POSITION PAPER OF TEKOM EUROPE ON THE EUROPEAN ARTIFICIAL INTELLIGENCE (AI) ACT

Stuttgart, 2024-03-11

Ref.: 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 2021/0106(COD) DRAFT (Final draft as updated on 21-01-2024) with draft agreements of the trilogue negotiations

The European Association for Technical Communication – tekom Europe strongly supports the adoption of the proposed AI Act by the Members of the European Parliament and the Council.

However, for the sake of transparency, ethics, human rights, justice and good practice, several clarifications regarding information for use of trustworthy AI systems and about the proper application of this act should be made soon after the adoption of the AI Act.

tekom Europe advocates the right of users of technologies of any kind to use them efficiently, effectively, sustainably, and safely. To support these goals, we promote standards and guidelines for providers, operators and developers to create appropriate instructions for use and technical documentation.

In the attached position paper, we make clear where we see a strong need for improvements and clarifications regarding the documentation of AI and instructions for use for AI.

SUMMARY

In the European Union, there is a need for the development and use of competitive, sustainable, and trustworthy artificial intelligence. This requires innovation support but also regulations in terms of product risk and safety, ethics, human rights, and justice. As part of this regulation, the EU's Artificial Intelligence Act (AI Act) requires AI to be *transparent*. This transparency requires and impacts information for use and technical documentation.

In several parts of the draft AI Act, it is mentioned that additional clarifications regarding technical documentation and help for developers and users are needed. Delegated acts, guidance documents to be issued by the Commission and standardization are explicitly mentioned.

At least the following issues should be dealt with in this context:

1. Quality standards for technical documentation and instructions regarding the use of generative AI (GenAI)
2. Minimum requirements on how technical documentation and instructions for use shall be created for AI in general
3. Requirements for the technical documentation and instructions for use of in-house, non-commercial AI
4. References to EN IEC IEEE 82079-1 as the international standard for information for use
5. More details of the simplified technical documentation form introduced in the proposal (with the draft agreements of the trilogues), including what is in it and who will create it

1. INTRODUCTION

In 2021, after several rounds of public and expert consultation, the EU proposed an AI Act for regulating AI. In 2023, MEPs voted to follow the European Parliament's (EP) position on AI, allowing the EC AI Act proposal to proceed to the trilogue stage. We are on the home strait, but the adoption of consensus negotiated in the trilogue by EP and the Council is still pending. If the AI Act is adopted and enters into force, it must be applied after 2 years.

The consensus in the trilogue included important changes. The consensus adopts the OECD's definition of AI.[1] It also requires more restrictive regulations, especially around implementations of specific AI, such as predictive policing, biometric surveillance, and emotion recognition. In addition, the amendments include an increased emphasis on transparency, a new list of prohibited types of AI, and greater protection of fundamental rights, health, safety, the environment, democracy, and law.

Changes also include new transparency and risk-management rules around general-purpose AI (GPAI), e.g. GenAI such as ChatGPT. This kind of AI is not explicitly considered in the EC AI Act proposal but is the most common current public understanding of AI. These new transparency requirements include the need for such AIs to disclose they are AI, to prevent their use for generating illegal data, and for their creators to publish summaries of copyrighted material used for AI training.[2]

TECHNICAL COMMUNICATION[3] IN THE AI ACT

As indicated by the dramatic acceptance of AI in 2023, AI is predicted to significantly transform most industries, streamlining processes, replacing jobs, creating new kinds of jobs, and augmenting existing roles.[4] It is also expected to impact society as a whole, for example, impacting the trustworthiness of online communication, with all that implies for social cohesion, justice, and democracy.

We understand that part of the AI Act is an attempt, through regulation, to enable, clarify, and manage this impact, ensuring its contribution to the greater flourishing of EU society and economy through safe, just, and fair implementation and integration. Through this, the Act conceives of AI regulation as a form of product safety and risk regulation.

GenAI is predicted to replace parts of most authoring jobs in industry, such as marketing, policy-writing, report-writing, instructional design, and technical communication. Yet, based on the latest available proposal, the Act remains insufficiently detailed on the way this ability of GenAI can impact authoring tasks relevant to the Act's requirements, that is, creating technical documentation itself. Furthermore, the Act's details on instructions for use remain too sparse for how GenAI can be used.

