European
DIGITAL SME
Alliance

DIGITAL SME Position Paper on the EU AI Act

September 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”). With this position paper, the European DIGITAL SME Alliance takes the opportunity to comment on the legislative draft.

The European DIGITAL SME Alliance generally welcomes a European approach to regulating Artificial Intelligence (AI). For instance, a harmonised approach can help provide more opportunities for SMEs to scale, as a regulation at European Union (EU) level ensures that the rules will be the same across all 27 member states. Also, a stable framework is very important, to ensure legal certainty and predictability for stakeholders. The EU’s vision for ethical AI and strengthening user choice and control may be able to set Europe apart in global competition[1]. After all, Europe has a strong human rights record and is recognised as a “normative power”[2], which provides legitimacy to set a global standard.

However, in addition to becoming the frontrunner when it comes to ethical AI and regulation, Europe needs to support AI innovation, development, and market uptake by European companies. While Europe has advantages in AI development, such as a strong industrial base and AI research and talent, analysts say that it is “punching far below its weight”[3].

Against this background, the European DIGITAL SME Alliance believes that the proposal for a European Act on AI requires additional efforts to ensure the right balance between innovation and regulation. While an ethical approach to AI is

[1] Erik Brattberg, Raluca Csernatoni, Venesa Rugova, 9 July 2020, “Europe and AI: Leading, Lagging Behind, or Carving Its Own Way?”, available at: https://carnegieendowment.org/2020/07/09/europe-and-ai-leading-lagging-behind-or-carving-its-own-way-pub-82236

[2] Ian Manners, 2020, “Normative Power Europe: A Contradiction in Terms?”, see: https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-5965.00353

[3] Ibid.

important both for EU citizens and businesses, we are concerned that several aspects of the proposal, in its current form, risk to hamper innovation and to overburden SMEs.

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 with the text.

As a more fundamental criticism to the proposed regulation, DIGITAL SME is questioning the approach of regulating AI via standards and the complexity associated with the so-called New Legislative Framework (NLF) approach: What are the consequences of using standards to regulate a technology that is not mature enough? SMEs may be reluctant to invest time and resources in the participation of standards-making of products and services that are still under development. SMEs participation in standardisation bodies is generally not representative of their percentage in the economy.[4] In other words, by delegating the details and the rules-setting to the standardisation organisations, large companies and research organisations obtain the opportunity to set the standards and to dominate new technologies and markets, without leaving room to digital SMEs. In order to avoid this, **it is pivotal that the European Commission installs rules and safeguards to make sure that there is real and effective representation of SMEs** in standards-making.

[4] This paper, e.g., lists figures for ETSI, which points to around 28% of SMEs in the membership, while SMEs make up 99% of all EU companies, see: Kirti Gupta, 2017, “The Role of SMEs and Startups in Standards Development”, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3001513

Executive summary

1) Definition of AI

The Definition of AI: The definition of Artificial Intelligence (AI) provided in the proposal is too broad. Some of the methods mentioned under Annex I (b)[5], (c)[6] 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. While we appreciate that the European Commission is building on the most broadly accepted AI definition[7], many AI experts are not in agreement today what the exact definition of AI is, and they are not in agreement about which specific algorithms and techniques would fall under the definition of AI.

Regulating the application rather than the technology. Building on the above-mentioned criticism of the definition, although the risk cases are relatively sound, AI is not a proper technological term nor a necessary and causative element in the mentioned risks (e.g., biometric identification or manipulation, social scoring). Risks stemming from these areas of application are not strictly limited to AI-technologies. Thus, there is a risk that organisations could circumvent the AI definition and carry out the same activity with a technology that is strictly speaking not AI. **Therefore, for high risks for society, it would be better to regulate the application than the technology**.[8]

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

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

[7] The OECD definition and AI principles, largely transposed on the AIA proposal, were 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

[8] See also: Michael Veale, Frederik Zuiderveen Borgesius, July 2021. Version 1.2., "Demystifying the draft EU AI Act", available at: https://arxiv.org/ftp/arxiv/papers/2107/2107.03721.pdf

2) Conformity assessment & compliance costs

Conformity assessments & compliance costs will be too high. This may put a burden on AI innovation as they bind financial and human resources of SMEs: The estimated compliance costs for SMEs that develop or deploy high-risk AI applications are estimated at around 6k – 7k€ according to the EC Impact Assessment[9], with the conformity assessment (for the notified body to monitor compliance with the documentation requirements) estimated at 3.5k€ to 7.5k€[10], which, leaves us at about 9.5k€ to 14.5k€ of total estimated costs. However, costs are likely to be substantially higher if the total costs are considered, including *external consultancy* + *internal costs* + *auditing costs*. External consulting and adding internal costs (e.g., the HR effort needed to complete the conformity assessment, internal legal advice) will likely multiply the auditing costs with a substantial factor. **In sectors that fall under the "New Legislative Framework" (NLF), even a change of an aesthetic element of a product requires a new certificate with limited discount for this type of small updates. Requiring this for AI systems would lead to high costs for SMEs.** Therefore, as DIGITAL SME, we would like to request the EC and the co-legislators **to calculate the total costs for SMEs that would be concerned by the regulation**. In addition, costs arising from the need to regularly update products and renew certification are missing from the equation. **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. **Therefore, the co-legislators need to re-calculate certification costs based on the points mentioned above, in order to realistically estimate the burden this may have on SMEs.**

