Bird & Bird

Key insights into the political agreement on the AI Act - Part 1

Podcast transcript – Feyo Sickinghe (Of Counsel, Netherlands), Dr. Simon Hembt (Associate, Germany) & Oliver Belitz (Associate, Germany)

February 2024

Feyo Sickinghe:

Welcome to Bird and Bird's podcast on key insights from the political agreement on the AI Act. This will be part one of the podcast on the new European AI regulations as it stands now, one of the hottest and debated topics in the regulatory environment as we speak.

My name is Feyo Sickinghe I will be your host today for the podcast, and I'm joined by my colleagues Simon Hembt. Hi Simon, good to see you. And on the other hand, Oliver Belitz is also here in the studio. Welcome to both of you on this podcast.

This podcast will have two parts, and this will be part one, in which we will be discussing the overall proposal for the Artificial Intelligence Act, which is in play at the moment in Brussels, the risks that are being addressed, risk categories, prohibitions, fundamental rights: in essence, the core of the regulation. The second part of the podcast will be about general-purpose AI models, open-source systems, enforcement penalties and all things you need to think of when applying artificial intelligence with the regulation coming forward shortly. And we will end the podcast, the second one, with some things to keep in mind when you're in the industry.

Just before Valentine's Day two European Committees IMCO and LIBE adopted the final text of the artificial intelligence act, paving the way for the formal adoption in the plenary votes which is scheduled in the European Parliament in April so we may expect the Artificial Intelligence act to be formally published in the European journal in May. The last 12 months have been particularly exciting for everybody following the negotiations in the Brussels arena.

We do get many questions from clients on AI also in helping them to start building an AI compliance framework, so this podcast dwells on the experience we have in talking to our clients on how to do this and to bring them to the next level of compliance given the status we're in.

So that, by means of an introduction, we go to the heart of the content, but before we jump into the regulation, first question to you Simon - Why do we need an AI regulation in Europe?

Dr. Simon Hembt:

Many thanks Feyo for the intro and for the first question. Yeah, I think AI is everywhere, we hear about new developments almost on a daily basis in the news or read on social media some new posts about it.

There are many benefits and many use cases for AI. Let's think of AI generated advertising, media, video games, we can use it in research, we can use it for healthcare, for infrastructure, for logistics, consumer goods; the list goes on and on. But there are also some risks for these use cases, and the risks differ massively. While AI generated content poses maybe some low transparency risk for some citizens, the control of critical infrastructure with an AI or public biometric surveillance of all citizens is associated with risks

that we are not really willing to accept, or they are so high that we need some regulation to cover it.

The European legislature therefore decided to regulate these risks in a tight model by a comprehensive set of rules, which is called the EU AI Act. The aim is to create a level playing field for all providers and deployers of AI in order to protect the rights of EU citizens.

Feyo Sickinghe:

I'm sure that this regulation, once it's out there, it will serve as an example in the so-called Brussels effect for other jurisdictions as well. When I was in Washington last November to speak about the AI regulation in Europe, I noticed there's great interest from the US audience and US businesses to see how we deal with it in Europe, not only for them in terms of doing business in Europe, but also to anticipate what might be coming towards them in the US. And that kind of shows the large interest we see in this regulation. So, there is a clear need for regulation in terms of risk management and to create a coherent approach and to prevent people from the need to invent the wheels themselves and all the uncertainties that would be pursuant to that.

Then if you go a bit deeper, which are the risks that this new AI bill will address?

Dr. Simon Hembt:

The AI Act is fundamentally a product safety law. Its core task is to find appropriate answers to different risk profiles of AI applications. The AI Act is protecting safety, fundamental rights and the democracy itself.

If you think about the safety of citizens, for instance, when we kind of control our infrastructure with AI, we think of heating, electricity or water supply, this could definitely pose dangers to life or health for the citizens. Also, you think of various degrees of severity, AI can also interfere with people's fundamental rights, if an AI decides on the admission to a university, or a job, or grants a loan, or makes decisions in law enforcement.

Feyo Sickinghe:

You mean bias - biased outcome of algorithms? Is that what you mean?

Dr. Simon Hembt:

Yeah, it's like if you get a black box and an AI algorithm and you cannot understand the decision, this opacity which we will - a subject we can discuss later on - it's important to understand why I'm not getting this loan.

There are many risks with AI systems so definitely the AI Act will need to find answers and does find answers for product safety, fundamental rights and democracy.

