THE INFLUENCERS: DIGITAL TRANSFORMATION

TRANSCRIPT

Kai Zenner

Leo von Gerlach	Hello, everybody, and welcome to another edition of the influences our podcast conversation on digital transformation and law. I'm Leo von Gerlach. And with me today is Kai Zenner. Kai is one of the masterminds behind the AI Act of the European Union. He serves as digital policy advisor at the European Parliament, and he is, more broadly, closely related to all aspects of Europe's digital agenda. As you may know, Europe has a very ambitious Digital Agenda to not make it one of the greatest innovator places, but at least one of those places who dedicate on digital regulation. Kai, great to speak with you today. Perhaps, let me start with a personal question. How do you evolve into your current role as a digital advisor at the European Parliament?
Kai Zenner	Sure. So first of all, many thanks for the invitation. And yeah, it was a little bit of a journey. I started my work life here in Brussels at Konrad-Adenauer-Foundation, a think tank from the Conservative Party in Germany, I was at the beginning starting to focus on data protection, but then more and more on artificial intelligence, when it started to become slowly a major topic for the European institutions.
Leo von Gerlach	Interesting. So just sticking with your personal story for a while. What have been the most challenging cliffs to get the AI Act across the finishing line specifically for you personally, but perhaps then also, in more general terms?
Kai Zenner	Yeah, I would say that we, in the European Parliament especially made our life particularly hard, and it was a little bit unnecessary. So we had a lot of drama, like you know it from television shows, and so on, it was a lot of egos that had particular interests or ideas. And even though artificial intelligence, of course, is also a topic where political parties have very different opinions, some of them have strong fears, others have strong hopes. It was really this personal element that made the process extremely hard. We had always setbacks, we had a huge fall outs between certain groups. And then we needed all with a lot of time to reestablish the communication channels. And maybe topic wise, I would say generative AI was a particular difficult topic because it was coming rather recently, and after the Commission made the initial proposal, so we needed to do a lot of catch up work. And the second topic, what was very hard was law enforcement agencies and their development and deployment of AI. Because there basically you have a 50/50 split in the European Parliament, and also some member states that want to have huge freedoms for their law enforcement agency, which is kind of a red line for especially left wing political groups in the Parliament. And this made or created an almost impossible to solve situation.
Leo von Gerlach	So much now on the legislative process and how that felt now turning to the outcome to the result. How do you feel about what has come out of it? How do you feel about the repercussions that this may have for other

	legislators around the world? And how do you feel about the effects overall?
Kai Zenner	I have really mixed feelings. So I think we did a lot of very good things with the European AI Act. We created principle base and more much more future proofed legislation. But on the other hand, due to those emotional fallouts that we had, and also this huge time pressure, there are a lot of flaws in the AI Act and yeah, it's a bit sad that they are there because they could have been easy to avoid. So let's say an advice that I would give other regions of the world if they are thinking about regulating AI or creating an AI policy is really to take your time, don't think about you need to adopt the AI law in under a year or whatsoever. It's such a dynamic field that everything should be really, really, really strongly assessed. And especially since AI is a horizontal topic, it's probably best to try to bring together all those different sectors and have also the very, very clear assessment, what are the effects? What are certain things that are working in one sector, but not at another sector, and so on. And here, I think the European Union could have done a little bit more.
Leo von Gerlach	So time is clearly a very relevant factor. And there are flaws due to the timing, but then also, the European legislator wanted to move fast, because he wanted to set the standard. And leading to the question: do you think the European legislator will achieve that goal of just having produced a kind of, let's say, gold standard for AI regulation? And perhaps more broadly, what would it take to grow into such a prestigious role of being a blueprint for AI regulation going forward?
Kai Zenner	I think the jury is out a little bit. So I think many, many regions or more countries around the world are of course, observing, monitoring very closely what is happening in the European Union. And we have a little bit of competition. When it's coming to AI policies or AI regulatory frameworks. We have as the UK approach, we have the U.S. approach with more sectorial strategy as the executive orders that is then implemented by sectorial agencies. We have a code of conduct in Singapore, the automated decision making law in China, in Canada a law. My assessment right now is that, again, there's now a kind of monitoring process, people will check what is really working, where are problems, where are certain best practices. And I could see a situation that maybe some states are now waiting for one - two years to have a better view and then probably cherry picking a little bit from here, a little bit from there and building by - with those pieces, a perfect solution for their own legal system. And of course, if now the AI is working quite well, then the chance would be indeed, there is at large parts of AI are copy-pasted, or at least then taken over and adjusted. As I said, the next month and the next one to two years will be decisive.
Leo von Gerlach	Let’s dive a little bit into the content of the AI Act. What do you see as the stand out provisions? What does make the AI Act special in particular, as opposed to other attempts to get their legislative arms around artificial intelligence?
Kai Zenner	This is easy, I always summarize it with three main conceptual points because we kind of touched it already. The AI Act is based on international principles. So there was a lot of prep work in UNESCO, G7, G20, OECD and so on. So you see things like transparency, human oversight, basically and all those different policy approaches that I have listed already. What makes the European AI Act really special is typical for Europe unique combination of product safety law, the so-called new legislative framework, which worked very well in the past for diverse