---

[1] OECD: "An AI system is a machine-based system that is capable of influencing the environment by producing an output (predictions, recommendations or decisions) for a given set of objectives. It uses machine and/or human-based data and inputs to (i) perceive real and/or virtual environments; (ii) abstract these perceptions into models through analysis in an automated manner (e.g., with machine learning), or manually; and (iii) use model inference to formulate options for outcomes. AI systems are designed to operate with varying levels of autonomy."

[2] https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence

[3] Technical communication is the process of defining, creating and delivering information products of information for use – for the safe, efficient, effective and sustainable use of products (goods, technical systems, software, services).

[4] Stevenson, B. Oct 2023. "AI Will Change Your Job. Can You Change Along With It?" *Bloomberg*. https://www.bloomberg.com/opinion/articles/2023-10-01/writers-strike-is-over-but-the-ai-jobs-debate-is-just-beginning, retrieved October 11, 2023.

To enable stakeholders to engage with an AI product, the AI Act does go into significant detail about required technical communication for AI. Technical communication is the process of defining, creating and delivering information products of information for use – for the safe, efficient, effective and sustainable use of products (goods, technical systems, software, services). The AI Act refers to two kinds of content relevant to technical communication: technical documentation and instructions for use (the latter frequently discussed under transparency). It also classifies AI into different kinds – *prohibited* (Article 5), *high-risk* (Article 6), and *low or minimal risk* (explanatory memorandum, 5.2.2).

Each kind has different technical communication demands, with most of the content focused on high-risk AI. For separate, obvious reasons, prohibited, low, and minimal-risk AI do not require extensive technical documentation or instructions for use; for example, prohibited AI cannot even be developed or sold in the EU, so technical documentation or instructions for use for this AI is irrelevant.

OWN ARTICLE AND ANNEX TO TECHNICAL DOCUMENTATION

In several places, the AI Act (based on the consensus reached in the trilogue) requires specific actions to be taken around technical communication, especially in Article 11 and Annex IV. Relevant to this paper, Article 52c provides details of technical documentation for GPAI.

According to Article 3 Definitions (15), "'instructions for use' means the information provided by the provider to inform the user of in particular an AI system's intended purpose and proper use." Technical documentation is not defined in Article 3, but Article 11 and Annex IV deal with it.

Article 11 "Technical documentation"

Article 11, entitled "Technical documentation", describes what kind of AI requires technical documentation and how the technical documentation should be drawn up.

11(1) sets out different requirements depending on the organization: complete technical documentation for larger organizations and simplified technical documentation for small and medium-sized enterprises (SMEs), including start-ups. The simplified technical documentation shall be provided through a form established by the EC. Where an SME, including start-ups, opts to provide the information required in Annex IV in a simplified manner, it shall use the form referred to in this paragraph. Notified bodies shall accept the form for the purpose of conformity assessment.

It then refers to Annex IV for more information (also entitled "TECHNICAL DOCUMENTATION").

Annex IV "TECHNICAL DOCUMENTATION"

The most explicit reference to technical documentation is Annex IV, which is wholly about what must be documented. The following are the points most relevant for the tekom Europe position paper, as numbered in Annex IV:

1. A general description of the AI system including its intended purpose, how the AI system interacts or can be used to interact with hardware or software including other AI systems that are not part of the AI system itself, instructions of use for the deployer and a basic description of the user-interface provided to the deployer, where applicable;
2. A detailed description of the elements of the AI system and of the process for its development, including assessment of the human oversight measures needed in accordance with Article 14;
3. Detailed information about the monitoring, functioning and control of the AI system, in particular with regard to its capabilities and limitations in performance, and human oversight measures needed in accordance with Article 14;
4. A detailed description of the risk management system in accordance with Article 9;

5. A description of relevant changes made by the provider to the system through its lifecycle;
[…]
8. A detailed description of the system in place to evaluate the AI system performance in the post-market phase in accordance with Article 61, including the post-market monitoring plan referred to in Article 61(3).