Feyo Sickinghe:

The examples you give are focused on what it would mean for you and me as an end user, as a consumer. Can you give us some examples how this would turn out in business-to-business relationships?

Dr. Simon Hembt:

In business-to-business relationships it’s also very important. If we work together, e.g., if you find some tools we use in clinics or in life sciences sector, it is also important between companies that there is a level playing field, that other companies can rely on that the AI provider is compliant with specific standards which in particular the AI Act is setting up. It’s kind of a great act that is setting the stage to implement standards for all stakeholders in the market.

Feyo Sickinghe:

That really makes sense I would say.

Another question to you, Simon; whom does this act apply to? Is it only applicable to companies who act from Europe? How about companies outside Europe?

Dr. Simon Hembt:

The key criterion for the applicability of the EU AI Act is whether the AI is placed on the European Union market, as a product or service, or its use affects people located in the EU. So, the next step would be that the addresses like providers and deployers of AI systems, which are placed in the European market or affect people here.

Feyo Sickinghe:

Deployer, that's a difficult word. Is that the same as a user or is that different?

Dr. Simon Hembt:

‘Deployer’ is, for instance, a company which is using an AI tool, e.g., companies implementing a large language model as a chat bot, a bank for instance, or it could be also a healthcare provider which is using an analytic AI to analyse some CT screenings, for instance. So, this is a deployer.

Feyo Sickinghe:

So that means it has a very broad scope. Everything that's being used and placed on the market in the EU is likely to fall within the scope of the regulation. Whenever you do something in Europe with AI, regardless of whether you are in EU business or operating outside of the EU, you still need to look into whether you're forwarding the scope with the products you use and deploy.

Let's talk about the risk categories. The AI Act has a risk-based approach and there's a lot of talks of what those categories exactly mean. Maybe a good one to pass over to you, Oliver, on how does that look like? And then, Simon, please jump in whenever you think that it is necessary.

Oliver Belitz:

Yes, of course. We already talked about this tiered approach. So, the core mechanic of the AI Act is that the AI Act categorises AI systems into certain categories depending on how much risk they pose for humans.

Maybe the first category is not AI Act applicable to that AI system, that is, for example, military use. Military use is explicitly excluded from the scope of the AI Act. The next category is minimal risk that maybe we will talk about later. Those are AI systems that only have to adhere to certain basic principles without a sanction. If they do not adhere to those principles then we have a category for certain AI systems that is a kind of basic transparency that applies to AI systems that are built for human interaction; AI systems that we right now call generative AI systems that produce, pictures, text and video that we have a certain transparency obligation to forbid deepfakes. And then we get to the high-risk category. So, I think we will talk about that in more depth in a minute. There we have some strict obligations facing deployers and providers of those systems. Next category is general purpose AI. I think you already said this will be the focus of our second part of the podcast and then the last category is prohibited systems. So, systems that are not allowed regardless of how you use it and how you deploy it.

Feyo Sickinghe:

There has been lots of talks on which type of system would fall in which category and that's being transcribed into the annexes of the regulation.

But then, still the question comes up - assuming that the AI Act will be adopted as it is now, will there still be room for AI systems and models which not do not have to adhere to any obligation at all? Is there still a subcategory under minimum risk?

Oliver Belitz:

Well, the minimal risk category kind of changed in the last draft. You spoke about the leak, before this leak in the version in the political agreement that was reached in December, we had an article that talked about basic principles, and it was it was not clear back then whether there will be any sanctions if you do not adhere to those principles.

In the current leak, no article speaks about those basic principles anymore, they are only mentioned in a recital. So, let's say the scope of this category changed a bit and now it is more of a recommendation so to say. So, a lot of AI systems will fall into that category which we call, that's not a term of the AI act, which we called 'minimal risk' and they shall adhere to those basic principles.

Feyo Sickinghe:

And we are not sure whether that was taken out on purpose or that it was an omission. But it does have consequences in practice, whether there is still a category left which has no need to adhere to the general principles or not. So, there's definitely something to look at later on.

Oliver Belitz:

Yes, and this will be the majority of AI systems.

Feyo Sickinghe:

Yes exactly. So, one can hardly say that it was an omission that was not made on purpose but well, let's see how that how that turns out, but definitely something to look into.

How can I know whether an AI system is high risk? What do I need to do? If I was a company, what do I need to do?