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

[9] European Commission, 21/04/2021, COMMISSION STAFF WORKING DOCUMENT, IMPACT ASSESSMENT Accompanying the Proposal for a Regulation of the European Parliament and of the Council, p. 71

[10] Ibid. p. 69

with certification schemes for cybersecurity[11]. **This hampers the SMEs' ability to innovate.**

We strongly suggest that the regulators move away from this approach towards a more SME-friendly approach. The duplication of requirements and assessments from existing regulation (such as GDPR, cybersecurity, but also conformity requirements in line with the NLF) needs to be avoided. Also, we would like to ask the co-legislators to ensure that the conformity assessments and compliance costs related to the regulation will not pose an excessive burden for SME innovators.

3) SME representation in standardisation and beyond

Any standard proposed by the standardisation organisations should include SME representatives in the making. It needs to be ensured that a standard that will be used as reference to the AI Act conformity assessment is actionable and easy-to-deploy for SMEs.

Conformity assessments will be based on standards, but SMEs are often 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.**

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[12] (e.g., governmentally funded research organisations, academia or large multinationals and industry associations

[11] 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.

[12] See, e.g., Corporate Europe, 2021, The lobby network - Big Tech's web of influence in the EU.pdf (corporateeurope.org), p. 6: 97 M€ per year, Google and Facebook more than 5M€, each.

representing large multinationals) SMEs need to be strongly represented in such a body to avoid disadvantages for SMEs.

We would like to ask the EU institutions to install rules and safeguards to make sure that there is a real and effective representation of SMEs in the standards making and beyond.

4) Clarifying liability and “placing on the market” to avoid limiting innovation

Roles and responsibilities: The regulation doesn't sufficiently take into consideration that AI development entails complex supply chains. Given the complex nature of AI solutions, 3rd party developers (among them probably many SMEs) are often involved to develop solutions for deployers (B2B customers) who ultimately provide the technology to their end users (internally or externally). Deployers are usually the ones who ultimately put the system to work, decide how to use and change the system, which data to retrain a model with, etc., with developers having only limited control over the use and further changes of the AI system after handover. We suggest making a distinction between developers and deployers of an AI system and clearly define responsibilities between these parties, taking into consideration which elements each of the parties have control over.

Definition of "placed on the market" or "put into service": For digital software, this definition is not sufficient and needs to be further clarified. Developing AI systems is a highly iterative process, and experimentation is a significant part of development. It needs to be clear at which stage of the development process the regulation applies, and should be noted that if regulation applies too early (e.g., when still in a Proof-of-Concept stage), costs of experimentation could increase significantly, hindering innovation

Open Source Software (OSS) and openness in AI-related coding and development is a fundamental driver of AI-innovation in academia and industry. SMEs, but also larger companies and researchers rely on OSS to build AI applications. Developers and researchers making AI code, sharing ideas, or making models available to others should not be limited due to uncertainty when it comes to “placing on the market” or being a “deployer” or “provider”. The legislator should clarify responsibilities and limit liability, potentially explicitly excluding OSS and open collaboration in order not to hinder innovation and to guarantee free and open access to AI codes and development by the community.

5) Rethinking high-risk

Identification of high-risk applications: Annex III provides different examples of high-risk applications. While the current proposal is a good first attempt to identify cases that belong to different risk categories, more guidance is needed for providers to be able to classify AI systems in practice. AI systems rarely have the exact same application as described in these examples in Annex III, making it difficult for providers, esp. for SMEs without access to a team of inhouse lawyers, to determine if an application would be considered high risk or not. **Clear criteria and a possibility to officially confirm the classification of specific use cases should be set up for SMEs.** This could be a service offered via the “sandboxes”. **In any case, sandboxes should be mandatory in all EU member states and functional upon the entry into force of the regulation.**

While we generally welcome the risk-based approach of the EU AI Act, **the current approach disregards the role of access to data and horizontal integration of a company, when it comes to determining societal risks**. A large company that has access to incredible amounts of data from various sources, such as Google or Facebook, has a much larger potential to develop manipulation techniques and to cause harm (see e.g., Cambridge Analytica scandal[13]). A large insurance company or bank that can merge their profiling algorithm result with other customer data can have a much wider impact on society than any SME. While we are aware that questions of contestability are tackled under the future Digital Markets Act (DMA), the issue of societal risks related to the size of a company is not addressed there. The upcoming AI Act could be an adequate place to take into account the size of the company as well as access to data and horizontal integration.

