EU AI Act Webinar - 20.03.2025

Hello everybody, my name is Monica Fernandez and I will be introducing you to the EU Act and key actions for 2024 in order to address it. Like I said, I'm Monica Fernandez and I am the Head of AI Assurance at Nemco Digital. I have a background in neuroscience and artificial intelligence and I have always been working on projects related to AI policy, education and research.

Without wasting any time, let's start with an overview of the policy frameworks that we see going on around the world. There's a lot of things going on in the US, Canada, China, UK, major regions. However, it is with no doubt Europe that stays the most mature when it comes to AI regulation.

This is because of the AI Act. However, if you want to stay updated on the regulations and guidelines and proposals that are coming out around the globe, feel free to sign up to our AI Trust Hub for free at ai-hub.nemco.com. Here you can find libraries of regulations and standards all related to AI as well as inside articles in a collection of our past webinars, all touching on topics like the AI Act or ISO 42000 and other major regulatory frameworks. Again, to stay updated, also feel free to follow us on LinkedIn where we also post news about the regulations and policies coming out in different countries, in different regions, as well as insights and reports on general AI governance and AI policy.

Diving into the EU AI Act, the AI Act is the first regulatory framework that covers all types of AI systems across all sectors. The most important thing to understand about the AI Act is that it follows a risk-based approach to AI regulation and it sets clear compliance and transparency requirements for all these different risk levels. Of course, as with every regulation, there are hard penalties to consider and we'll touch on these penalties in a few slides.

And this regulation is having a global impact on AI governance because we are noticing that other regions and other countries are starting to get inspired by this regulation and they're drafting their own regulatory frameworks using similar risk-based approaches or similar requirements when it comes to developing and deploying AI in a safe and trustworthy manner. Now, this regulation was adopted in 2024 but it will be fully enforced in 2026. Now, the risk categorization under the EU AI Act.

The risk categorization under this regulation can be visualized in a pyramid scheme where at the top of the pyramid we have prohibited AI practices. As the title suggests, these practices are completely prohibited in the EU and I will give some examples in just a second. And then we have high-risk AI systems which is what most of the regulation is drafted for.

So, high-risk AI systems that must undergo a conformity assessment and that must adhere to different sets of requirements to a very long list of requirements. Then we have certain AI systems or limited-risk AI systems that must adhere to transparency requirements mostly. And then as a different category, we have general-purpose AI models which they differentiate

between those with or without systemic risk.

And these, due to the nature and complexity of these types of models, they have to adhere to a different set of requirements. Now, here we find some examples. Again, this is a non-exhaustive list of examples and we can see that under the prohibitive AI system category, we find practices that are those involved with social scoring or behavioral manipulation of any kind or systems that can be used for emotion recognition in sensitive places like the workplace or schools or biometric categorization that deduces sensitive characteristics of people.

Then under high-risk AI systems, we have systems that are covered by central product safety regulations like medical devices or vehicles or toys. And we have biometric identification, categorization, and emotion recognition that does not fall under prohibited practices already. And then systems that are involved in the access to essential services or that are involved in education and vocational training or involved in employment and workers management.

Then in the category of certain AI systems, we have systems like chatbots or certain generative AI or those that can create, generate deep fakes. And then as a separate category, like I said, we have general purpose AI models like Gemini or any other general purpose AI models with multiple functionalities. Then as key requirements for high-risk AI systems, we will be looking at this list.

Well, this is only a brief overview of the list. Of course, there are some more details to it, but just to get a brief overview, providers of high-risk AI systems must adhere to requirements related to risk management, to data and data governance, to transparency and provision of information. So making sure that you're providing enough and appropriate information to the deployers of your systems.

You have to implement human oversight measures and ensure there's enough accuracy for business and cybersecurity measures in place, as well as taking care of quality management systems and that your AI system is part of this quality management system. And then, well, there are other requirements, but one of the most important ones as well is to register your system in the EU database and of course, cooperate with supervisory authorities. Then the obligations for deployers of high-risk AI systems are a little bit more relaxed than those of providers, but there are still some, as you can see.

So the first few obligations are related to basically obtaining all the information that they need to obtain from the providers and follow the instructions of use correctly, implement still human oversight measures and make sure that the data that is being input into the system is appropriate and implement ongoing monitoring and evaluation measures to make sure that the system is performing as it should. And then we see other requirements that we have already seen in those of providers of high-risk AI systems like regulatory cooperation, cooperating with with supervisory authorities when needed. And then as key requirements of general purpose AI models, we have those that are, well, they're normally about transparency over training data and implementing policy to comply with EU copyright law and of course,

produce and maintain technical documentation.

Well, at least enough information to also give enough information to downstream users. And then general purpose AI models with systemic risk have to adhere to an extra set of requirements on top of the already existing requirements for general purpose AI models. And this involves notifying the European Commission that you are a provider of a general purpose AI model with systemic risk and that you deploy model evaluation adversary testing in your models and that you employ cybersecurity processes in place as well as reporting incidents and deploying a different set of risk mitigation measures that are more appropriate for these kind of models.