Article 52c "Obligations for providers of general purpose AI models"

Most relevant to GenAI, the focus of this paper, Article 52c, describes the obligations of GPAI providers in terms of technical documentation. 52c(1a) specifies the technical documentation for GPAI (and thus, GenAI):

1. Providers of general-purpose AI models shall:

(a) draw up and keep up to date the technical documentation of the model, including its training and testing process and the results of its evaluation, which shall contain, at a minimum, the elements set out in Annex IV for the purpose of providing it, upon request, to the AI Office and the national competent authorities

Transparency through technical communication

Another important part of the AI Act regarding technical communication's impact on regulated AI is *transparency.* Transparency (which includes traceability, explainability, and communication) is one of the seven key attributes of *trustworthy AI* – AI that is ethical, robust, and legal. It does not necessarily require anything to have technical documentation or instructions for use. It can also arise from AI design, such as what kind of messages the AI communicates about itself when interacting with the user.

However, in many cases, communication by the AI about itself is not enough for AI to be sufficiently transparent. An AI can be too complex to sufficiently communicate its behavior or use. This is particularly the case with foundational, general-purpose AI (GPAI) like GenAI, where the specification of the technology includes a wide-ranging (possibly even ill-defined) set of behaviors and uses. Developers of the actual technology also admit they do not fully understand how it works.[5] As such, the actual AI may have behaviors and uses that go beyond even that specification.

Furthermore, high-risk AI systems may need transparency without first engaging with the AI. The features, limits, and bugs of, for example, a potentially dangerous AI are better learned without needing to use it. In such cases, as a proxy to understanding through doing, technical documentation is essential.

Article 13 "Transparency and provision of information to users" and Article 52 "Transparency obligations for providers and users of certain AI systems and GPAI models" both concern the transparency of high-risk AI systems. Article 13 explicitly states the requirement that "high-risk AI systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to users."

According to Art. 13(3b), these instructions for use shall contain at least the following information: "the characteristics, capabilities and limitations of performance of the high-risk AI system, including:"

(i) its intended purpose;

[5] "Why We Need to See Inside AI's Black Box", *Scientific American*, URL = https://www.scientificamerican.com/article/why-we-need-to-see-inside-ais-black-box/, accessed Jan. 31, 2024

(ii) the level of accuracy, including its metrics, robustness and cybersecurity referred to in Article 15 against which the high-risk AI system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity;
(iii) any known or foreseeable circumstance, related to the use of the high-risk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights referred to in Article 9(2);
(iiia) where applicable, the technical capabilities and characteristics of the AI system to provide information that is relevant to explain its output.
(iv) when appropriate, its performance regarding the specific persons or groups of persons on which the system is intended to be used;
(v) when appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used, taking into account the intended purpose of the AI system.

Article 52 concerns "certain AI systems", those that interact with natural persons (e.g., conversational AI such as ChatGPT or Gemini). It obliges the provider to ensure that the natural persons concerned are informed that they are interacting with an AI system unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use.

This includes AI for emotion recognition and biometric categorizations (exceptions are non-public-facing law enforcement AIs). It also includes media-manipulating AI (such as "deep fakes") which creates content that appreciably resembles real-world things and would be falsely thought of as real.

Other References to Technical Communication

Both the articles and annexes include several other references to requirements involving technical communication. **Article 14 on human oversight** (and **Article 13(3d)**) detail requirements around *human oversight*. The AI must be designed to enable human oversight of high-risk AI use (14.3). A *natural person* (14.1) must be assigned the role of the individual who has human oversight and enabled (14.4) to a) fully understand the AI capability, identify its mistakes, anomalies, and unexpected performance and b) remain aware of the possible tendency for overreliance on AI output, c) correct output and d) stop using or disregard the AI and e) intervene or stop an AI (through a "stop" button or similar). Also, (14.5) user action or decision must not be taken without verification and confirmation by at least two natural persons.

Article 13(3d) states that instructions for use must include human oversight measures (from Article 14), including "technical measures put in place to facilitate the interpretation of the outputs of AI systems by the deployers".

Technical communication is also discussed in other parts of the AI Act that are not discussed in this paper. These are: responsibilities of relevant "operators",[6] e.g. technical documentation for authorized representatives (Article 25) and importers (Article 26); documentation keeping (Article 18); AI training, testing, validation, and testing results (Article 54(1) point (i), Annex IV); the processing of personal data (Article 54.1); the post-marketing monitoring plan (Article 61.3); the location of technical

[6] According to Article 3 Definitions (8), "operator" means the provider, product manufacturer, deployer, authorized representative, importer or distributor

documentation for law enforcement, immigration, and asylum (Article 70(2) and Annex VIII point 11); how technical documentation can be controlled in the conformity assessment of AI (Annex VII point 4).

