RocaJunyent Informs

Data Protection, Cybersecurity and Technology Department

19 July 2024

On 12 July 2024, the final text of the new Artificial Intelligence Regulation ("**ARI**" or "**Regulation**")[1] was published in the Official Journal of the European Union. We analyse its key points in this alert.

1. What does RIA consider Artificial Intelligence Systems?

The RIA is designed to oversee and regulate the implementation of Artificial Intelligence ("**AI**"), with a particular focus on mitigating the risks associated with its development and use.

The Regulation defines **AI Systems** as machine-based systems that are designed to operate with different levels of autonomy and that can show adaptive capabilities after deployment, and that, for explicit or implicit goals, infer from the input information they receive how to generate output results, such as predictions, content, recommendations or decisions, which can influence physical or virtual environments.

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules in the field of artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation)

The RIA also places particular emphasis on **General Purpose AI Systems**, defining them as systems based on a **General Purpose AI Model**, which is trained on a large volume of data using large-scale self-monitoring, which exhibits a considerable degree of generality and is capable of competently performing a wide variety of different tasks, regardless of how the model is introduced to the market, and which can be integrated into various downstream systems or applications, except AI models that are used for research, development or prototyping activities prior to their introduction to the market; General Purpose AI Systems can serve a variety of purposes, both for direct use and for integration into other AI systems.

2. What roles does the RIA identify?

The RIA identifies the following roles in the lifecycle of IA systems and models:

a) **Provider:** A natural or legal person, public authority or body that develops an AI system or model and brings it to the market or puts it into service under its own name or brand, either free of charge or for a fee.
b) **Deployer:** A natural or legal person or public authority that uses an AI system under its own authority, except when the use is of a personal and non-professional nature.
c) **Importer:** A natural or legal person located in the European Union who places on the market an AI system bearing the name or trademark of an entity established outside the EU.
d) **Distributor: A** natural or legal person in the supply chain, other than the supplier or importer, who places an AI system on the market in the European Union.
e) **Authorised representative:** A natural or legal person in the European Union who, by written mandate from a supplier, undertakes the obligations and procedures set out in the regulation on behalf of the supplier.
f) **Product manufacturer:** Manufacturer as defined in the harmonised legislation listed in Annex I of the RIA.

The six roles are collectively referred to as "operator" and all of them can be applied in the context of AI systems. However, in the context of models, only the roles of supplier or authorised representative can be applied. That is, it is not possible to be a deployment manager, importer, distributor or manufacturer of the product with respect to an AI model.

3. What is the scope of application?

The scope of the Regulation extends beyond organisations established in the European Union ("**EU**") to those using, developing or operating Artificial Intelligence ("**AI**") systems and models in the European market. This implies that many multinationals, with a presence or commercial interactions in the EU, will also have to apply it.

4. To which IA systems does RIA not apply?

The AI Regulation shall not apply to AI systems and tools dedicated to:

a) **Military and National Security Purposes:** AI systems used exclusively for military, defence or national security purposes.
b) **International cooperation:** AI systems used by public authorities of third countries or international organisations in the framework of international cooperation agreements with the EU or its Member States, provided that the protection of fundamental rights and freedoms is ensured.
c) **Scientific research and development:** AI systems and models developed and used exclusively for scientific research and development.
d) **Pre-commercial testing and development:** Activities of research, testing or development of AI systems or models prior to their introduction to the market or putting into service (except testing under real conditions).
e) **Personal non-professional use:** AI systems used by natural persons in purely personal and non-professional activities.

f) **Free and open source licences:** Some AI systems released under free and open source licences, except those that are prohibited or high risk.

5. How are AI Systems categorised?

IA Systems are categorised according to the risk they pose to people's fundamental rights, with Unacceptable Risk, High Risk, Limited Risk and Minimal Risk Systems.

Unacceptable Risk:

The following IA Systems are categorised as Unacceptable Risk and are therefore prohibited by the RIA:

1. **Inference of sensitive characteristics:** Biometric and individual categorisation to infer sensitive characteristics such as race, religious, ideological or sexual orientation, among others, pose serious privacy and discrimination risks.
2. **Biometric recognition in public spaces:** The use of remote and real-time biometric recognition in publicly accessible spaces for the purpose of crime prevention or investigation, without meeting certain exception requirements (such as specific criminal offences and strict conditions).
3. **Facial image scraping:** The generalised scraping of facial images from the internet or CCTV to generate or extend facial recognition databases.
4. **Emotion recognition in sensitive environments**: Emotion recognition in work and educational environments, except for medical or security purposes,
5. **Social scoring:** Social **scoring** systems that evaluate individuals or groups according to their social behaviour or personal characteristics (known, inferred or predicted).
6. **Manipulation**: Systems that use subliminal, manipulative or deceptive techniques to alter people's behaviour, impairing their ability to make informed decisions and leading them to make harmful decisions they would not otherwise have made.
7. **Exploitation of vulnerabilities**: Systems that exploit vulnerabilities of individuals (age, creditworthiness, disability, etc.) or groups of individuals to influence their behaviour causing significant harm.
8. **Crime risk prediction**: Systems that assess and predict the risk of committing crimes based solely on the profiling of a natural person.