As with every regulation, there are hard penalties to consider. Non-compliance with prohibited AI rules will be facing 35 million or up to 7% of total annual turnover. Non-compliance with other obligations will be a little bit less but still pretty significant, up to 3% of global annual turnover in fines.

And then the most fines, the most cause of fines that will be seen will be those that are about supplying incorrect, incomplete or misleading information to regulators where companies could be facing up to 7.5 million euros or up to 1% of global annual turnover in fines. Now this is what the timeline looks like for the EU-AI Act. The EU-AI Act is a living regulation.

We'll be seeing that certain obligations are being enforced in different time points and delegated acts and additional guidelines will be also released and published as time goes by, at least until 2027. And at the beginning of the timeline, we can see that the regulation was published and it came into force in August 2024. And then in February of this year, the bans on prohibited AI systems applied as well as the AI literacy rules.

And in August of this year, the provisions of general purpose AI models come into place. Now I'm only going to focus on the first half of this timeline due to the time limitations that I have for this webinar, but there will be another webinar that can focus on the second half of this timeline. Now, even if your obligations as an organization does not fully apply until let's say 2026 or 2027, it doesn't mean that you cannot act today.

It's really good enough that you're listening to this webinar that you jumped into to learn more about the AI Act. But what Nemco Digital is offering to companies today is the AI Trustmark that basically assures clients of transparency, reliability, and regulatory alignment with major regulatory frameworks, including the AI Act, so that you as a company can enhance user confidence and increase market credibility. Now, jumping into bans of prohibited AI systems, these came into effect in February 2nd of 2025, so basically only two months ago.

And what this means is the following. Now, fines apply on August 2nd of 2025. And like I said, these are the biggest fines that one would be facing.

And what one should be aware of is that there are also a lot of exceptions, and that the list of

prohibited AI systems will be reassessed annually. And of course, prohibitions apply irrespective of the role of the actor. So it doesn't matter if your company is a provider or a deployer or even a distributor or an importer of AI systems.

If you fall into this category, if you are bound to be involved with these kind of practices, you would be facing fines of this scale. So basically, what should be in your to-do list is that you have to examine basically your AI systems and determine if they are prohibited or not, and then review the list of prohibited practices yearly for any kind of updates as this may change. And then last but not least, you should consider whether any of the exceptions apply.

AI literacy rules. These also came into effect on February 2nd of this year, so two months ago. And these apply to providers and deployers of all kinds of AI systems.

It doesn't matter the risk level. And what this means is that providers and deployers must ensure that there is a sufficient level of AI literacy among their staff and those acting on their behalf. So what should be in your to-do list? Now, there are no clear guidelines in the regulation of what you should do as part of AI literacy, but there is a good amount of best practices out there.

And what we have done at Nemco Digital is that we have developed our own AI literacy scheme that involves, that puts all of these best practices together to ensure that your staff and those acting on your behalf and that are involved with the AI system have a sufficient level of AI literacy. So this is reflected in this to-do list, what our AI literacy program looks like, and we're going to give a webinar on this at the end of this month, I believe on the 31st of May, of March. But this is what the program looks like.

It basically starts off with us helping you assess AI literacy readiness in your organization and define a strategy of how to do this. Then, of course, one has to define the capability requirements. So this involves mapping the roles and responsibilities with AI training outcomes, as well as assessing any required skill sets that will be based on the AI application and its risks, its intended use, and so on.

Then, of course, you would train your staff, one has to train their staff and facilitate cross-team sessions or measure learning impact. And then last but not least, implementing governance for continuous growth structure is a crucial step in the AI literacy program, because this doesn't only involve AI literacy refreshers, but it also allows you to monitor the capabilities and also benchmark against industry standards. This is an overview of, well, a complete overview of the primary AI-related roles in an organization that can be used to structure and build a robust AI literacy program.

We will dive into these roles better in the AI literacy webinar that we will be holding specifically for this. General purpose AI models. Now, the rules for general purpose AI models come into effect on August 2nd of 2025.

And what this basically means that in a year's time from then, the fines will apply. So on August 2nd of 2026, the fine will start to apply for general purpose AI models. Now, general purpose codes of practice are being drafted right now, and they should be available around May of 2025.

And this will give more indications and guidelines of how to implement on a more technical level the provisions of general purpose AI models. And in everyone's to-do list, the only task that at least for now one should have is that you should understand the concepts and relationships between general purpose AI models, general purpose AI systems, AI systems, high-risk AI systems, and understand how these different concepts are reflected in the regulation and what does that mean for you as a provider or as a deployer of a general purpose AI model that is embedding it into a bigger system. How does this affect the obligations that apply to you today? For providers of general purpose AI models is what the to-do list should look like.

