Proposed EU Regulation on Artificial Intelligence

Members of WLG's Artificial Intelligence Group discussed the Proposed EU Regulation on Artificial Intelligence in a recent Q&A with Johannes Juranek, CMS Austria; Brian McElligott, Mason Hayes & Curran (Ireland); Kim Parviainen, Castrén & Snellman (Finland); Adaya María Esteban Ruiz and Alejandro Negro Sala, Cuatrecasas (Spain). Check out some of their insights below.

1. Give us a quick overview of the Proposed Regulation. (Johannes)
The European Commission proposed the first-ever legal framework on Artificial Intelligence in April of 2021. It's still a draft, but the model follows the NLF regulation, which stands for new legislative framework regulation. The proposal is part of the EC's larger European Strategy for Data, which seeks to "defend and promote European values and rights on how we design, make and deploy technology in the economy. The draft provides for severe penalties, like GDPR, in part exceeding GDPR penalties.

2. To whom would this regulation apply? (Johannes)
The regulation would apply to:
- providers that market in the EU or put AI systems into service in the EU;
- users of AI systems in the EU; and
- providers and users of AI systems whose output is used within the EU.

3. Define the types of systems this would apply to. (Johannes)
The definition is broader than what is currently viewed as AI, the regulation could cover e-commerce or social media platforms, and lawmakers can revise the definition of AI systems.

4. The regulation will follow a risk-based approach. What are the levels of risk and types of systems associated with those risks? (Johannes)
- Unacceptable risk (e.g., social scoring)
- High risk (e.g., recruitment, medical devices)
- Transparency risk (e.g., impersonation, bots)
- Minimal or no risk (e.g., spam filters)

5. What's an example of a high-risk system and what are the requirements for such? (Brian)
A software tool that can automate the candidate selection process as part of recruitment and employment would be considered a high-risk system.
For a high-risk AI application like this there are 7 requirements to adhere to:
- Create and implement a risk management system
- Take great care with data and data governance
- Create and provide users with technical documentation
- Accurate and detailed record-keeping
- Be transparent with information to users
- Ensure an appropriate level of human oversight
- Be diligent with accuracy, robustness, and cybersecurity

6. What are the obligations of the users and producers of artificial intelligence? (Kim)
Users and producers will be obligated to complete a so-called conformity assessment of these high-level requirements, for which more detailed standards would be developed by bodies like the European Committee for Standardization. Depending on which high-risk subcategory you fall into, you could either perform this assessment yourself and declare your conformity, or need to go to a certified testing body that will review your documentation and put the stamp on your conformity.

7. What does this mean from a compliance perspective? (Alejandro)

The framework for the proposed EU regulation on AI is based on the increasingly widespread risk-based and accountability principles. Consequently, the burden of proof will be placed on companies, and compliance teams will have a more relevant role. As will the lawyers – there will be an increase in work for them in the future.

Those principles have already been applied in data protection as from the entry into force of the GDPR by means of risk-based assessments.

Compliance would be achieved in high-risk AI systems through comprehensive ex-ante internal control checks by the providers (with the exception of remote biometric identification systems that would be subject to third-party conformity assessment), combined with a strong ex-post enforcement.

I think that a comprehensive ex-ante conformity assessment through internal checks, combined with a strong ex-post enforcement, could be an effective and reasonable solution for those systems, given the fact that the AI sector is very innovative and a real expertise in auditing this technology does not yet exist.

This pro-compliance regimen means a more relevant role of compliance teams which are subject to more duties and obligations. This will undoubtedly cause companies to expand their compliance teams and hire more professionals with this specific background.

8. Whether you're performing this internally, or hire a third party, you need knowledgeable people. Won't this be a really excessive administrative - and in particular cost - burden to companies? (Brian)

It's of course speculative at the moment, but taking the example of the AI recruitment system from earlier, the requirements need to be taken into consideration from day one, when sitting down to design a product using high-risk AI - AI by design. You'll need specific expertise that doesn't even yet exist - AI regulatory experts will need to upskill and work with the engineers from the outset. You'll see many product owners asking themselves how am I going to meet these standards, and how many new AI people do I need to recruit - and where will I even get them if they don't yet exist?

