European DIGITAL SME Alliance

DIGITAL SME reply to the AI Act consultation

6 August 2021

Introduction

On 21 April 2021, the European Commission has published a proposal for a European Act on Artificial Intelligence ("referred to as AI Act"). After careful assessment of the AI Act proposal, European DIGITAL SME Alliance believes that the proposal requires additional efforts to ensure the right balance between innovation and regulation.

In the following, AI experts from SMEs have identified some of the key issues related to the current text of the proposal. DIGITAL SME sees significant risks in the approach proposed by the European Commission with regards to high compliance costs for SMEs, the complex requirements related to the proposed conformity assessments, and associated burdens on SME resources and innovation-capacity. Our experts have also identified a number of technical issues in the text.

While DIGITAL SME generally welcomes a harmonised approach to regulating AI in the EU and believes that ethical AI is important both for EU citizens and businesses, we are concerned that several aspects of the proposal, in its current form, risks to hamper innovation and to overburden SMEs.

DIGITAL SME main comments

- **The definition of Artificial Intelligence (AI) provided in the proposal is too broad.** Some of the methods mentioned under Annex I (b)[1], (c)[2] have been applied for decades without falling under any specific regulation. For instance, concerning c), insurances or credit rating organisations are applying statistical models to rate their customers. In addition, AI experts are not in agreement

[1] Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;
[2] Statistical approaches, Bayesian estimation, search and optimization methods.

today what the exact definition of AI is. Moreover, they are not in agreement about which specific algorithms would fall under the definition of AI.

- The **requirements regarding data quality**, such as defined in the recital 44[3] and **Art. 10 (3)**[4] are unrealistic. Requiring data to be "error-free" and "complete" is hard to define and unrealistic in real-world applications. These requirements impose a purely academic assumption which in reality is never being met.
- **Fines (Art. 71) for non-compliance** need to be **proportionate** and **limited** for SMEs.
- Conformity assessments will be based on standards, but SMEs are not included in the standards development as they are under-represented in standardisation organisations. Oftentimes, this leads to standards which are written in a way that is non-practical and not applicable for SMEs. **We strongly advise that standards are written with the active participation of SMEs, and to avoid a "one-size-fits-all" approach,** often adopted by research organisations, large companies, and legal and ethical experts. **The standards referred to in order to comply with the regulation should be available free of charge.**
- **Conformity assessments will be too costly. This may put a burden on AI innovation as they bound financial and human resources of SMEs**: The conformity assessment and certification procedure are estimated at around 5k – 7k€ according to the EC Impact Assessment, which seems unrealistic. Costs are likely to be substantially higher due: Total costs = ***external consultancy*** **+** ***internal costs*** **+** ***auditing cost*** (5k-7k €). However, *external consultancy* + *the internal costs* are missing from the equation in the Impact Assessment, and will likely multiply the auditing costs with a substantial factor. The EC and regulators are requested **to calculate the total costs** instead of the auditing costs only. **Otherwise, a regulation that requires SMEs to make these significant investments, will likely push SMEs out of the market.** This is exactly the opposite of the intention to support a thriving and innovative AI ecosystem in Europe.

[3] See p. 29 EN version of the AI Act
[4] See p. 48 EN version of the AI Act

- **SMEs will not be able to pass on these costs to their customers in the final customer end pricing.** The market is global and highly competitive. Therefore, customers will choose cheaper solutions and **Europe risks to be left behind in technology development and global competition.** Moreover, certification schemes and conformity assessment for AI will duplicate the burden that is already put on SMEs with certification schemes for cybersecurity[5]. **This hampers the SMEs' ability to innovate. We strongly suggest that the regulators move away from this approach towards a more SME-friendly approach and avoid duplication of requirements and assessments.**
- **The expert group proposed in Art. 57 needs to ensure SME participation that reflects their importance in the market (99% of EU companies are SMEs).** Given the lobbying strength of other entities (e.g., governmentally funded research organisations, academia or large multinationals and industry associations representing large multinationals).
- The high-risk sectors as set out in Annex III (see Art. 6) should be revised, as they include AI applications that do not have a direct impact for the public, for citizens, or for customers or are common practice (e.g., 5 (b)).

Please refer to the different parts below for more details on each aspect. For specific issues, DIGITAL SME is providing input regarding A) technical remarks, B) remarks on quality assurance and certification, and C) impact on innovation, D) general remarks in the different sections below.

