European DIGITAL SME Alliance

The largest network of ICT small and medium enterprises (SMEs) in Europe,

MARCH 2022

FACT SHEET
AI Act & SMEs
Supporting AI Innovators

On 21 April 2021, the European Commission put forward a proposal for an Artificial Intelligence Act (AI Act) to set European rules for AI. This document gathers comments from SME experts in DIGITAL SME's Focus Group AI. It aims to contribute to making the Act the best regulatory framework available for an innovative, trustful and responsible AI ecosystem.

Tel: +32 2893 0235
Email: office@digitalsme.eu
EU Transparency Register: 082698126468-52
Address: Rue Marie-Thérèse 21, 1000 Brussels, Belgium

https://digitalsme.eu

DIGITAL SME FG AI
Focus Group Artificial Intelligence
An initiative together with the European Commission's Joint Research Centre

AI Act & SMEs: Supporting AI Innovators

1. The AI Act may stifle the innovativeness of Europe's businesses.

The AI Act intends to position European businesses as frontrunners in ethical AI solutions. While this is welcome, a highly regulated approach may limit the innovativeness of SMEs. Why is this the case? SMEs often provide *tailor-made* and *agile* software solutions, including AI applications, rather than off-the-shelf software. However, over-regulation and standardisation threatens such business models as it prescribes one correct approach, where there may be several. This is especially true in a not yet mature environment, such as is the case in many areas of AI application. If Europe moves too fast towards a standardised and highly regulated approach, this will push SMEs out of the market, even if they provide better solutions than larger players.

For example: *Tailor-made data analysis.*
What's the advantage of working with an SME? A large company will often provide a fully integrated software and dashboard to monitor data and processes. SMEs, on the other hand, often programme tailor-made software upon the demand of their clients, and build on the existing infrastructure to help their customers optimise their processes. While the large player will benefit from a highly regulated and standardised approach, the business model of the SME relies precisely on a tailor-made agile approach that cannot be approved by conformity assessments in advance.

Our proposal: *Avoid regulating SMEs in areas that do not pose risks.*
It is precisely the innovation potential of such tailor-made approaches that support the competitiveness of Europe's economy. Therefore, the proposal of the AI Act should be revised with the aim in mind to support the competitiveness and innovation-potential of businesses, especially SMEs.

2. The definition of AI provided in the proposal is too broad.

We appreciate that the European Commission proposal is building on the broadly accepted AI definition first put forward by the OECD[1]. However, many AI experts are not in agreement today what the exact definition of AI is. With continuous innovation happening in the field, a static definition based on enumerating a set of technologies existing today will be incomplete tomorrow. Further, some of the practices specified in Annex I (b)[2], (c)[3] of the AI Act include non-AI statistical and optimisation techniques that are widely applied and in use in different sectors of the economy.

For example: *Optimisation methods, e.g., in logistics.*
The AI Act includes in its definition in Annex I "statistical approaches, Bayesian estimation, search and optimization methods". Insurances or credit rating organisations are applying statistical models to rate their customers. This is a largely accepted common practice today. Likewise, optimisation methods are common classical technology in many application domains (e.g., logistics).

[1] 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

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

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

Flaw in this approach: *The scope of the AI Act will be too wide.*
SMEs applying statistical approaches, e.g., in the logistics, in the manufacturing or machinery sector, e.g., to optimise processes, may fall under the scope of the regulation even though they are performing tasks which are strictly speaking not "AI" and may not pose a high-risk, as the actual risk depends on the application of the technique.

Our proposal: *Revise the AI definition and in particular Annex I.*
The definition of AI should be revised and ensure that a) it includes a necessary component of "autonomy" in decision-making and b) that it does not include widely used statistics and optimisation methods. On the other hand c) the definition should be future-proof and allow for the inclusion of technological approaches that cover more powerful forms of AI in the future.

3. Real risks are not adequately addressed.

While the current proposal defines different risk categories and bans certain uses of AI, which have a high potential risk for society (for instance: biometric surveillance, general purpose storing), it also includes clearly stated exceptions, omissions, and loopholes[4]. We think it is in the interest of SMEs and European citizens to adequately address the real and future risks of AI according to the overall risk for society and fundamental rights.

