LEWIATAN

Warszawa, 17 października 2022 r.
KL/396/191/ET/2022

Pani
Anna Weber
Dyrektor Departamentu Tożsamości Cyfrowej
Kancelaria Prezesa Rady Ministrów

Szanowna Pani Dyrektor,

W związku z publikacją tekstu kompromisowego dotyczącego *projektu Rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze unii* (COM(2021) 206), Konfederacja Lewiatan przesyła uwagi do niniejszego tekstu.

Z poważaniem

Grzegorz Baczewski
Dyrektor Generalny Konfederacji Lewiatan

Załącznik: Stanowisko Konfederacji Lewiatan w sprawie *projektu Rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze unii*.

Remarks of the Polish Confederation Lewiatan on the compromise text of the Artificial Intelligence Act

We, Polish Confederation Lewiatan and our members observe with attention the work in the Parliament and Council of the EU's Artificial Intelligence Act, which it first-of-its-kind framework for artificial intelligence (AI) legislation globally. The businesses we represent have been supportive of the objectives of the AI Act, particularly the Commission's goal to establish a balanced and proportionate horizontal regulatory approach to Artificial Intelligence.

We welcome this opportunity to provide feedback to current draft of the Act.

1. Definition of AI systems

Presidency Compromise	Suggested amendment
Article 3.1	
„Artificial intelligence system" (AI system) means a system that is designed to operate with a certain level of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of ~~human-defined~~ objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts;	„Artificial intelligence system" (AI system) means a system that is designed to operate with a certain level of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve ~~a given set of~~ human-defined **intended-purpose** ~~objectives~~ using machine learning and/or logic and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts;

Justification

We welcome the Presidency's objective to fine-tune the definition of AI systems, but disagree with the idea that the reference to „human-defined" objectives is not essential for the purposes of this definition. Importantly, we believe that the definition should include a reference to „human-defined intended purpose" to ensure alignment with the overall Regulation. The concept of the intended purpose given to AI systems is an essential element of the AI Act, as this is the decisive criterion which helps establish the level of risk for an AI system in the context of the AI Act.

2. General purpose AI systems

a) General remarks

General-purpose AI systems are an important part of the AI ecosystem. These 'off the shelf' AI solutions [such as application programming interfaces (APIs) and open source systems (OSS)] **have democratized access to and use of AI technologies** for organizations of all sizes, nationalities, and across the various industries. These AI systems are the basis for a number of applications, capable of pursuing a wide variety of purposes.

General-purpose AI systems are purpose neutral: they are versatile by design, **and are not themselves high-risk** because these systems are not intended for any specific purpose. The term general-purpose does not refer to the idea that they can be used for any and all applications, but rather that downstream deployers can apply them in a variety of ways, with a wide range of potential benefits and risks. This is more than a nuance -- because the deployer will be the one identifying the purpose of such general systems, and the attendant benefits and risks.

We are concerned that adding general-purpose AI as a new class of AI systems in the scope of the AI Act – as suggested by some amendments in the Council and in the Parliament – would fundamentally affect the architecture of the entire bill, creating an imbalance in risk-based approach of the AI Act. **Assigning stringent obligations on the providers of these systems goes against the objective of pre-determining and clarifying the balance of responsibilities in the AI value chain.**

Requiring providers of general use AI systems to assume high-risk obligations under the AI Act, simply because deployers might potentially use them in a high risk setting, would end up capturing a broad swath of systems across a range of maturities that are not specifically intended for high-risk use cases. This would hamper collaboration and innovation of enterprises across Europe seeking to use these systems for their specific needs, many of which are not high-risk. This includes limiting the ability of downstream deployers to leverage general purpose translation apps, customer service bots, and even visual identification tools in contexts they can only fully understand. It would also effectively require providers of general-purpose AI systems to facilitate their use in high-risk applications. **In fact, this could create a compliance gap that could harm consumers if general purpose systems are deployed in a high risk manner not envisioned by the provider (and in some cases against the provider's terms of service), and the provider of a system is unaware of how a deployer is using the system due to EU privacy and security obligations.**

Specifically, requirements to monitor use of general purpose AI systems (including open source software) for potential high-risk use cases would conflict with GDPR privacy and security requirements. This could significantly impact the open-source community, a key driver of innovation and competitiveness in AI. Open-source software providers, including academics and SMEs, inherently have no way of monitoring how third parties use their software, and often lack resources and tools to engage in extensive compliance activities. This may force a difficult decision to simply not offer general purpose AI systems or open-source systems in Europe which would harm the innovation ecosystem.