[5] The proposal from the Commission is to have certification schemes for all AI applications coming from sectors not already regulated, similar to the cybersecurity certification schemes set up under the EU Cybersecurity Act. The cost of compliance cannot be absorbed by SMEs.

Detailed comments

A) Technical Remarks:

Annex I of proposed AI Act tries to name a list of specific AI algorithms which would fall under this regulation. The list given there is not specific enough, for the following reasons[6]:

1.1. The phrase "using a wide range of methods" is vague, given the strong implications of this legislation.

1.2. AI experts are not even in agreement today what the exact definition of AI is. Moreover, they are not in agreement about which specific algorithms would fall under the definition of AI.

1.3. Likewise, some of the methods mentioned under Annex I (b)[7], (c)[8] have been around for decades and have never been considered to require regulations.

1.4. Instead, a suggestion could be to approach the regulation AI from the application side, *without* referring to specific algorithms, since also "non-AI" algorithms are being used (for decades) for autonomous decision making, e.g., in mortgages, loans, insurances, clinical trials, and many other areas. The application domain determines whether they need regulation or not.

[6] The OECD definition and AI principles, largely transposed on the AIA proposal where adopted on 22 May 2019 by the OECD member countries when they approved the OECD Council Recommendation on Artificial Intelligence (https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449). The OECD AI Principles are the first such principles signed up to by governments. Although we can question the definitions, they were already largely debated in the OECD AI working groups and consensus was reached. All the countries listed herein adhere to the definition and also to the AI principles since 2019: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#adherents

[7] Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

[8] Statistical approaches, Bayesian estimation, search and optimization methods.

1.5. Requirements regarding data quality, set out in recital 44[9] and Art. 10 (3)[10] are unrealistic. Requiring data to be "error-free" and "complete" is hard to define and unrealistic in real-world applications. These requirements impose a purely academic assumption which in reality is never being met.

1.6. The precision measures, required in recital (49), p.30, are required to be transparent and understandable to the users. Most users, however, will not be able to understand such KPIs easily, such as for example accuracy, precision, recall, F1-measure, MAE, MSE, AUC, ROC, AUROC, loss functions, to mention a few. Without gross oversimplification, it will often not be possible to make them easily understandable.

1.7. The technical robustness required in (Art. 50) in terms of errors, faults, unexpected situations cannot be assured for AI systems, since AI systems can also be trained to undertake adversarial attacks and to improve their performance in those continuously. AI learns – so it can also learn adversarial behaviour.

1.8. The technical parts of the document would generally benefit from more AI / statistics and optimization / application domain expertise.

B) Remarks on Quality Assurance and Certification:

Putting all requirements together, the document seems to propose – for certain application domains as specified in Annex III:

- a new (so far, largely unspecified) certification approach for such AI systems or
- AI-based components of technical systems in areas such as referred to in Annex II (implicitly requiring a second certification, namely CE)
-

[9] See p. 29 EN version of the AI Act
[10] See p. 48 EN version of the AI Act

provided that technology as specified in Annex I is deployed (which is insufficiently and too broadly specified at the same time).

For further clarification, Annex II explicitly relates to application domains, too, including specifically machinery, toys, recreational craft and personal watercraft, lifts, equipment and protective systems intended for use in potentially explosive atmospheres, radio equipment, pressure equipment, cableway installations, personal protective equipment, appliances burning gaseous fuels, medical devices, in vitro diagnostic medical devices.

1.9. The proposal from the Commission is to have parallel certification schemes for all AI applications coming from sectors not already regulated, similar to the cyber security one. This is not feasible because SMEs are still struggling with certification schemes for cybersecurity. This hampers the SME's ability to innovate.

1.10. If the conformity assessments will be based on standards, but SMEs are not included in the standards development as they are under-represented in standardisation organisations, this will be a burden for SMEs as the standards will be written in a way that will be non-practical and not applicable for SMEs. **We strongly advice that standards are written with the active participation of SMEs, and to avoid a "one-size-fits-all" approach, often adopted by research organisations, large companies, and legal and ethical experts.**

1.11. The conformity assessment and certification procedure are estimated at around 5k – 7k€, which we find questionable for the reasons detailed below. The EC and regulators are requested to calculate the total costs instead of the auditing costs only.

