bitkom

Position Paper

The User-Provider-Relationship under the proposed Artificial Intelligence Act
11.11.2022

Merle Uhl
Policy Officer for
Artificial Intelligence &
Digitalization

T+49 30 27576-242
m.uhl@bitkom.org

Albrechtstraße 10
10117 Berlin

General Remarks

Since the user-provider-relationship is not only crucial to a successful functioning of the AI Act but also subject to an ongoing discussion among the stakeholders involved in the legislative process, Bitkom holds the view that it is of importance to actively contribute to this discussion by the means of the following position paper in order to ensure that responsibilities are distributed in a practicable and fair manner.

We understand one of the main drivers of the debate around the user-provider-relationship to be a mismatch between requirements of the AI Act, especially in articles 8 to 15, and the capabilities of who is considered the provider and the user. Similar considerations are coming with the proposed inclusion of general purpose AI (GPAI) to be found in the latest compromise proposal of the Czech council Presidency on GPAI, already introduced by the earlier French Presidency. Therefore, this paper aims at highlighting the origins of the concerns and provides some principles that should be taken into account when discussing these articles.

Requirements of (GPAI) Providers

Central to this topic are the requirements of providers and the conditions under which a user becomes the provider of an AI system. While the obligations of providers are listed in Article 16, obligations that apply to users are formulated in Article 29. We assume that there is also the possibility that one stakeholder must fulfill all requirements, if Article 28 applies.

According to Article 28 in the Commission proposal a user is considered provider – and, thus, must fulfill the obligations of Article 16 which includes Articles 8 to 15 - if they.

a) place on the market or puts into service a high-risk AI system under their name or trademark;

b) modify the intended purpose of a high-risk AI system already placed on the market or put into service; or

c) make a substantial modification to the high-risk AI system.

According to the last proposal of the French council Presidency on GPAI, providers of systems that may fall under the risk categorisation of the AI Act need to comply with articles 9, 10, 11, 13(2) and 13(3)(a) to (e), 15, 16aa, 16e, 16f, 16g, 16i, 16j, 25, 48 and 61. These "shall apply irrespective of whether the general purpose AI system is placed on the market or put into service as a pre-trained model and whether further fine-tuning of the model is to be performed by the user of the general purpose AI system.". The Czech Council Presidency in their latest compromise from November 3rd left the exact provisions to be further detailed out by implementing acts.

Mismatch with Capabilities

For "normal" as well as GPAI providers, the proposals in our view still leave some inconsistencies with regards to whom has to fulfil certain requirements. In specific, we would like to point out the ambiguous transition from user to provider (Article 28) and want to provide an evaluation of some of the Articles in Chapter 2 with regards to the user-provider relationship and GPAI.

Transition from user to provider according to Article 28

The three modes of transitioning from being the user to being the provider that are laid out in Article 28 possibly come with varying involvement and technical access to the respective high-risk AI system. Especially under point (a), the then provider might only have limited capabilities to fulfil what is ask for within the process of claiming conformity within the AI Act. It should be possible to contractually deviate from that provision, as the fact that a high-risk AI system is under a company's name or trademark put on the market, does not necessarily enable it to show all that is asked for in articles 8 to 15. This becomes especially relevant in the case of white-label-solutions where the technical solution is only labeled with another company's name or trademark. There should be the possibility for the buyer of a white-label-solution to not become the provider of the high-risk AI system as she simply does not have the technical means to ensure the fulfillment of the requirements. Thus, it should be clarified what options there are to use white-label-solutions where the seller keeps the obligation to declare conformity.

Risk management requirements according to Article 9

We welcome very much the Commission's proposal to follow a risk-based approach in the regulation of AI. The notion of risk is thus central to the functioning of the approach. We acknowledge that GPAI as basis or building block for a lot of AI systems plays an important role but is not associated with a risk that arises from an application's specific context of use. Thus, implementing a risk management system for GPAI in our opinion does not help to contribute to a reduction of risk which we understand as the main purpose of this regulation. Assessing risk in a specific application makes it possible to mitigate it efficiently, while imagining all possible applications of a GPAI system comes with a high burden and – most importantly - no effective tackling of the risks that might arise in a concrete use case. We fully acknowledge that in order to make AI in the EU hold to the AI Acts standards it is necessary to collaborate within the value chain. We also think that there is room for improvement when it comes to detailing that out.

Data governance requirements according to Article 10

Since stakeholders who are considered providers under the AI Act might not have access to the relevant data sets an AI systems has been trained with, data governance obligations may be impossible for them to fulfill. Several possible scenarios raise questions regarding this requirement:

- If a user re-trains an AI system with her own data without modifying its intended purpose, the re-training would not be considered a substantial modification and the system is not put into service under the user's name or trademark (which means that the user would not be considered provider), how is the provider supposed to fulfil the data governance requirements according to Article 10 without having access to the user's data?
- What happens if a user becomes the provider of a high-risk AI system by putting it into service under their name or trademark but does not customize the model any further? In this case, under Article 28. 2, the initial provider must still comply with the provisions of the AI Act. Yet, the new provider also needs to comply with Article 10 only without or with incomplete information on the data sets. This is connected to the already explained uncertainties around Article 28.

Here we see the necessity to collaborate in order to be compliant with the AI Act for both sides. Users might need to support the provider of their AI system with information concerning data sets they used to fine-tune a model. Upstream and GPAI providers might need to enable their buyers to fulfill what is ask of them when models are delivered pre-trained.

Recommendation

Based on the considerations above, we want to highlight some principles that should be taken into account when discussing the relationships in the value chain under the AI Act.

Including GPAI into the scope of the AI Act deviates from the risk-based approach which we see critical. It does not serve the overall aim of efficient risk mitigation. Without a specific intended purpose, it is hard to determine the risk and reduce it. However, it is necessary that stakeholders in the value chain work together for tackling risk effectively. High-risk AI system providers will use GPAI for which they need support and information to be compliant with the AI Act. They can best identify the possible risks arising from the system in their specific application but require information which depending on the exact relationships in the value chain can only be supplied by other stakeholders.

Concerning the information that needs to be delivered by these stakeholders, it must be ensured that it serves the ultimate goal of enabling the provider to be compliant. It furthermore should not infringe on intellectual property rights, confidential business information, or trade secrets. Thus, collaboration on these principles should be enabled and will serve the purpose of mitigating risks that might come with certain AI systems.

Bitkom vertritt mehr als 2.000 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.