Now, first of all, one should undertake a thorough governance review and make sure that they can make the necessary adjustments to ensure compliance. Then one must perform a thorough IP assessment as the requirements are quite deeply connected with IP laws, especially copyright and data training applications. And one should continuously monitor the threshold of systemic risk as this may be adjusted over time by a delegated as like similar as with the list of prohibited AI practices.

This can be changed annually, so one should stay away and monitor the threshold of this. And then last but not least, one should stay aware of codes of practice as these could include specific and technical details on how to comply with the obligations more in practice. Now, forthcoming initiatives.

These initiatives may be coming out or will be coming out at least until August 2nd of 2027. So we can expect that throughout these two years, there will be delegated and implementing acts adopted as well as guidance documents, codes of conduct, codes of practice, and even standardization requests to support the living regulation of the AI Act. In terms of standards, the European harmonized standards will be available around the end of 2025.

However, the European standardization bodies in charge of these standards, they have broadly agreed that the companies that comply with international standards like on AI, for example, ISO-IEC 42001 can leverage their original compliance to meet the relevant provisions of the AI Act. So as part of your to-do list, you should monitor the work of the Commission in developing the legislative and non-legislative initiatives and seek to comply with international standards on AI, including ISO-IEC 42001. We will also have short and longer webinars on ISO 42001 that you can join and learn more about in future webinars.

So what to do today? What we tend to tell our customers is that as a first step or one of the things you can do today is take care of your AI inventory. So take care of what systems and models are you dealing with today or are you planning on dealing with or developing or using.

Make sure you have complete visibility across all AI operations, maintaining the necessary records of all these systems and models and to ensure a level of transparency and make sure that you have the documentation in place to start any governance journey you may want to start in order to start adhering to regulations like the AI Act.

Then taking care of your AI inventory also naturally allows you to assign clear responsibilities and keep track of any decision-making processes and integrate a certain level of human oversight. You can also classify and manage risk levels according to risk-based regulatory frameworks like the AI Act or your own risk analysis and you can also track life cycle stages ensuring proper updates, maintenance and the commissioning of systems whenever they have to be decommissioned. So there are good practices involved with taking care of your AI inventory that naturally helps you create and implement good AI governance in your organization as well as adhering to regulations like the AI Act.

Then more specific to the AI Act, it's important to understand the risk category that your system falls into because not only can it fall into one but it can fall into more than one at the same time. This is something people often forget and a systems risk category hugely depends on things like the intended use of the system, the potential impact as well as other factors that need to to be considered. So what we do at Namco Digital, we have been helping our clients so far as well with this kind of process where we have often started off with giving more in-depth awareness of the AI Act, going a little bit more deep into the requirements and the obligations of this regulation followed by an in-house consultation on the AI system or the AI use case at hand of what we're dealing with and then moving on to a product questionnaire that we hand in to our customer in order to get more insights and explanations about the use case at hand that we would then use in order to make a proper risk specification against the EU AI Act criteria.

Then as deliverables, we have given out evaluation reports as well as recommendations, how did we reach the conclusions that you are a high-risk AI provider or a low-risk AI provider or deployer as well as an evaluation statement stating the results of the process. Now key interests of Namco Digital's service offerings, these can be summarized like this. So the key interests of our clients today, I've already slightly mentioned the AI Trustmark and ISO42000.

So in terms of AI Trustmark, there will be a webinar on this in April and same for ISO42000, there will be a more in-depth webinar on this topic. But basically what we help our clients with, we help them with getting ready for ISO certification, we help them with global market access and risk categorization like I already briefly explained in the previous slide. We also help with general AI governance assessment where we do an AI governance maturity scan.

This is quite valuable for clients that seek to identify gaps in their AI governance maturity and in a way so that they can mitigate any potential risks, but also become better and more mature at AI governance which naturally will also increase or enhance your level of compliance with certain regulations and allow you to ensure that you are implementing AI not just effectively but in a responsible manner. And then AI trainings and workshops. I've already mentioned that

we have an AI literacy program and we have an upcoming webinar on that.

So here are four of our 30-minute upcoming webinars. The AI literacy one is the first one. You will be having access to it on March 31st.

You can join it live. Then our AI governance assessment webinar will be held on April 22nd. The AI Trustmark webinar on April 11th and the ISO-IC 42001 readiness webinar will be held on May 7th.

Now last but not least, how you can learn more about our service offerings. Of course please feel free to browse our website and contact us if you want like a 50-minute consultation on anything or if you want to dive deeper on anything or on your use case. We're more than happy to set up any meetings with you.

We have a service brochure that you can find on the website on the AI Trust Hub and of course the LinkedIn community. Feel free to follow it in order to stay updated of any relevant regulations and news related to not just regulations but governance as well and our freely accessible AI Trust Hub where we maintain a database library of standards and regulations policies that are being drafted and published globally. That is all.

Here you have a QR code if you want to set up that 15-minute AI consultation where we can talk about any problems that you may be facing or any insights that could be valuable for your business. That is all. Thank you very much.

Here you have our email address as well as of course the URL for our website. Thank you very much and I hope you all have a great day.