1.11.1. Typically, the total cost for certification includes ***external consultancy + internal costs + auditing cost***. The above estimate of 5k – 7k corresponds with the typical auditing costs, once the auditee is fully prepared for passing the audit. The other cost factors exceed this by far, since a) significant consulting is necessary and b) significant internal staff costs, and possible also investment costs are caused by certification. For SMEs to compete in a level-playing field, they should be supported. Regulatory sandboxes could be one form of support.

1.11.2. Due to these financial and human resource investments, SMEs will likely be pushed out of the market. This is already happening today due to other certifications such as ISO 9001 and information security management system requirements such as ISO 27001 / TISAX. This can be simplified through implementation guides such as the SBS SME Guide on ISO/IEC 27001.

1.11.3. It is unclear whether in Art. 17 (p. 53), the quality assurance is different from existing ones such as ISO 9001:2015, or ISO 27001 – since there is no mentioning of these systems. We advise to build on existing standards, if applicable.

1.11.4. The CE certification requirement in addition to the auditing requirement imposes another burden for SMEs which seems impossible to meet. Moreover, in Annex II a wide range of directives and regulations are mentioned, for which it is unclear what the impact would be. For the moment, we have to assume that only application domains mentioned in Annex III are affected by this regulation, however subject to CE certification once AI components as defined (insufficiently) in Annex I are integrated into such system. This would require retrospectively certifying thousands of running systems, due to the fact that statistical models and optimization algorithms are currently being used in many critical systems in infrastructure, transportation, utilities, finance, etc.

1.11.5. The Fines (Art. 71) for non-compliance need to be proportionate to the size of the undertaking and limited for SMEs.

C) Remarks on Impact on Innovation:

1.12. The requirement to send data to regulators is not motivated clearly. It seems to almost imply that regulators could, as a bank or a company like Google, provide software code for inspection. This creates IPR issues, data protection issues, etc.

1.13. The Commission implies spending a significant amount of money (17% of the AI investment budget) on validation and regulation of AI, without a

central contact but instead 27 local agencies and one central supervisory agency (NCA). This will lead to market divergence.

1.14. We observe that regulation without appropriate technical understanding, as exemplified by the few technical parts of this document, will cause a major burden to the innovation capability of European AI industry specifically and European industry generally, as far as anything related is the industry sectors mentioned in Annex II are affected.

1.15. Despite all recommendations by the AI expert group, advocating the need for finding a balance between the legal part and the technical part, the document is dominated by the legal aspects, in an early stage of technology development in this area. We advise a better balance between technology, legal, and ethical aspects.

1.16. The cost of compliance with the certification requirements cannot be absorbed by SME providers, and will not be accepted by their customers (i.e. mostly SMEs in other sectors) when trying to include them into the final customer end pricing. The market is already global and highly competitive, and Europe will be left behind in technology development even stronger than it already is, as of today.

1.17. The expert group proposed in Art. 57 needs to include significant participation of SMEs. Moreover, we suggest participation of governmentally funded research organizations, academia, large multinational companies and their industry associations to be adjusted and/or limited, as their interests are in opposition to those of SMEs. Given the lobbying strength of such entities, we recommend at least 40% SME participation in the expert group.

1.18. The high-risk sectors as set out in Annex III (see Art. 6) should be revised, as they include many AI applications that do not have a direct impact for the public, for citizens, or for customers.

D) General remarks

D.1 : Remarks regarding the Explanatory Memorandum

1. The Explanatory Memorandum (1.1, p.3) specifies that "For some specific AI systems, only minimum transparency obligations are proposed, in particular when chatbots or 'deep fakes' are used." We are not sure whether we understand this correctly, but in particular such applications should be strongly regulated, and the simple requirement stated in Art. 52, 3 to "disclose that the content has been artificially generated or manipulated" is considered completely insufficient as this disclosing statement can of course be hidden in general terms of business, for example.
2. In Section 1.2 of the Explanatory Memorandum (p.5), it is explicitly stated that "In relation to AI systems that are components of large-scale IT systems in the Area of Freedom, Security and Justice managed by the European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA), the proposal will not apply to those AI systems that have been placed on the market or put into service before one year has elapsed from the date of application of this Regulation, unless the replacement or amendment of those legal acts leads to a significant change in the design or intended purpose of the AI system or AI systems concerned." We find such exceptions unfair from the perspective of SMEs and potentially concerning from the perspective of an EU citizen.

