ZEPOS & YANNOPOULOS

Data Protection & Cybersecurity Newsletter
22 April 2021

The European Commission releases its draft regulation on Artificial Intelligence

On 21 April 2021, the European Commission ("EC") released its long-awaited draft proposal for a regulation on artificial intelligence ("AI Regulation"). This is the first comprehensive legislative attempt to regulate AI, as it establishes a uniform framework for the development, marketing and use of AI systems across the EU. Due to its extra-territorial scope, the regulation is applicable to providers placing AI systems in the EU market irrespective of their place of establishment, evidencing the European Union's intention to become the regulatory standard-setter in the field of AI world-wide.

In line with the EC's White Paper of February 2020, the AI Regulation adopts a human-centric approach that aims to boost innovation, while safeguarding the fundamental EU values and freedoms. Depending of the level of risks, certain AI practices are prohibited, as posing unacceptable risks, whereas a number of requirements are established for high-risk AI systems and limited transparency obligations are stipulated for certain AI systems that pose increased risks of impersonation and deception.

1. Prohibited AI practices

Echoing the Cambridge Analytica case, but also in response to concerns on mass surveillance, the AI Regulation sets out a list of prohibited AI practices as contravening the EU values and violating fundamental rights. Most of these provisions are focused on the digital environment and, given their broad wording, can have a serious impact on the operation of social media companies and digital platforms. More specifically, the regulation bans AI systems which:

- manipulate human behaviour in a manner that causes or is likely to cause physical or psychological harm;
- exploit the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to manipulate their behaviour in a manner that causes or is likely to cause physical or psychological harm;
- are used by public authorities or on their behalf to evaluate or classify the trustworthiness of individuals based on their social scoring; and
- provide 'real-time' remote biometric identification and are used in publicly accessible spaces for the purpose of law enforcement, unless such use is strictly necessary for specific objectives.

2. High-risk AI systems

The vast part of the AI Regulation focuses on regulating high-risk AI systems, namely AI systems that have a significant harmful impact on the health, safety and fundamental rights of individuals. With the aim to create legal certainty, the regulation identifies high-risk AI in an exhaustive manner. Having said so, depending on technological progress, the EC may amend this list from time-to-time.

Among others, high-risk AI systems include those used in the following areas:

- biometric identification and categorisation of natural persons;
- critical infrastructures (e.g. transport) that could put the life and health of citizens at risk;
- educational or vocational training that may determine the access to education and professional course of someone's life (e.g. scoring of exams);
- safety components of products (e.g. AI application in robot-assisted surgery);
- employment, workers management and access to self-employment (e.g. CV-sorting software for recruitment procedures);
- essential private and public services (e.g. credit scoring denying citizens opportunity to obtain a loan); and
- law enforcement that may interfere with people's fundamental rights (e.g. evaluation of the reliability of evidence).

High-risk AI systems need to comply with certain mandatory requirements taking into account the intended purpose of the use of the system and based on a risk management system developed and maintained by the provider. In particular, AI systems must:

- Be developed on the basis of high-quality of training, validation and testing data sets, in order to minimise errors and discriminatory outcomes (*data governance*).
- Before they are placed on the market or put into service, technical documentation describing the AI system, its elements and process for development, should demonstrate the compliance of the system with the requirements of the regulation. Such documentation shall be accessible to the national competent authorities and notified bodies (*technical documentation*).
- Be designed and developed, so as to ensure the automatic recording of events ('logs') while the system operates, in order to ensure traceability of the system's functioning throughout its lifecycle (*record keeping*).
- Provide necessary information, in order to enable users to interpret the system's output and use it appropriately. Among others, users should be provided with instructions for use in a clear and comprehensive manner (*transparency and provision of information to the users*).
- Be designed in a way that they can be overseen, so that humans may prevent or minimise potential risks to health, safety and fundamental rights generated by the systems (*human oversight*).
- Achieve an appropriate level of accuracy, robustness and security and perform consistently in these respects throughout their lifecycle (*accuracy, robustness and security*).

These obligations primarily vest with the provider of high-risk AI systems, namely the developer or the person that has the system developed with a view of placing it on the market under its own name. On top of this, providers of high-risk AI systems are required to put in place quality management systems that ensure compliance with the AI Regulation, perform conformity assessments and retain post-market monitoring systems. Also, they need to register certain high-risk AI systems in a centralised EU database, which shall be accessible to the public.

In addition to the providers' obligations, the AI Regulation sets forth certain obligations for all relevant actors involved in the sale and supply chain of high-risk AI systems, notably to the importers and distributors, but interestingly also to the users of such systems.

3. Transparency obligations for specific AI systems

Regardless of qualifying as 'high risk', AI systems which pose increased risks of impersonation and deception are subject to specific transparency obligations. These systems are:

- AI systems intended to interact with natural persons (e.g. AI chat-box);
- Emotion recognition or biometric categorisation systems; and
- AI tools that generate or manipulate image, audio or video content that resembles existing persons, objects, places ('deep fakes').

4. Measures to support innovation

Inspired by the sandbox initiatives of some EU data protection authorities, the AI Regulation endorses the establishment of AI regulatory sandboxes at a national level to facilitate the development and testing of innovative AI systems under strict regulatory oversight. The objectives of the regulatory sandboxes, which require the close cooperation between providers and supervisory authorities, are to foster AI innovation, by allowing experimentation, and to enhance oversight and understanding of the opportunities and risks by the competent authorities.

Also, a set of measures are identified to reduce the regulatory burden for small-scale providers and start-ups, including providing for priority access to the AI regulatory sandboxes, awareness raising activities and a dedicated hub in the national competent authorities for providing guidance.

5. Supervision and sanctions

The AI Regulation establishes the European Artificial Intelligence Board, which shall ensure the supervision and consistent application of the AI Regulation across the EU. Also, each EU member state shall appoint one or more competent authorities to monitor local compliance and impose fines and other administrative sanctions.

Although liability rules are not included in the scope of this regulation, the latter provides for high administrative sanctions, which in some cases may be up to € 30M or, if the offender is a company, up to 6% of the total worldwide annual turnover, whichever is higher.

The AI Regulation will now be subject to trilogue negotiations with the EU Council and the EU Parliament.

Contact us

Mary Deligianni

Partner | Data Protection & Cybersecurity

m.deligianni@zeya.com

Nothing in this newsletter shall be construed as legal advice. The newsletter is necessarily generalised. Professional advice should therefore be sought before any action is undertaken based on this newsletter.

Established in 1893, Zepos & Yannopoulos is one of the leading and largest Law firms in Greece providing comprehensive legal and tax services to companies conducting business in Greece.

280 Kifissias Ave., 152 32 Halandri, Athens, Greece
newsletters@zeya.com
Tel.: (+30) 210 696.70.00 | Fax: (+30) 210 699.46.40

www.zeya.com
Subscribe
LinkedIn