Rather than impose obligations on all general-purpose systems, the AI Act should focus on systems intended to be available for use in high-risk applications, while protecting open-source software and general-purpose systems that are not intended for use in high-risk applications. Providers of general-purpose systems who choose to enable their use in high-risk applications are naturally incentivized to assist deployers of high-risk applications with all essential, relevant and reasonably expected information that is necessary for the new provider to comply with the obligations set out in this Regulation. This approach would be in line with the general approach in other EU legislation, such as in the European Copyright Directive, the Data Governance Act or the Digital Content Directive. It is notable that the EU legislator's justification for the exclusions - as expressed most clearly in Recital 32 to the latter - are the same ones that are applicable here, namely to "avoid imposing obstacles" to the beneficial contribution of open source software "to research and innovation".

Providers of general-purpose AI systems are often not best equipped to anticipate downstream uses of the technology, and these systems cannot be defined as having an intended purpose or risk profile per se. The deployers of these systems are best positioned to understand how they have chosen to deploy the system and their attendant risks, implement effective risk management strategies, conduct post-market monitoring or logging, which providers of general use systems are not equipped to do because they will not have visibility into how deployers are using these systems for security and privacy reasons. Ultimately, **deployers are best positioned to understand which controls and risk mitigations are most appropriate to their specific use case, and to implement them appropriately.**

This is not to say that providers of general-purpose AI systems that are deployed by third parties cannot play an important role in enabling compliance with the AIA. **Providers of general-purpose systems who choose to enable third parties to deploy them in high-risk applications should provide documentation and information about relevant compliance activities that enable deployers to comply with the Act.**

Against this backdrop, we would suggest to **clarify that when other actors in the value chain modify a general-purpose system in a way that makes it high-risk, they should assume the responsibilities of a provider, and that the developer of the general-purpose system is not a provider under the AIA.** The deployer that modifies the system for use in a high-risk application is best equipped to identify the risks associated with their specific use case, data, and application, implement effective risk controls, and ensure that general-purpose systems they deploy in high-risk applications are appropriate to their needs, including working with providers of general-purpose systems to ensure their high-risk applications are compliant.

b) Responsibilities of General Purpose AI providers that would be difficult or impossible to meet in practice and why

- **Employ appropriate data governance practices (Article 10):** While providers of AI systems often manage the data on which the system is initially trained, many systems ingest data from users as part of their operations, and whether and how that data is retained, used and deleted is often controlled by the deployer of a system. As an example, an entity that develops a system to analyze health records often will not have access to the health records of patients in a hospital that deploys the system, nor will they have any control of how the health system ingests, uses, retains or deletes that data in the course of operating the system. The deployer of the system, in this case the hospital, will be the one to control and process patient data, understand how that data is being used and how patient needs may evolve throughout the life of the product. Note that this challenge is reflected in the proposal already, with Article 29 assigning responsibilities for certain downstream data requirements to the user/deployer rather than the original provider.
- **Provide technical documentation and keep it up to date throughout the life of the system (Article 11):** Technical documentation will require information from the provider of AI systems regarding the training, development, and performance of the system, but information on how the system interacts with other systems used by the deployer, whether and how it is patched and updated, and how the system interacts with the deployer's real-world user data will need to be supplied by the deployer.
- **Provide transparency to users (Article 13):** The provider of an AI system deployed by a third party through a website or app often will not control the actual user interface through which users interact with the system. While documentation about the development, training, and performance of the system may be offered by the provider, the deployer of the system must be responsible for ensuring that relevant information, for example, about application-specific decision-making or opportunities for appeal, is appropriately surfaced to users.
- **Ensure appropriate human oversight of the system (Article 14):** In many, if not most, cases, appropriate human oversight of AI systems will require appropriate training, oversight, and accountability for users of the system. While providers can create mechanisms for incorporating human input and feedback and exercising oversight, ensuring that users are appropriately trained to use the system—and that oversight and accountability structures are in place to ensure the system is used as intended—will necessarily be determined by the deployer of the system.
- **Ensure that systems are used in such a way that they achieve appropriate levels of accuracy, robustness, and cybersecurity (Article 15):** Accuracy, robustness and security are highly dependent on choices made by deployers of AI systems, in addition to the developer of the AI system itself. As an example, deployers will generally determine access control for AI systems they use, conduct network monitoring and threat intelligence activities to identify potential cyber threats, and conduct user training on how to avoid security breaches.
- **Conduct post-market monitoring of the system's performance (Article 61) and correct for unfair bias:** Providers of AI systems often lack direct access to the system as deployed by their customers, meaning that they are unable to monitor system performance, identify indicators of bias, and take steps to correct them. In some cases, deployers may need to work with providers to correct for bias that arises

due to features of the system, but in other cases they may be more easily corrected by adjusting any additional data the system is trained on or how the system is used.