9. There's an extraterritorial reach of this draft regulation. Would it be possible in the future to just not market a product in the European Union and do it from somewhere else? (Adaya)

The scope of application of this proposed regulation is very broad and comprises:
- all actors within the value chain of the AI systems (that is, providers, product manufacturers, importers and distributors);
- covers both all AI systems placed on the market or used in the EU; and
- also, those located in a third country, where the output produced by this system is used in the EU.

Therefore, it has extra-territorial effects that go beyond the European Union, very similar to data protection regulation scope of application.

This seems quite logic considering all the globalization and internationalization. New technologies and systems are deployed nowadays in several countries at the same time, while keeping the "core headquarters" on the other corner of the world, so we need general regulations.

10. What happens if you don't comply? (Adaya)

According to this draft, and depending on the obligation infringed under the proposal, the operator can be subject to really high administrative fines, of up to EUR 30,000 000 or, if the offender is a company, up to 6 % of its total worldwide annual turnover for the preceding financial year, whichever is higher, for 2 types of infringements: (a) non-compliance with the prohibition of the AI practices that are prohibited (under article 5); (b) non-compliance of the high-risk AI system with the data governance requirements laid down in Article 10. 4, which refer to the training, validation and

testing data sets used. Just to remember, those training data shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, behavioral or functional setting within which the high-risk AI system is intended to be used.

When the non-compliance of the AI system refers to any requirements or obligations under this Regulation, other than those laid down in those Articles 5 and 10, that we have just seen, the operator shall be subject to administrative fines of up to EUR 20, 000 000 or, if the offender is a company, up to 4 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

There is also another type of sanction for the supply of incorrect, incomplete or misleading information to notified bodies and national competent authorities in reply to any request. In such cases, operators shall be subject to administrative fines of up to EUR 10, 000 000 or, if the offender is a company, up to 2 % of its total worldwide annual turnover for the preceding financial year, again whichever is higher.

As we can see, the quantification of these fines is very similar to those related to data protection. In fact, they follow the same criteria, and the same high quantities that surely will create the same fear that the GDPR did.

11. Aside from fines, what are the other legal risks according to the draft? (Adaya)

Apart from this draft regulation, AI systems must also take into consideration many other obligations in other fields before its deployment in the market: from GDPR and any other data protection obligations to other human rights and non-discrimination obligations.

On the one hand, GDPR and data protection obligations move towards transparency, legitimacy, data minimization, storage limitation, accuracy, integrity and security and accountability. In this regard, fines derived from infringements of GDPR are becoming extremely high. For instance, in Spain, the highest sanctions have been imposed to telecommunications and financial entities sectors, with fines up to 5, 6 or 8 million euros. But in Europe happens the same: UK has imposed fines up to 20 and 22 million euros; in Germany, it was 35 million; or 50 million in France.

Other fundamental and human rights, such as discrimination and equality must also be considered. For instance, in Italy there has been a couple of relevant rulings in the past few months regarding algorithms and its lack of transparency and discrimination.

Additionally, product liability and safety regulation must be considered, including where applicable sector-specific liability regulation. There is also a proposal of regulation issued by the EP on AI and product liability.

Other contractual obligations among the parties in the AI supply chain can also arise.

12. What will the impact of the regulation be on SMEs and Start-Ups? (Brian)

These types of companies could really struggle with the new proposals and indeed any flavor of them. While many of them are actually well appraised of issues like bias, ethics, transparency and explainability, they are not, however, used to actually planning and implementing a strategic compliance program to deal with those issues. None of them would be equipped with the resources or skill sets to do this. Gaining those skills or procuring them externally will be a real challenge but one they will be required by law to meet.

13. What will this impact on SMEs/Start-ups/New Market Entrants mean for the EU AI market? Could this result in having a monopolizing or anti-competitive effect? (Kim)

Yes, there is, I think, a very real risk of anti-competitive effects. The more stringent these rules are, the higher the barriers to entry for start-ups and new players of course become. These might not have the resources to navigate this complex regulatory framework in the way that larger companies are able to. And coming up with new ideas a lot of times is based on a kind of "freedom to tinker" with new technologies. This proposal will limit that, I fear.

Listen in to the full webinar