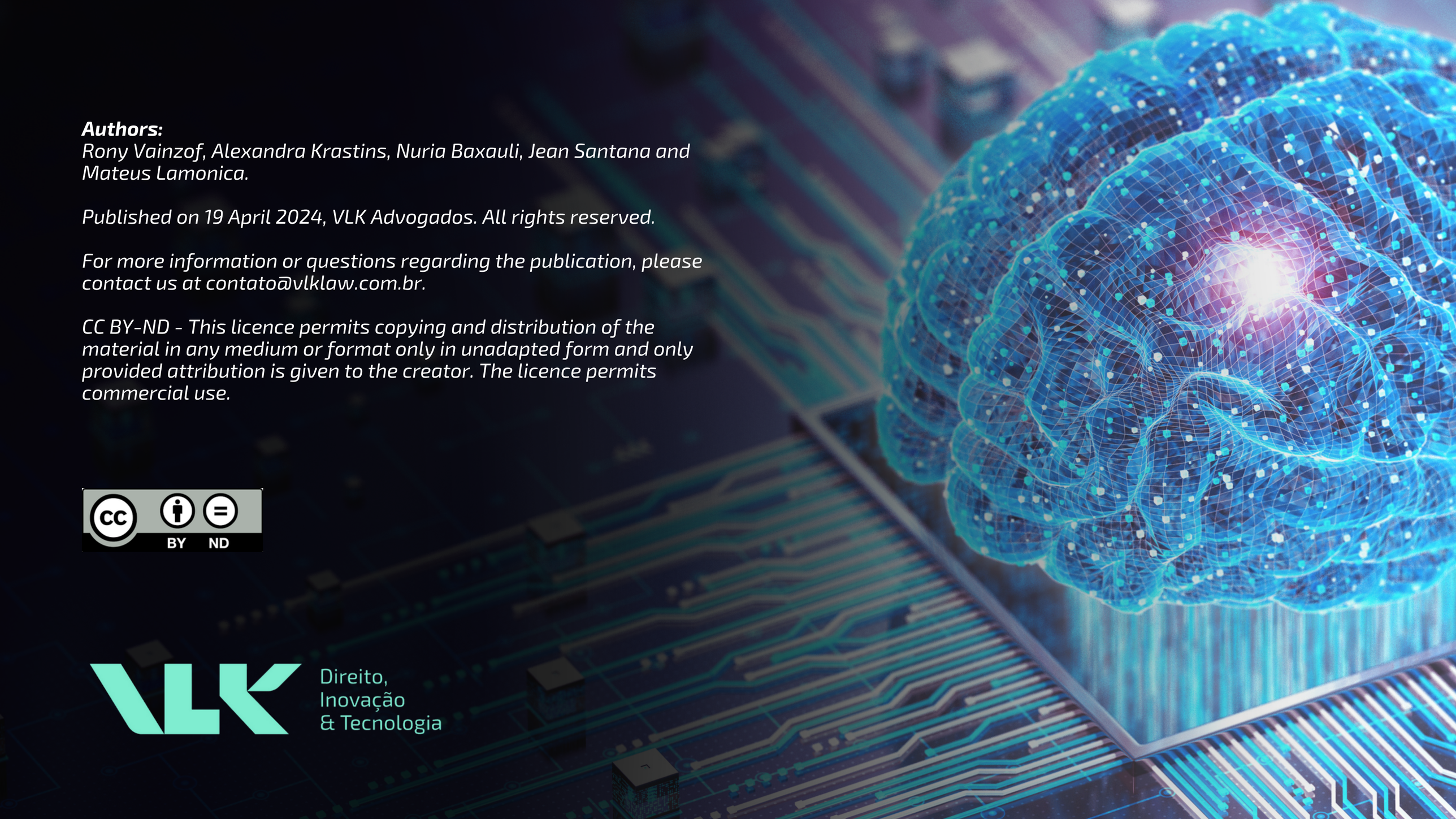
65) '**Systemic risk**' means a risk that is specific to the high-impact capabilities of general purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain;

14) "**Componente de segurança**", um componente de um produto ou sistema de IA que cumpre uma função de segurança nesse produto ou sistema de IA, ou cuja falha ou anomalia põe em risco a saúde e a segurança de pessoas ou bens;

Authors:
Rony Vainzof, Alexandra Krastins, Nuria Baxauli, Jean Santana and Mateus Lamonica.

Published on 19 April 2024, VLK Advogados.

For more information or questions regarding the publication, please contact us at contato@vlklaw.com.br.



Direito,
Inovação
& Tecnologia