- **Put in place an appropriate risk management system (Article 9):** All of these elements are critical to establishing an effective risk management system for AI systems. While developers will need to take effective measures to manage risks associated with the design of the system, only deployers are in a position to evaluate whether mitigations put in place by developers are appropriate to their use case and organization.

c) Suggested amendments

- Definition of general-purpose AI

General purpose AI system means an AI system that is able to perform generally applicable functions for multiple potential purposes, such as image or speech recognition, audio or video generation, pattern detection, question answering, and translation, and that is largely customizable.

- [New] Definition of free and open source general-purpose AI

Free and open source AI system means a general-purpose AI system where the source code is openly shared by the developer or developers and can be freely accessed, used, modified and redistributed by any natural or legal person pursuant to a license agreement.

- Obligations for providers and deployers of high-risk general-purpose AI systems

General purpose AI systems shall not be considered as having an intended purpose within the meaning of this Regulation unless those systems have been adapted to a specific intended purpose that falls within the scope of this Regulation.

Any natural or legal person that adapts a general purpose AI system to a specific intended purpose and places it on the market or puts it into service shall be considered the provider and be subject to the obligations laid down in this Regulation.

The original provider of a general purpose AI system shall comply with Article 11 of this Regulation to the extent the elements of the technical documentation are relevant to general purpose applications, the initial provider was involved in or has control over these elements and is in possession of the relevant information . After placing it on the market or putting it to service, and without compromising its own intellectual property rights or trade secrets, the original provider should provide the new provider referred to in paragraph 2 with all essential, relevant and reasonably expected information that is necessary for the new provider to comply with the obligations set out in this Regulation.

Paragraph 3 shall not apply when the original provider has excluded any high-risk uses of the general-purpose AI system in the terms of service, policies, instructions of use, documentation, or other information accompanying the general purpose AI system or where the general purpose AI system subject to the adaptation referred to in paragraph 2 is a free and open source general-purpose AI system.

The original provider of a general purpose AI system shall only be responsible for compliance with the obligations in paragraph 4 towards the natural or legal person that adapts the general purpose AI application to a specific intended purpose.

d) Title IA

Presidency Compromise	Suggested amendment
Title IA	
Article 4a *Compliance of general purpose AI systems with this Regulation* Without prejudice to Articles 5 and 52 of this Regulation, general purpose AI systems shall only comply with the requirements and obligations set out in Article 4b. Such requirements and obligations 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. Article 4b *Requirements for general purpose AI systems and obligations for providers of such systems* 1. General purpose AI systems which may be used as high risk AI systems or as components of AI high risk AI systems in the meaning of Article 6, shall comply with the requirements established in Title III, Chapter 2 of this Regulation as from the date of application of the implementing acts adopted by the Commission in accordance with the examination procedure referred to	*Delete*

in Article 74(2) no later than 18 months after the entry into force of this Regulation. Those implementing acts shall specify and adapt the application of the requirements established in Title III, Chapter 2 to general purpose AI systems in the light of their characteristics, technical feasibility and of market and technological developments. ~~Articles, 9, 10, 11, 13(2) and 13(3)(a) to (c) and 13(3)(e) and 15 of this Regulation~~. When fulfilling those requirements, the generally acknowledged state of the art shall be taken into account, including as reflected in relevant harmonised standards or common specifications. 2. Providers of general purpose AI systems referred to in paragraph 1 shall comply with the obligations set out in Articles 16aa, 16e, 16f, 16g, 16i, 16j, 25, 48 and 61. 3. For the purpose of complying with the obligations set out in Article 16e, providers shall follow the conformity assessment procedure based on internal control set out in Annex VI, points 3 and 4. 4. Providers of such systems shall also keep the technical documentation referred to in Article 11 at the disposal of the national competent authorities for a period ending ten years after the general purpose AI system is placed on the Union market or put into service in the Union. 5. Providers of general purpose AI systems shall cooperate with and provide the necessary information to other providers intending to put into service or place such systems on the Union market as high-risk AI systems or as components of high-risk AI systems, with a view to enabling the latter to comply with	*Delete*

their obligations under this Regulation. Such cooperation between providers shall preserve, as appropriate, intellectual property rights, and confidential business information or trade secrets in accordance with Article 70. In order to ensure uniform conditions for the implementation of this Regulation as regards the information to be shared by the providers of general purpose AI systems, the Commission may adopt implementing acts in accordance with the examination procedure referred to in Article 74(2). 6. In complying with the requirements and obligations referred to in paragraphs 1, 2 and 3: – any reference to the intended purpose shall be understood as referring to possible use of the general purpose AI systems as high risk AI systems or as components of AI high risk systems in the meaning of Article 6; – any reference to the requirements for high-risk AI systems in Chapter II, Title III shall be understood as referring only to the requirements set out in the present Article. Article 4c *Exceptions to Article 4b* Article 4b shall not apply when the provider has explicitly excluded any all high- risk uses in the instructions of use or information accompanying the general purpose AI system. Such exclusion shall be made in good faith and shall not be deemed justified if the provider has	

sufficient reasons to consider that the system may be misused. When the provider detects or is informed about ~~statistically significant trends of~~ market misuse they shall take all necessary and proportionate measures to prevent such further misuse, in particular taking into account the scale of the misuse and the seriousness of the associated risks.	