Therefore, it may be necessary to revisit the criteria that determine a high risk for society overall and include the criteria of size in combination with access to data that can cause harm to fundamental rights.

[13] See, e.g., Alex Hern, 6 May 2018, The Guardian, [Cambridge Analytica: how did it turn clicks into votes? | Big data | The Guardian]

Detailed comments

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

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:

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

1.2. While we appreciate that the European Commission is relying on the most broadly accepted definition provided by the OECD[14], many 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)[15], (c)[16] have been around for decades and have never been considered to require regulations –

[14] The OECD definition and AI principles, largely transposed on the AIA proposal, were 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

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

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

for good reasons, as these methods are per se not high-risk or harmful, but just standard technology and also not an AI technology.

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, plant control systems, and many other areas. The application domain determines whether they need regulation or not.

1.5. Requirements regarding data quality, set out in recital 44[17] and Art. 10 (3)[18] are unrealistic. Requiring data to be "error-free" and "complete" is impossible to define and imposes a purely academic assumption which in real-world applications is never 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 the common technical 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 those 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:

[17] See p. 29 EN version of the AI Act

[18] See p. 48 EN version of the AI Act

- 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)

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 cybersecurity 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 initial compliance costs are estimated at around 6k – 7k€ according to the EC Impact Assessment, 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 initial compliance costs 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 possibly 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. In any case, the compliance costs for SMEs should be limited and/or they should be provided with financial support to account for those costs.

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. Annex II refers to a wide range of directives and regulations, which may be covered by the regulation and for which it is unclear how the regulation would interact with existing ones and new standards relevant for AI.

1.11.5. 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, e.g., statistical models and optimization algorithms are currently being used in many critical systems in infrastructure, transportation, utilities, finance, etc.

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

1.11.7. Cost of compliance: What makes things even worse is the compliance of different versions of the same product. Every time the SME developer releases an update of the same product, they will have to pay. Note that in all sectors that the EU has regulated through standards, SMEs complain that conformity assessment bodies need to issue a new certificate even for the smallest product modifications, irrespectively from their impact on safety. In sectors that fall under the “New Legislative Framework” (NLF), even a change of an aesthetic element of a product requires a new certificate with limited discount for this type of small updates.

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. Based on the European Commission Impact Assessment, a study by the Centre for Data Innovation calculates 17% overhead costs (both fixed costs (e.g., setting up the quality management system, designing workflows and system architectures to comply with the Act’s stipulations, conducting conformity assessment procedures) and variable costs (i.e., ongoing monitoring of the AI system to ensure it complies with the AIA)[19].

1.14. SMEs benefit from harmonized rules across all 27 member states, and a strong governance structure that ensures coordinated and harmonized application of the rules.

1.15. We are concerned that the regulation may cause a major burden to the innovation potential of the European AI industry specifically and European industry generally (especially the industry sectors mentioned in Annex II).

1.16. 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.

1.17. The cost of compliance with the certification requirements cannot be absorbed by SMEs, 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

[19] https://www2.datainnovation.org/2021-aia-costs.pdf, p. 7

be left behind in technology development even stronger than it already is, as of today.

1.18. 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.

1.19. 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)).

D) General remarks

D.1 : Stability and clarity of the framework

1. Stability & clarity of the framework: A stable framework is very important, to ensure legal certainty and predictability for stakeholders. The possibilities to amend annexes need to be clearly defined and include adequate consultation, also of SMEs.

D.2 : Remarks regarding the Explanatory Memorandum

2. 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 easily be hidden in general terms of business, for example.
3. 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.3: 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.
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. While 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), neither one of them is "artificially intelligent", as they are all just performing a mathematical interpolation to derive a prediction for a new data record, based on existing data records. In many cases, undesirable biases are introduced into the models not by the modelling technology, but by the data that is used for modelling and by the application domain experts who select the data and/or influence/tune the resulting models. Therefore, we recommend not to regulate the technology, but its application in terms of the application domains and the selection of data for training the AI.
3. Recital (38): While many different types of AI-based system for surveillance and manipulation of citizens fall under this regulation, as an observation we remark that this topic defines 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." Again, we consider such obvious exemptions from the regulatory requirements as unfair for SMEs and concerning for EU citizens, who are likely interested in transparency regarding reasons, and potential errors, in case of having been identified as potential criminals.

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.4: 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 IS0 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”?

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 Ms. Annika Linck and Mr. Omar Dhaher, 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:

Ms. Annika Linck, Senior EU Policy Manager

E-Mail: a.linck@digitalsme.eu

Mr. Omar Dhaher, Senior Technology Manager

E-Mail: o.dhaher@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 more than 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.