Warsaw, 10th February 2022

Axel Voss
Member of the European Parliament
Parlement européen
Bât. ALTIERO SPINELLI
15E146
60, rue Wiertz / Wiertzstraat 60
B-1047 Bruxelles/Brussel

The Position of the Digital Poland Association for

a *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS*

Dear Sir,

On behalf of the Digital Poland Association, the industry organization of employers, which brings together the largest companies from the RTV and IT industry operating in Poland, including manufacturers, importers and distributors of electrical and electronic equipment, I would like to submit our position on the above act.

First of all, we welcomes the Commission's AI Act proposal as it largely reflects the views Digital Poland Association has advocated for over the last few years. Especially when we think about using AI in the context of 5G technology. 5G is not only a new connectivity solution for consumers and enterprise segments but the enabler of a whole new way of creating value within a digital economy. This technology does not come only with the necessary network deployment, but with all the potential released by the power of Internet of Things (IoT), Artificial Intelligence (AI), Data management and Data-driven Networks and cloud-based solutions. Our member companies relies on the use of AI and the insights and

decision-making processes supported by data. AI is for example used to increase network performance and enable network automation.

To realize the full potential of AI, trust needs to be established in the development, deployment and use of AI. This is critically why we builds human trust in AI, addressing aspects spanning from explainability and human oversight to security, and built-in safety mechanisms. Trustworthiness is a prerequisite for AI and we are building it into the system by design.

Our position focuses on specific areas for additional clarification and ensuring that requirements will be feasible and effectively manage risk:

- Reflect the complexity of the AI ecosystem in the balance of obligations for different stakeholders. It will seldom be feasible or effective for providers of general-use AI systems to manage all of the risks associated with potential application in high-risk systems, as is currently envisaged in the AIA. For example, the provider will often not have access to the operational data necessary for post-market monitoring if the AI system has been put into operation by another entity. To address this, we recommend a new class of "deployers" be added to the AIA with responsibility for complying with regulatory requirements associated with deploying general-use AI systems in high-risk applications.
- Hold providers, deployers and users to feasible standards. As currently phrased, certain requirements of the regulation will be extremely difficult or impossible to meet in practice (e.g., the Art 10(3) requirement that datasets be "free of errors and complete" demands a level of perfection that is not technically feasible). We do not disagree with the spirit of the requirements, but they should be composed in a fashion that reflects feasible, best practice standards.
- Clarify certain provisions to provide legal certainty around scope and protect privacy. The AIA includes a number of terms and provisions that would benefit from further clarification to ensure that providers of AI systems understand how the scope and requirements of the AIA apply to their products. For example, the definitions of "safety components" and "significant changes" could be further clarified to provide legal certainty around when systems come in scope of requirements for high-risk AI systems.

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

- Innovation and trustworthiness must be seen as the two sides of one coin, when it comes to the use of AI. A proper balance should therefore be struck to this end throughout the proposal, without compromising safety and fundamental rights.

- Data and information gathering is often costly, cumbersome and involve many steps in the supply change. It is therefore important to ensure that the required obligations are relevant and possible to fulfill. For example, there are no guarantees for totally flawless data, in terms of high-quality data and the training, validation and testing of data (Articles 10 and 15; recital 44).

The proposed definition of artificial intelligence system (AI system), Article 3 (1) and Annex I

- The definition of 'AI system' is broad, especially when taking into account the techniques and approaches listed in Annex I. Some of these are rather basic algorithms and techniques not posing any major concerns around safety, reliability or fundamental rights. Some of the techniques and approaches listed in Annex I are traditionally also used in non-AI systems. The techniques in Annex I should therefore be used with some caution when standing alone.
- One way of mitigating these rather wide effects would be for the definition of AI system to only refer to those AI algorithms and techniques that, either as standalone or combined, may pose a potentially high risk to safety or fundamental rights due to their evolving nature or other aspects of their functioning.

The proposed definitions in Article 3 and more specifically on the division of responsibilities between 'providers' in Article 3 (2), and 'users' as defined in Article 3 (4)

- As a general point, the proposed definitions need to be consistent with the NLF definitions and not introduce any new key concepts, which could cause uncertainty as to the future interpretation of the two co-existing legal frameworks.
- Following the principles of the NLF, AI system providers will carry most obligations and requirements set in the AI Act. Many obligations and some of the requirements can in practice, though, only be managed by the entity in control of the AI system and its deployment in practice, which means the user. For example, a provider cannot

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

reasonably foresee all potential effects of the system and what data will be used to (re-)train and feed the AI system.

- The issue of allocating responsibility between providers and users (Chapters 2 and 3) needs to be seen against this backdrop, with a view to striving for a proper balance in order to reflect the complexity of AI systems and their value chain. A principle of balancing of responsibilities/ obligations has to be taken into account.

Amendments to Annex I, Article 4

While fully understanding the need and the challenge to accommodate technical progress by way of creating a sufficiently flexible legislative framework, the definition of AI system forms part of the essential provisions of the proposed Regulation. According to the Treaty, delegated acts may only relate to supplementing or amending 'non-essential' provisions in EU basic acts (Article 290(1) TFEU). Any adjustments to the legal definition that may become necessary after the Regulation enters into force should therefore only be made by way of an ordinary legislative procedure, with the full inclusion and consultation of stakeholders in the legislative process. Possible changes also need to meet fact-based criteria and be preceded by a thorough impact assessment.