Justification

This proposal on General Purpose AI (GPAI) is extremely concerning for several reasons. First, it strongly deviates from the AI Act's risk-based approach in the sense that it would classify all GPAI as high-risk as it would treat GPAI that may be used for high risk uses like a high-risk AI system. Second, it would impose several requirements on providers of GPAI which are impossible to comply with when the provider does not have insight into whether the GPAI is put to high risk uses by the user. In most cases, GPAI providers are not aware and do not control the intended purpose of an AI system, which is decided by the user of GPAI. In particular, the obligations set out in Articles 16e, 16g, 16i, 16j, 48 would be extremely difficult for providers of GPAI to comply without knowing what the intended purpose of the AI system is. Obligations set out in Article 61 would equally be difficult to comply with since measures to mitigate the risks that the AI Act is trying to address would not take place at the tooling level, but rather in the model development and training phases which are controlled by the user. While GPAI tooling providers have a fundamental responsibility to develop tools that are trustworthy and secure, placing the same obligations on GPAI tooling providers as those that apply to providers of high-risk AI systems does not make sense, is unnecessarily burdensome and does not further the objectives of the Act.

We believe that there is no need for the AI Act to have a specific section on GPAI. The original text of the Commission should stand in order to maintain the risk-based approach: AI systems which are put to high-risk use are already covered by the provisions of the AI Act, and any system or tool which is not high-risk is not covered and should not be regulated like high-risk systems. In line with the Commission's draft proposal, GPAI providers have a commercial interest in cooperating with users to help them comply with the requirements and obligations of the AI Act, as already included in Recital 60.

Since so many elements regarding compliance with the obligations and requirements of the AI Act depend on the intended purpose given to an AI system as well as on what happens at the later stages of building an AI system, which involves providers and third parties other than the GPAI provider, the best option is to fine-tune the allocation of responsibilities and clarify that the entity which decides over the intended purpose of an AI system or gives an intended purpose to GPAI becomes the provider. Importantly, the text should mention that this allocation can be modified through contracts.

3. Definition of high risk

Presidency Compromise	Suggested amendment
Article 6	
3. AI systems referred to in Annex III shall be considered high-risk ~~**in any of the following cases**~~: ~~**(a) the output of the system is immediately effective with respect to the intended purpose of the system without the need for a human to validate it;**~~ (b) the output of the system ~~**consists of information that constitutes the sole basis or**~~ is not purely accessory in respect of the relevant action or decision to be taken by the human, and may therefore lead to a significant risk to the health, safety or fundamental rights. In order to ensure uniform conditions for the implementation of this Regulation, the Commission shall, no later than one year after the entry into force of this Regulation, adopt implementing acts to specify further the purely accessory nature of the information across the relevant high-risk AI systems referred to in Annex III. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74, paragraph 2.	3. AI systems referred to in Annex III shall be considered high-risk **in any of the following cases:** **(a) the output of the system is immediately effective with respect to the intended purpose of the system without the need for a human to validate it;** b) the output of the system consists of information that constitutes the sole basis or ~~**is not purely accessory in respect of**~~ **significantly determines** the relevant action or decision to be taken by the human, and may therefore lead to a significant risk to the health, safety or fundamental rights. In order to ensure uniform conditions for the implementation of this Regulation, the Commission shall, no later than one year after the entry into force of this Regulation, adopt implementing acts to specify further ~~**the purely accessory nature of**~~ **how** the information across the relevant high-risk AI systems referred to in Annex III **is considered significantly determinant**. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74, paragraph 2.

Justification

We welcome the Presidency's overall aim to clarify the scenarios in which AI systems designated in Annex III are viewed as being high-risk and subject to additional compliance obligations. As the Czech Presidency noted, it is indeed critical to assess "the significance of the output of the AI system in relation to the decision or action taken by a human". However, unless further clarified, the current wording of Art. 6(3) may have the same effect as the original draft: any AI system within the categories listed in Annex III that has any impact on human decision-making may be viewed as an inherently high-risk AI system.

KL/396/191/ET/2022