High Risk

An AI system is considered high risk if it meets any of the following conditions:

1. It is intended to be a safety component of a product regulated by EU harmonised legislation (Annex I), or it is the product itself.
2. The AI product or system must undergo a third party conformity assessment according to harmonised EU legislation (Annex I).
3. Belongs to one of the eight sectors identified in Annex III of the RIA and may present a significant risk to health, safety or fundamental rights, or substantially influence decision making
   a. Biometrics
   b. Critical Infrastructures
   c. Education and Vocational Training
   d. Employment, employee management and access to self-employment
   e. Access to and enjoyment of essential private services and essential public services and benefits
   f. Ensuring compliance with the right
   g. Migration, asylum and border control management

h. Administration of justice and democratic processes

Suppliers who consider a system belonging to the described sectors not to be high risk must document their assessment prior to commercialisation and register it.

6. How are AI Models categorised for general use?

a) Systemic Risk:

A general-purpose AI model is considered systemic risk if it meets any of the following conditions:

1. High-impact capacities assessed through appropriate technical tools and methodologies, using indicators and benchmarks.
2. Decision of the European Commission on the basis of set criteria:
   a. The number of model parameters;
   b. The quality or size of the data set, e.g. measured through cryptofiches;
   c. The amount of computation used to train the model, measured in floating point operations or indicated by a combination of other variables, such as the estimated cost of training, the estimated time required or the estimated energy consumption for training;
   d. The input and output modalities of the model, such as text-to-text conversion (large language models), text-to-image conversion, multimodality and pointer thresholds to determine the high-impact capabilities of each modality, and the specific type of inputs and outputs (e.g. biological sequences);
   e. Benchmarks and assessments of the model's capabilities, also taking into account the number of tasks without additional training, the adaptability to learn new and different tasks, its level of autonomy and scalability, and the tools it has access to;
   f. Whether its impact on the internal market is significant due to its scope, which will be assumed when it has been made available to at least 10 000 registered professional users established in the EU;
   g. The number of registered end-users.

b) Ordinary Risks

All models not rated as systemic risk.

7. What are test spaces and how will they work?

With the aim of strengthening European competitiveness in the field of AI, a controlled test space ("**Sandbox**") is set up to provide a controlled environment for developing, testing, and validating innovative AI systems under real-world conditions. The Regulation seeks to establish common rules for the creation of a Sandbox and a framework for cooperation between the supervisory authorities involved. However, the specific requirements for access to sandboxes will be determined by the local supervisory authorities. In Spain, Royal Decree 817/2023 of 8 November aims to create the first controlled environment to test the application of certain requirements set out in the Regulation.

8. What are the codes of conduct mentioned in the IA Regulation?

Codes of conduct are tools to promote ethics, transparency and accountability in the development and use of AI. The Office of IA and the Member States shall encourage and facilitate the development of codes of conduct, designed to be applied on a voluntary basis by providers of IA systems. These codes are intended to encourage the voluntary application of the requirements set out in Chapter III, Section 2 to non-high-risk AI systems. They should include, inter alia, governance arrangements, industry best practices and the adoption of technical solutions.

9. When will it apply?

The RIA will be phased in gradually:

1st) 1 August 2024: Entry into force of the RIA
2nd) 2 February 2025: Entry into force of the use bans, six months after the entry into force of the regulation.
3rd) 2 May 2025: Deadline for the finalisation of codes of practice, nine months after the entry into force of the regulation.
4th) 2 August 2025: Entry into application of the provisions targeting AI models, 12 months after the entry into force of the regulation.
5th) 2 August 2026: Entry into application of the remainder of the rule, 24 months after the entry into force of the regulation.
6th) 2 August 2027: Entry into application of Article 6.1 and Annex I of the RIA for rating High Risk systems, thirty-six months after the entry into force of the regulation.

A review of the IA Regulation should be carried out after 5 years.

10. What are the supervisory bodies?

In Spain, the competent supervisory authority for the Artificial Intelligence Regulation is the AESIA (Agencia Española de Supervisión de la Inteligencia Artificial). At the European level, a European Committee on Artificial Intelligence will be established with one representative from each Member State, tasked with guiding the implementation of the regulation, drafting guidelines and establishing rules for sandboxes. The European AI Office plays a crucial role in overseeing compliance with the regulation in the Member States, ensuring uniform and effective application across all sectors using AI systems. It works in collaboration with national authorities to coordinate monitoring and training activities, ensuring that the standards set are respected. At the international level, the Office participates in global fora and agreements to promote global AI governance and share common regulatory strategies.

11. What are the breaches and penalties?

Fines for breaches of the RIA were set as a percentage of the overall annual turnover of the offending company in the previous financial year or a pre-determined amount, whichever was higher. The maximum would be 7% of the overall turnover. The punitive measures are designed to ensure compliance with the RIA and to encourage ethical and responsible use of artificial intelligence. Some of the sanctions that could be applied include the following:

In IA models, up to 15M euros or 3% of turnover for non-compliance with obligations.

In AI Systems:

- Up to €35M, or 7% of annual turnover for companies for breaching the Regulation's prohibitions.
- Up to €15M, or 3% of annual turnover for non-compliance with the obligations of the Regulation to suppliers, importers, distributors, users.
- Up to €7.5M, or 1% of annual turnover for supplying incorrect information to notified entities or national competent authorities

In addition to financial penalties, companies may face a number of consequences for breaches of the RIA. Prohibition of use. In serious cases of non-compliance, competent authorities may impose a ban on the use of certain artificial intelligence systems or all AI-related activity on the offending company. Withdrawal of certifications and licences. If a company has obtained certifications or licences for the use of AI systems and is found to be in breach of the RIA regulations, these certifications or licences may be

revoked. Civil and criminal liability. In addition to administrative sanctions, companies and individuals responsible for the development or misuse of AI systems may face civil and criminal legal action for damages caused to third parties or for violations of fundamental rights.