	products like medical devices, toys and so on and so on. Then, we combined it with fundamental rights protection, then we combined it with a risk based approach that is basically focusing on forbidden AI systems or high risk AI systems. And the European Parliament in the end also included value chain approach, meaning that not only those actors that are using AI systems, are producing it, should be covered by the law. But also, all those actors along value chains that are playing a part. And those three things. So product safety, then the value chain and this specific type of risk based approach, I didn't see to that extent in other areas of the world.
Leo von Gerlach	So you spoke about the actors, the agents whose activities are going to be regulated. And that brings us straight to the application on individual businesses and how they should align with the new regulation, perhaps to start there, what are the most immediate consequences for a business for those who provide or deploy a system with regard to the AI Act?
Kai Zenner	I think every company should really, right now do a proper assessment of what they're doing, how they're doing it, and so on. Many companies are already using AI, quite heavily, maybe even without knowing it. So this kind of principal assessment, internal assessment is really key. And on top of that, or basically, based on the conclusions, you as a company then need to check, okay, which systems now, are maybe already kind of aligned with what the AI Act is trying to achieve? Where do we need to do adjustments and so on? The most immediate or the most urgent area is, of course, the prohibitions in Article 5, because according to Article 113, there is only a transition period of six months, meaning that if now the AI Act is entering into force, in the summer, companies could already face prohibitions in the end of the year. And this could, for example, mean, that commercially used practice or technology that you as a company have sold so far without a problem is suddenly facing the prohibition, which means that after identifying those potential technologies for prohibitions, those companies should immediately reach out to the Commission, to engage in some dialogue, if this is really a consequence that the commission is aware of, I would say is this is really the most important point right now.
Leo von Gerlach	So this is really interesting. And as you said, important, so the unacceptable risks, and the systems that play to them will become prohibited already at the end of the year. So unacceptable risks relate to those that are, let's say, facial recognition databases, that are social scoring applications that may be manipulative techniques at the workplace. So there are a number of very, let's say, general terms in those prohibited applications. How much actual problem to understand what that means do you expect?—You mentioned the communication with the EU Commission. Will that solve the problem for the businesses?
Kai Zenner	I really hope so as I said at the beginning, for me, the AI Act is a mixed bag of really good ideas, really good chapters, but also bad articles, bad paragraphs, and for me, Article Five, belongs to the second category, I think, many of those prohibitions, and again, I underlined already that the effects could be severe, it could happen that certain useful practices are certainly prohibited and why? Because indeed, if you check Article Five, it's not really clear what is now exactly social scoring, the recitals are helping a little bit. And there are also other cases like emotional recognition, where it's written down that, for example, those anti-sleep systems set up for example, detecting sets of pilots in a plane is starting to get very tired, that those are not falling under the prohibitions, but there are hundreds of other use cases where it's not clear at all. What could help is based on companies reaching out to the Commission or the

	AI Office, on behalf of the Commission will provide additional guidelines according to Article 96 of the AI Act. And one of those guidelines is exactly about the questions that we are discussing now, what those prohibitions really mean? So you will see probably much more information in those guidelines. The problem is, of course, is guidelines are not legally binding. And therefore, companies do not have full legal certainty in any case.
Leo von Gerlach	Perhaps moving from those important unacceptable risk applications now, to the main area of the AI Act, those high risk applications, that's again, a broad term within the meaning of the AI Act, because it enshrines all the applications that are relevant to get access to critical infrastructure, such as education, or employment or financing and the like. Given the broadness of that application of “high risk application”, do you see most AI systems falling under this high risk category?
Kai Zenner	It's a really good question. The Commission would argue, no, they never did impact assessment on this point, as the Commission itself never checked, how many systems would for example, qualify as high risk, there was an annex study from the Brussels-based think tank CEPs, which was doing it in 2021. And they assumed that five to 15% of all AI systems in 2021, would qualify as high risk, but CEPs themselves already in 2022, I think, or 23, were saying that probably this assessment should be updated, because this number may be is not correct anymore. So actually, when it comes to high risk, but the same also for prohibitions, right now, no one really knows, what is the evidence? What is the number, so it should be maybe risk pyramid, which would mean the lowest amount as a prohibitions under 1%, the top of the pyramid. But if this is really happening in the reality and practice, again, no one knows. And due to the fact that, as you said, those high risk categories are also rather broadly and vague, similar to the prohibitions, it could happen that a lot of stuff is falling in those subcategories. You mentioned, critical infrastructure, it's mentioned in this particular point, annex 3.2. That's the operation and management of critical infrastructure, as high risk, is it already a drone that is being used to double checks is safety, the reliability of a certain critical infrastructure element? I would say it's reducing risk. So it should not be there. But you could definitely argue also the opposite. The only things that will help is that also on that point, there will be additional guidelines by the European Commission. So hopefully in the future, it's more clear.
Leo von Gerlach	So there is the question, what is high risk and what is not? But there is the additional question, what is “high risk” and how does it relate to something different that the AI Act regulates, namely, general purpose AI or so-called foundational models, which just cuts the pie in a different way? So how do you see the mechanics, the legislative mechanics working in the relationship between high risk system, their regulation and general purpose AI, and their regulation, and how it fits together?
Kai Zenner	Let me give you a practical example. The European Parliament was kind of thinking of this kind of way you’ll see in the example in the following way, say is GPT-4 from OpenAI, which is the foundation model. This foundational model is completely undefined. Very broad, doesn't have any intended purposes and so on. ChatGPT, however, also from OpenAI, of course, is already a general purpose AI system, because it can be already used for certain purposes. It's still a general purpose AI system because it has hundreds of different purposes, but it's already much more narrow compared to GPT4, so the baseline foundation model and what we wanted to do as European Parliament. In the end the way we were able to bring it through was to first of all, make sure that the