Oliver Belitz:

The current version of the AI Act provides for a certain system for classifying whether an AI system is high risk or whether it is not. I would say it is a three-step system. The first step is if an AI system is intended to be used as a safety component for certain products and those products are listed in an annex, for example, machinery or personal watercrafts, lifts, pressure equipment, all kinds of products that fall under a certain Product Safety regime in the EU, if the AI system is intended to be a safety component in those products, that is high risk AI, that is the first step. The second step, I think you've already mentioned that we have currently an Annex number 3 and the Annex number 3 lists certain use cases that will indicate that a certain AI system is high risk, that is the second step. The third step is a filter system that came up in the

trilogue negotiations somewhere in September last year, and those are exemptions.

Feyo Sickinghe:

That was a new invention in terms of regulation. I haven't seen it before.

Oliver Belitz:

That's completely right. I think some ember States were afraid that too many AI systems will fall under the high risk category because it's relatively easy to fall into. I think we will talk about the examples, but, for example, critical infrastructure or law enforcement, there are a lot of AI systems that could fall in this use case category and then they wanted to make sure that only systems that actually pose a high risk for humans fall under that category and they try to achieve that by implementing a new so-called filter system.

The filter system is nothing more than four exceptions and if one of those exceptions apply a system is no longer a high-risk AI system, and those are, for example, if the AI system is only performing a narrow procedural task. So, we will have to see what exactly is a "narrow procedural task" but that would be one of those exceptions and then an AI system, for example, used in critical infrastructure is no longer high-risk AI.

Feyo Sickinghe:

So, companies need to follow a three-step approach to see whether their product is listed. In general, in Product Safety regulation or whether it's on the list and if so, whether any filter conditions apply and that still is very broad, but I'm sure the Commission will be coming with some further guidance on that.

Two topics shortly to discuss before we round up. One of the most heated points was the new prohibitions: Which AI systems will be prohibited? Can you give us some examples, Oliver?

Oliver Belitz:

Yes, of course. One example would be social scoring. If you use an AI system to create a scoring system for all people that will later on decide whether they will be able to get a certain job, for example, or if they get a certain flat. So social scoring is prohibited. Predictive policing is prohibited as well. For example, if you use certain characteristics of a human being and then come to the conclusion that this human being will commit a certain crime and you start law enforcement based on that information alone without a human loop, that would be prohibited as well. Another one is, for example, emotion recognition in the workplace. So, there are some examples for prohibited systems.

Feyo Sickinghe:

Yeah, facial recognition, post and real time have been discussed very much in heated debates but will be allowed under very strict conditions for law enforcement purposes and the exact wording will tell us how strong those requirements will be. But that has definitely been one of the most heated topics in the discussion so far.

Last topic for now to discuss - Simon, we briefly touched upon fundamental rights already; one of the new things that comes up, a fundamental rights impact assessment has to be done. That must be quite a challenge, because the fundamental rights concept, it is clear what it is, but how to do that? And who should do it?

Dr. Simon Hembt:

Yeah, this is what’s new in the latest version, not in the January version or the December version of the AI Act. We found that bodies that provide public services, either governed by public or private law, like banks or insurers, have to conduct a fundamental right impact assessment here. And what is it? This assessment should include details of how the high-risk AI system will be utilised within the deployer's operation. For instance, the duration and the frequency of its intended use, the types of individuals and groups who are likely to be impacted by its deployment in the specific context, the particular risk of harm that could affect these individuals or groups, a description of how human oversight will be implemented, and the measures planned in event of a risk realisation. So, this will definitely be a new obligation for deployers of such high-risk systems that provide for public services, it's really advisable to prepare in advance and to establish the structures to comply with it.

Feyo Sickinghe:

I would say a fundamental rights assessment, in itself is fundamental for applying high risk systems and how that would work out is also something that that needs to be tested, also in conjunction with the GDPR, the Privacy Regulation which is in place.

Lots of food for thought and thinking how that would work out, but, for now, we come to a close of part one of this session.

Many thanks to you, Simon Hembt and Oliver Belitz, for taking us to the essence of the artificial intelligence regulation.

In part 2 of this podcast, we will address general purpose AI models, how they will be regulated, the threshold for general purpose AI models, the systemic risks, biometric identification, open-source AI systems, how to deal with it, bias enforcement penalties and some things to keep in mind when applying the AI Act.

Thanks for now and stay tuned, stay healthy and stay safe with AI.

twobirds.com

Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca • Copenhagen • Dubai • Dublin • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Luxembourg • Lyon • Madrid • Milan • Munich • Paris • Prague • Rome • San Francisco • Shanghai • Shenzhen • Singapore • Stockholm • Sydney • Warsaw