LEWIATAN

Warszawa, 2 listopada 2023 r.
KL/414/193/ET/2023

Pani
Inez Okulska
Dyrektorka Departamentu Innowacji i Technologii
Ministerstwo Cyfryzacji

Szanowna Pani Dyrektor,

w związku z trwającymi pracami nad projektem Rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze unii, Konfederacja Lewiatan przesyła uwagi do niniejszego tekstu.

Z poważaniem

Maciej Witucki
Prezydent 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.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

LEWIATAN

Remarks of the Polish Confederation Lewiatan on the Artificial Intelligence Act - trilogues

1. Classification of AI systems

Welcome the intention to combine the positions of the Council and Parliament to filter out low-risk use cases and beneficial use cases that would be captured in the very broad high-risk categories in Annex III. Welcome Parliament's proposal to focus on use cases that pose a significant risk of harm. The Commission's proposal is a step in the right direction, but there are several shortcomings and a lack of legal clarity in the proposal.

Starting point: The high-risk categories in Annex III are very broad and cover many low-risk use cases. If detailed documentation requirements are required for all use cases that could fall under Annex III, even low-risk use case providers would be burdened with significant compliance obligations.

- **Ask:** Use cases should not be classified as high-risk by default, but only if the specific application is used in a risky manner.

Condition "harm": While the general definition of high-risk in Art. 6(2) refers to "harm" the conditions that are crucial to assess the risk level entirely miss this dimension and remain very technical. This risks to pull use cases that are ultimately not causing harm into the high-risk regulation.

- **ASK:** Support the addition of a condition that excludes AI systems that do not pose a significant risk to the health, safety or fundamental rights of natural persons."

Condition "preparatory task": A clearer distinction between core and peripheral function is required for legal certainty.

- **ASK:** Clarify that an AI system is intended to perform a preparatory task to an assessment relevant for the purpose of the use case listed in Annex III, and the preparatory task represents the core function of the AI system.

Profiling: Considering any AI that includes "profiling" as defined in the GDPR as high risk is too broad and misleading. Recommender systems such as proposing or playing specific music based on previous user requests would fall under high-risk. Also, AI used for verification – which is explicitly excluded from the high-risk biometric identification category – would be in scope.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

- **ASK:** Refrain from adding any "profiling" under high-risk by either rejecting this addition or specifying the actual problem, based on a narrow and clear definition.

Procedure: Providers are required to document the assessment of individual use cases. Depending on the final text, this could include numerous low-risk use cases as well as high-risk use cases. Many of these documentations will include sensitive business data that require confidentiality safeguards if being shared with third parties.

- **ASK:** Providers should be required to share this data with authorities only upon reasoned request and reasonable belief that a system has been incorrectly classified as low risk.

2. List of high-risk AI use cases

Biometric identification (BID): BID that requires interaction with the user is no mass surveillance. Verification systems are often used by more than just one but several individuals (i.e., several family members using a voice assistant that provides personalized features, i.e., "play my favorite music"). The Parliament's proposal to expand the category to "inferences" to "biometric-based data" would significantly expand this category to a broad range of use cases that may indirectly link to biometric data, including non-personal data. This vague reference also undermines legal certainty.

- **ASK:** Support the Presidency's proposals to (a) only consider BID that is applied in a "remote" way as high-risk, (b) not exclude "one-to-many" verification from the exemption, (c) not include biometric-based data. Additionally, the inclusion of "inferences" should be rejected.

AI in the Workplace: The vast majority of AI in the workplace does not cause harm, on the contrary it enhances safety and drives efficiency. For the most part, AI used for "monitoring and evaluating of performance and behavior" focuses not on individuals but on general workplace processes that are not based on personal-data. While task allocation that is not based on personal traits is explicitly excluded, the text on evaluating and monitoring of performance remains unclear.

- **ASK:** Clarify in the recitals that AI which is not based on personal traits is excluded.

3. Prohibitions:

Inferring of Emotions: Parliament's proposed ban is very broad and is not supported by evidence or risk analysis. It would prohibit many risk-free and extremely useful use cases. Do not support the inclusion of the proposal. If policymakers seek a compromise, at least positive workplace use cases that are not about profiling but are increasing security and

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.
NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

improving employee or customer satisfaction should be excluded (i.e., coaching tools that are under control of the employee; recognition of sentiments to identify and resolve negative experiences). The definition of emotion recognition is not sufficiently clear and may even include non-personal data.