The concept of 'high-risk' AI systems in Article 6, Annex II and III

- In addition to adapting to existing product safety legislation, the proposed Regulation also sets its own category of high-risk use cases.
- The risk-based approach should focus on whether the intended use of AI in the sector involves a significant risk to safety or fundamental rights, rather than the entire sectors. This is crucial in order to ensure that provisions are properly targeted.
- AI systems, used in electronic communications networks and equipment, including mobile networks and 5G, should not be classified as high-risk AI systems (Annex III, section 2). Equipment building up the communications networks is already sufficiently governed by NLF based legal instruments encompassing relevant safety aspects. This reasoning being fully in line with the abovementioned notion of limiting the scope to focusing on and targeting clear risks to the physical or psychological health of humans or EU fundamental values. For more detailed key points on the concept of 'critical

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

infrastructure' and the possible inclusion therein of 'digital infrastructure', see the Annex (Chapter 4) to this Paper.

- Individual components in the digital infrastructure are already covered by e.g Annex II and GDPR. The current draft regulation would merit from some further clarity around the differences between Annex II and III, in particular if Annex III is to include 'digital infrastructure', as suggested in the Presidency compromise proposal.

Conformity assessment, Chapter 2 and Article 43 (3)

- It should be ensured that the proposed classification under Article 6 does not lead to the promotion of mandatory third-party conformity assessment in for instance the field of radio equipment, where it is not called for, Article 43 (3).
- As currently drafted, high-risk AI systems are expected to undergo a new conformity assessment procedure whenever they are substantially modified, Art. 43 (4). Substantial modifications should, in our view, be assessed in light of the essential requirements, and it must be up to the manufacturer to assess if a modification is deemed to be 'substantial' or not.

What's more the proposed AI Act builds on the New Legislative Framework, NLF, which is the basis for product compliance obligations in the EU. Alignment of the proposed regulation with the NLF (in for example the Radio Equipment Directive and the Machinery Directive) is of particular importance. For most of the NLF legislation, this means amongst other things ensuring that any new requirements stemming from the proposed regulation can be integrated into the entire already existing chain of harmonized standards, conformity assessments, declarations of conformity and market surveillance. The integration of AI as a component of a product must not be seen as changing the overarching obligations related to product safety in the specific case of for example radio equipment. The well-established core principles, definitions, and procedures in the NLF should be the starting point and form the basis for any development of harmonized standards, laying down detailed technical requirements aiming to fulfill the essential requirements in the proposed AI regulation. Accordingly, we do not advocate technical specifications in implementing acts developed outside ordinary NLF procedures.

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

ANNEX

The concept of ‘digital infrastructure’ as part of ‘critical infrastructure’ in the context of the AI Act.

AI in products (mobile networks etc)

- Mobile networks and other digital infrastructure are critical and provide services that European citizens and business rely on. We do not contest the overall importance of such infrastructure.
- AI technology is used to ensure optimization and to deliver the best quality of service to consumers and business, given the often limited resources available, in e.g. network management, control, sustainability, slicing, predicting outages etc.
- The AI consists very often of a simple algorithm and decision trees. The reason for that is because the AI is used to manage machines instead of people.
- AI in communication networks do not have any direct human health, human safety or fundamental rights element precisely because they have no direct contact with or impact on human beings. Specifically, there are no commonly known use cases where AI in communication networks etc. has any direct impact on the safety and health of humans.

Safety first and by design

- All products, covered by the term ‘digital infrastructure’, which are placed on the market or put into service in the EU, are regulated by and in compliance with relevant EU safety legislation (Radio Equipment Directive, RED, and the Low Voltage Directive, LVD).
- AI is basically another piece of software. What differentiates it from the traditional programming is the fact that it is driven by data, thus it is not deterministic. This is why it is very important for us to introduce the correct network safety mechanisms, when using this software in critical environments (like live networks).

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

- A safe design of AI system would include, for example, a network safety fallback mechanism that the machine-learning system will use in case of undesired behavior. This practically means that whenever the AI algorithm is unsure of the action it deploys, it uses some hard-coded rules on how to behave. That will not be the optimal behavior, but it guarantees that it is a safe one.
- Another example, is using simulated and emulated environments to test potentially unsafe actions of the system before putting it to use in the network. In this way, a potentially unsafe action in a digital representation of the network is put to a test beforehand, rather than testing the actual network and according to the results deploy it, or not, to the live network.
- In short, the AI in new applications - compared to old, plain software - cannot jeopardize the overall functioning of the networks. The failure or malfunctioning of these AI systems will not put at risk the life and health of persons at large scale. Nor will it lead to appreciable disruptions in the ordinary conduct of social and economic activities.

Recommendation to remove the reference to 'Digital infrastructure' in Annex III and go back to the original wording of the Commission

We would propose to remove the reference to 'Digital Infrastructure' in Annex III, in the Presidency's compromise proposal.

- The removal of the reference to 'Digital infrastructure' is consistent with keeping all security of ICT products and services within the scope of the Directive on security of network and information systems, currently being revised (NIS2). The proposed inclusion is also inconsistent with the spirit of NIS2, which repealed the cyber security provisions from the European Electronic Communications Code, bringing them under the one legislative act. This new inclusion in the AI Act would threaten this approach.
- The overall purpose of the proposed AI Act is about safety and fundamental rights, and not about resilience of networks. Definitions from the proposed CER directive are accordingly based on a different purpose, thus not targeting the twin objective of promoting the uptake of AI and of giving people and other users the confidence to embrace AI-based solutions.

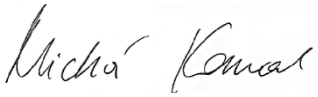
www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

- The proposed CER directive targets service providers and operations and do not include any product requirements, whereas the proposed AI Act is based on the EU product safety legislation.

Bearing in mind all the above arguments and comments, we hope that our position will be positively received and will be taken into account during the work on the final shape of this regulation.

We remain at your disposal in case of any questions and during the further processing of the document.

Sincerely yours,
Michał Kanownik



President of
Digital Poland Association