	model developer is already designing the model to an extent that is possible in a way that is coming closer to the high risk obligations that later developers need to fulfill that are building their AI system on top of the model. And secondly, that the model provider, sending all the necessary information about some model downstream to all those players, as I said, that are developing high risk AI systems. So in the end, again, we have this value chain approach, and hope now that it's working in practice, meaning that all is important information from upstream is really going to downstream in ways that enables downstream actors to become fully compliant with the AI Act. One remark I need to make, it's rather difficult now to think through cases where already a general purpose AI system like ChatGPT is used for high risk use cases, the whole AI Act was having the intention to only regulate narrow, high risk AI systems that have one intended purpose. So for example, one AI systems that is only used for a specific education purpose. But of course, with ChatGPT, you can use it for education purposes, for employment purposes, for also others that are not high risk. And therefore, it's not really clear right now what will happen with those systems that can be used for multiple intended purposes, some of them high risk.
Leo von Gerlach	So here may be a likelihood that we need to look at these two providers in conjunction both the foundational model provider and those who provide the downstream application, the foundational model provider just being responsible for the interoperability and the documentation of the transparency of all this and the application provider then for the additional regulation requirements, leading to the question of how challenging will that be for either of them, in terms of the progress of technology, the abilities and inabilities to be compliant with some of those requirements? To give an example - How easy will it be to watermark any generated content by a generative AI model? How easy will it be to comply with providing summaries of the training material that had been used in the purpose or in the context of pre training? So how much alignment is there between technology and the requirements of the regulation?
Kai Zenner	As I said at the beginning, I think the whole AI Act was well intended. But especially now in the implementation phase, it's really creating a huge new, let's call it AI governance ecosystems that need to be built up first. And also, best practices need to be identified – how to, in your example, how to do a proper summary of the copyright protected content should be written or drafted. Right now, no one really knows. There will be a template from the European AI office that is specifying it when the office will publish this template. Well, no one knows right now. Hopefully, it will be in summer because then the rules will become already applicable. But to stay with this example. Right now, the practical implementation is completely unclear. So there's a lot of legal uncertainty due to this vagueness in the AI Act, but to also defend a little bit the AI Act and the policymakers or the EU here, I think it's rather typical for such a groundbreaking new piece of legislation that you have a kind of transition period and because of that, we have actually different transition periods for the AI Act, which you can see in Article 113. So there are a lot of things happening in the next three years, and a lot of additional pieces of secondary legislation will be added.
Leo von Gerlach	So I understand a number of uncertainties remain, there are certain challenges to pave the way perhaps to conclude, what are the tools, the additional tools that any of the European Union institutions is going to provide to make life of business easier, you spoke about templates, you

	spoke about guidelines, perhaps a word on what we can expect to make it easier to actually apply the AI Act to understand what it all means for our respective businesses.
Kai Zenner	First of all, there will be hopefully in time harmonized technical standards from ISO from CEN-CENELEC. From the national standardization bodies, and that should do the vast majority of specifications giving a clearer picture in technical terms, how, for example, provide proper data governance in accordance with Article 10 of the AI Act and so on, then, indeed, there will be additional guidelines, according to Article 96, then there will be delegated Acts implementing Acts from the European Commission, there will be those templates and other pieces or other structures like a single point of contacts, and so on, and so on. And on top of all of that, there is also this idea of public-private partnership in the AI Act, there will be things like Regulatory Sandboxes, where legislator or enforcement bodies can join regulatory dialogue with companies and both of them can figure out what are the best ways to make a product or service compliant with the AI Act and there are also new mechanisms, or, let's say bodies, in the whole, let's call it a digital governance system of the European Union, for example, the advisory forum or the scientific panel, where companies can join. And in this new advisory groups, they are also having the chance to indicate that they have certain problems, they can flag risks or new opportunities. And all of that should really create a much more future-proof and cooperative piece of digital legislation. But of course means also that companies now need to be much more active than in the past. They need to contribute in order to make this system work.
Leo von Gerlach	Kai, this is extremely insightful, has been fascinating speaking with you I'm sure we will be speaking again, but for now, thank you so much for joining and thank you everybody for listening in. I hope you'll join us again for the next session of the Influencers, which will be coming up soon but for now take care goodbye.