TEKOM EUROPE CONCERNS AND REQUESTS

Annex IV specifies what is required of technical documentation. Annex VII outlines how the notifying body will use the technical documentation, thereby providing an EU technical documentation certificate. Other areas discuss how the technical documentation is to be managed, once it is available.

However,

(1) The AI Act does not sufficiently detail instructions for use for GPAI such as GenAI.
(2) More specific details are needed on the production of technical documentation, specifically for the simplified technical documentation form and, generally, given that AI itself can produce technical documentation.
(3) The AI Act seems primarily conceived as a product for others' use. It does not consider anything specifically about an organization's in-house AI.

1. Who creates the simplified technical documentation form referred to in Article 11(1)?

Article 11(1) states that, to help smaller organizations (SMEs including startups), the EC shall create a simplified form for providing required technical documentation.

So that organizations creating such technical documentation can better prepare, we request that the EC provide more details on what is in that form, how its contents will be decided, and what interest groups will be involved in its creation.

1. Will the form include everything specified in the AI Act?
2. If so, what further details not provided in the AI Act are expected from larger organizations that cannot use the form?
3. If not everything in the AI Act is required, how will the EC decide what can be omitted in the form for SMEs and startups, assuming that the AI Act specifies what is required?
4. In answering these questions, who will be consulted or design the form? For example, will AI experts, product safety experts, and/or technical communication experts be consulted?

2. What are instructions for use with GenAI?

Annex IV requires technical documentation that includes instructions for use. However, there is currently no clarity on what that means for one form of now-popular AI – foundational AI such as GenAI, especially of the conversational kind.

Foundational models such as GenAI raise questions about determining what to include in these instructions for use. The AI Act refers to complete instructions for use (13.2), the level of accuracy that can be expected (13.3ii), and any known or foreseeable circumstances through misuse that may lead to risks to health, safety, or fundamental rights (13.3iii). What counts as complete instructions for use for such models?

Some instructions are easy to specify, such as installation and registration instructions, as well as instructions for how to enter input into various interfaces, such as text chat, instructions for more sophisticated environments such as sandboxes, and various elements such as temperature sliders. However, for other aspects of the AI, the completeness of the instructions for use is not as clear.

Interaction with these models is intended to be open-ended. Prompts are intended by GenAI designers to take almost any form (adjusted by ethical and legal concerns). For example, chat GenAI

based on large language models (LLMs) is intended to take any language input (in a known language) and provide natural-sounding responses (in that language). Other models (and more advanced integrated models) promise code-writing, image generation, and video responses. Some models also allow non-textual prompts, for example, image, audio, and video.

Some providers also promise to deliver accurate responses or provide services that imply such accuracy, for example, chatbots as search engines. Yet, accuracy is a significant problem with these models, undermining this specification. One way to address this has arisen as a secondary industry around GenAI, what is informally called *prompt engineering*: the careful construction of prompts to get the intended results. Participants in this industry offer solutions that either compensate for or avoid the limitations of the model. For AIs that take natural language, some of these prompts are more like code than natural language.

Thus, are instructions for using GenAI complete if they state that prompts can be any text (or non-textual prompts, where possible) – even if such an interaction frequently fails to return the results intended by the user? Should the instructions also include engineered prompts? Most instructions do not provide merely any way to use something, but the best intended way known by the providers. If specific engineered prompts get intended results more efficiently and accurately than simply requesting with natural language, and this is known to the providers, should the instructions include these prompts (– or, where they frequently change, reference to a live source where such prompts can be found)?

Furthermore, what are the levels of accuracy that must be documented? Are the levels at the providers' discretion or according to the industry in which they are intended for use?

The differences in technical documentation and instructions for use are significant. The most common current form of GenAI is large language models, which are trained on masses of language data. Pre-training and fine-tuning of such models include various elements, such as feedback from AI (RLAIF) and humans (RLHF). How the training is done is included in the technical documentation of the training data (Article 52(1a)).