- **ASK:** Support but broaden the Presidency's proposal to exempt AI used for safety reasons, to include other positive use cases like coaching and efficiency gains. Additionally, positive use cases that increase employee or customer satisfaction must be excluded. The definition of emotion recognition needs to be clear and exclude biometric-based data.

Real-time and post remote Biometric Identification (BID): The Parliament's proposed blanket ban on BID in public spaces risks to outlaw private entities' beneficial use cases that are not about mass surveillance. The considered compromises do not clarify whether private entities would be included and whether the exemption of BID used for verification would be limited to systems that allow one-to-one verification.

- **ASK:** Limit a prohibition to public entities and clarify that the exemption is not limited to "one-to-many" verification, in line with the definition for BID as high-risk.

Categorization of persons: AI should not be used for harmful classification of natural persons. The proposed additional category from the Parliament is defined extremely broadly and is not limited to AI that uses "sensitive" data as defined in the GDPR: It includes any AI-based categorization of people based on the "inference" of such data. Positive use cases that benefit users – such as enhancing accessibility or identifying biased data sets – could be prohibited.

- **ASK:** Reject the Parliament proposal. The Presidency's proposal to alternatively categories these use cases as high-risk is not appropriate in cases where they do not impose actual risks.

4. Asymmetric approach for regulating foundation models and general-purpose AI (GPAI).

As Polish Confederation Lewiatan we want to express our concerns with recent developments on fundamental building blocks of the AI Act. Since the publication of the AI Act by the European Commission, industry has consistently supported a risk-based approach to AI regulation. We support the AI Act's overarching objectives of promoting trust and innovation in AI, and our members are all committed to the safe and responsible development, deployment and use of AI.

LEWIATAN

We believe that co-legislators should avoid undermining this proportionate and evidence-based approach by forcing an expansive asymmetric approach to regulate Foundation Models and General Purpose AI.

The Policymakers involved in these final decisions must take key factors into account:

- The approach of focusing on the risk of use cases is already acknowledged as a more future-proof way of providing protections for EU citizens and should be maintained.

- Market interoperability is crucial. International and national commitments, the White House Voluntary AI Commitments, as well as regulatory approaches of other nations and trading blocs are also moving at pace. Unjustified asymmetry is not proportionate and not backed by compelling evidence. Discriminating against certain providers can never lead to an internationally aligned approach and will, again, harm European innovation in AI.

- We are concerned about the direction of the various proposals to regulate GPAIs and/or AI Foundation models which include diverging and unclear scopes and definitions. These proposals do not take into account the complexity of the AI value chain and are not consistent with the AI Act's technology neutral approach, which regulates the use of AI systems according to actual risk, not the types of technology being used.

- It is still very early days for AI technology, and rapid developments are yet to come. The market is already fundamentally different than one year ago with many new players and great leaps in what AI can do. Any asymmetric regulation is likely to become outdated within a few years, if not months.

- Creating a "glass ceiling" through arbitrary size criteria, such as the amount of compute used for Foundation Model training or the number of users of General Purpose AI, would hold back European innovators from scaling up. It would also distort innovative practices and create disincentives, where companies would have to consider if and how they take on the additional asymmetric requirements and restrictions.

- There are clear examples that smaller models, and models from smaller companies, can have the same or higher impact as larger models and companies. It all depends on how they are used, not necessarily by whom. There is simply no evidence of any correlation between these risks and the size of providers.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

- Current discussions around requirements for general-purpose AI systems (GPAIs) and foundation models focus on diligence and safeguards, but they are not linked to limited liability considerations in line with the nature of those systems. AI providers should not be held responsible for the use of AI systems/models by downstream users, as this is technically impossible to control and mitigate.

- The General Product Safety Regulation has rightly avoided attempts to adopt such competition-motivated ideas of asymmetry. Appropriate safety requirements should apply to all to avoid fragmented safeguards that undermine users' trust. A small company can cause huge damage, while larger companies have built-in incentives to be as careful as possible.

- There is already an extensive and robust EU legal framework ensuring IP protection and enforcement, so there is no need for copyright related provisions to be included in the AI Act.

- Learning from the Digital Services Act (DSA), there is now a realisation by several EU Member States that risky services – which they had wanted covered by the asymmetric regime – have fallen outside the circle drawn for the DSA. That line in the DSA was debated for 18 months and is not perfect. Trying to draw such a line in the mere weeks left to conclude the AI Act is rolling the dice with Europe's competitiveness and safety.

KL/414/193/ET/2023