D.2: Issues identified in relation to the Recitals

It is unclear how many recitals relate to Annex III. A list of the issues identified with the recitals is summarized below.

1. Recital (36): Many systems are in use today for employee selection, matching applicants and profiles using AI-technology or statistical methods. The same applies for employee evaluation, supervision, and performance scoring. So these systems all should be regulated, according to this requirement.

2. Recital (37): For credit scoring and insurance premiums, for example, statistical methods have been in use for decades, without regulation at all. The regulation would immediately apply to these and many other applications of statistical and AI-based models. By the way, technologically, there is no difference between an AI-based scoring model (that might use a random forest model, for example) and a statistical one (that might use a linear model, for example).
3. Recital (38): While many different types of AI-based system for surveillance and manipulation of citizens fall under this regulation, as observation we remark that this topic defines interesting exemptions, namely (emphasis added): "AI systems specifically intended *to be used for administrative proceedings by tax and customs authorities should not be considered high-risk AI systems* used by law enforcement authorities for the purposes of prevention, detection, investigation and prosecution of criminal offences."
4. Recitals (71, 72): What exactly is a "regulatory sandbox"? In the German version of this document, it translates into "Reallabor" (i.e., "real-world laboratory"). This raises questions such as "who will get access?", "who pays for the sandboxes?", "who covers the extra efforts for SMEs to get access?".
5. Recital (78): A "post-market monitoring system" is required here. However, who will cover the costs for developing that? For SMEs, this will create the next big cost factor – pricing it into the end-customer price will not work out.

D.3: Comments on specific articles

1. Title I, Article 2, 1.c): How could this be achieved? E.g., assume a credit card transaction happening in the EU, but real-time scored by the credit card issuing company located in the US? Analysis of social network profiles by a US-based company in the US for the purpose of e.g. targeting advertisement (thus influencing people's behaviour), influencing voting behaviour, etc.?
2. Title II, Article 5, (1)(c): Why does this only mention public authorities, but not companies, while the provisions before do not make this specialization?
3. Article 10 (6): "Appropriate data governance and management practices shall apply for the development of high-risk AI systems other than those which make use of techniques involving the training of models in order to ensure that those

high-risk AI systems comply with paragraph 2." The German translation of this explicitly says "training of models with data", so we wonder why – if "training of models with data" does not happen ("… other than those …") – data governance and management practices shall apply.

4. Article 12 (1) and (2): What are the "recognized standards or common specifications" that might apply to the logging? Do we need to expect another formalization and certification here, again? It should also be recognized that, potentially, paragraph 2 could imply enormous amounts of data to be logged, again depending on what regulation will require.
5. Article 17: It needs to be defined whether this section describes a new quality management system, or whether it cannot simply use a reference to existing approaches, such as ISO 9001:2015 on quality management and ISO 27001 or TISAX for ISMS. In general, the document does not put the QM-requirements proposed here into context with existing certifications in the QM domain.
6. Article 52, 1: In paragraph 1 this article states "AI systems"; should this not be "high-risk AI systems"?

European DIGITAL SME Alliance

About this document

This document has been drawn up based on input from DIGITAL SME's Task Force AI & Standards, composed by Prof. Thomas Bäck, Dr. Emilia Tantar, Prof. Stelian Brad, Mr. Petko Karamotchev, Dr. George Sharkov, Dr. Luca Maggiani, Mr. Jose Santos. The input on this document has been coordinated by Mr. Omar Dhaher and Ms. Annika Linck and is consulted with DIGITAL SME's general membership, in particular the DIGITAL SME Focus Group AI.

For further information on this position paper, please contact:

Mr. Omar Dhaher, Senior Technology Manager

E-Mail: o.dhaher@digitalsme.eu

Ms. Annika Linck, Senior EU Policy Manager

E-Mail: a.linck@digitalsme.eu

About European DIGITAL SME Alliance:

European DIGITAL SME Alliance (DIGITAL SME) is the largest network of small and medium sized enterprises (SMEs) in the ICT sector in Europe, connecting about 45,000 digital SMEs. The Alliance is the joint effort of 30 national and regional SME associations from EU member states and neighbouring countries to put digital SME at the centre of the EU agenda.