For GenAI responses, these processes generally capture two different levels of accuracy: general naturalness and (especially ethical) appropriateness. In addition, several benchmarking groups in AI research and industry-test different models against each other for several relevant deliverables, including safety.

These accuracy levels are broad. They do not specify if the GenAI is excellent at decisions or recommendations against more specific standards, such as medical, engineering, or software standards. For specification at the AI Act level, we ask: should these broad levels be specified? If so, are they enough? Or should there also be, based on how the AI is intended to be used, reference to industry-relevant accuracy levels, for example, a GenAI for medical diagnosis meets the same accuracy levels as an average medical expert; a QA manufacturing GenAI has the same error-detection success as an inexperienced QA controller?

3. Can AI alone produce technical documentation for AI, or does it require human oversight? Who or what is responsible for technical documentation of AI?

We demand the regulators clarify further how technical documentation can be generated and the responsibilities for it. We already use AI to partially create technical documentation. However, some in the AI industry may consider technical documentation to be something that AIs can do wholly by themselves, as software applications can automatically generate user-relevant texts like log files,

error messages, and contextual documentation. So long as the technical documentation is correct, and assessed as such by the notifying body, they may believe it is not important how it is produced.

Yet, as stated in Article 11, such technical documentation is important for certifying high-risk AI as a safe product. This includes risk-assessment technical documentation.

First, we demand that the part of technical communication that deals with risk assessment be left outside AI's capabilities at all due to the specificities of this technical documentation and the direct connections to the safety of products. This includes AI documenting itself. We demand that the risk assessment be drawn up under human control, with AI playing no significant part in the creation.

Second, we demand the EC clarify the risk category of technical documentation, and as such AI creating technical documentation. Here are some questions to consider:

1. Is AI engaged in technical documentation a high-risk AI or low-risk (or minimal risk) AI?
2. Must an AI that creates technical documentation be certified to create technical documentation (that is, it is high-risk AI)?
3. Specifically, is an AI that generates technical documentation for any technology a safety component of the production process for that technology, and so (Article 6(1)) a high-risk AI requiring human oversight (Article 14)?
4. Can a high-risk AI that is not yet certified for conformity generate its own documentation on its own, without human authorship?
5. If documenting is high-risk because of its role in safety, could an AI that is not yet clearly high-risk or low risk become high-risk by default **because** it documents itself? Or is it only high-risk in documenting high-risk technology (AI or otherwise)?

4. Do isolated/in-house AIs require conformity assessment, including EU-certified technical documentation?

One kind of AI likely to be developed by many organizations, especially large organizations, is in-house AI for use by that organization and no one else. This is already being done by several large organizations in the EU. Details on how to approach such an AI seem to be missing in the Act. It may be that the requirements are sufficient for such AIs. However, some of the requirements seem irrelevant – those around products sold and marketed in the EU market. These AIs are typically isolated behind company intranets or similar secure in-house systems.

We ask that the regulators provide further details beyond the Act which are specific to in-house-developed AI, including guidance, especially with respect to such AIs' technical documentation. We demand clarity on whether such AIs must be risk-assessed and certified and if they require the same technical documentation as commercial AIs require. For example, could they use the form intended for SMEs and start-ups, no matter the size of the developing organization?

For in-house AI systems, we propose following the approach of the Machinery Regulation (EU 2023/1230) regarding machines that a manufacturer produces for their own use. That is, the same obligations to provide technical documentation and instructions for use apply to AI as to any machinery meant for the manufacturer's own use.

The European Association for Technical Communication - tekom Europe e.V. is the largest professional and technical association for technical communication worldwide. It was founded in 2013 and represents around 9,500 members in 11 country organizations and three corporate members. It aims at promoting the professional interests of all persons involved in technical communication. Technical communication is the process of defining, creating, and delivering information products of information for use – for the safe, efficient, effective and sustainable use of products (goods, technical systems, software, services).

European Association for Technical Communication – tekom Europe e.V.
European Transparency Register identification number: 786849753139-77
Heilbronner Strasse 86
70191 Stuttgart
GERMANY
President: Dr. Tiziana Sicilia
Executive Director: Dr. Michael Fritz
Contact: Dr. Gabriela Fleischer g.fleischer@tekom.de