For example:
A large tech company, or an insurance company or bank that can merge their profiling algorithm result with other customer data. This may pose risks for fundamental rights of individuals, and for society as a whole. This risk is largely due to the power these larger players have to combine different data sets, and it is less about the specific technique applied. On the other hand, SMEs applying statistical approaches, e.g., in the logistics, in the manufacturing or machinery sector, e.g., to optimise processes, may fall under the scope of the regulation as performing "high-risk" AI, while there is no direct safety risk from applying these techniques (as long as the machine does not operate autonomously) and there is no risk for society and fundamental rights overall.

Flaw in this approach: *It does not address the real risks.*
The approach does not address the overall high-risks for society and fundamental rights, nor does it necessarily address real safety issues or risks for consumers. Further, the list of high-risk AI application does not include certain applications that we consider to be high-risk, especially in the light of recent attempts to influence individual voting behaviour and citizen's opinions by targeted messages and fake news[5].

[4] For instance, the AI Act states: "For some specific AI systems, only minimum transparency obligations are proposed, in particular when chatbots or 'deep fakes' are used." Further, there are exemptions for eu-LISA; exemptions for administrative proceedings by tax and customs authorities (see recital 38).

[5] Examples include: AI systems that may provide (false) information (misinformation, deep fakes), or AI systems intended to be used for the purpose of diagnosing or classifying mental health of natural persons, or for identifying or approximating the psychological profile or character traits of natural persons from proprietary or public data sources or a combination thereof about natural persons, regardless of the intention of such AI systems (e.g., medical diagnostics, target marketing, influencing voting behavior); nor AI systems intended to be used for the purpose of scoring, permanently behaviorally surveilling, or otherwise assessing natural persons regarding their access to or amount of fees paid for obtaining important insurances, such as e.g. health insurances, insurances for disability or other inabilities to work (including caused by psychological, mental, burn-out and similar reasons), and car and other transportation operations insurances (including occasional or permanent behavior observation, surveillance and analysis).

Our proposal: *Regulate the application rather than the technology in light of high-risks for society & fundamental rights.*
Artificial Intelligence, as defined in the AI Act, is not a properly defined technological term that can be considered as a necessary and causative element in the risks mentioned in the Act (e.g., biometric identification or manipulation, social scoring). Risks stemming from these *areas of application* are not strictly limited to AI-technologies. Therefore, for *high risks for society*, it would be better to regulate the application than the technology. When considering high risks, we propose to revisit the AI definition. Some experts suggest including concepts such as "autonomy in decision-making". That means that, for instance, a self-learning AI which automatically adapts manufacturing processes or driving behaviour without a human in the loop would be considered high-risk, but not the use of software that helps to optimise logistics or data management after results are checked by a human. Further, when evaluating high risks for society and fundamental rights, other elements should play a role, such as the size of the company, their ability to access and combine to data from different sources, that can cause harm to fundamental rights of individuals and pose a risk for society overall. Further, some experts advise to apply more stringent criteria to ´deep fakes´, especially since ´deep fakes´ can form a high risk for society if used in the context of misinformation. In addition, experts pointed out that systems mentioned under recital 38 (tax, customs) and section 1.2 (legacy systems in freedom, security, justice) are excluded, while they pose more fundamental risks to citizens.

4. Conformity assessments & compliance costs will be prohibitive for SMEs.

A regulation that requires SMEs to make significant investments for conformity assessment and compliance will likely push them out of the market. This is exactly the opposite of the intention to support a thriving and innovative AI ecosystem in Europe.

For example:
The compliance costs for SMEs that develop or deploy high-risk AI applications are estimated at around 6k – 7k€ according to the EC Impact Assessment[6], with the conformity assessment estimated at 3.5k€ to 7.5k€ [7] , which, leaves us at about 9.5k€ to 14.5k€ of total estimated costs. However, this calculation excludes likely spendings such as external consultancy + internal 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 by a substantial factor. For instance, setting up a new Quality Management System is estimated to cost between 193,000 — 330,000 EUR[8]. In addition, costs arising from the need to regularly update products and renew certification are missing from the equation.

Flaw in this approach: *It risks limiting innovation and competitiveness.*
It will be important to address unwanted consequences and the additional burden stemming from the AI Act for SMEs, as additional costs may likely act as a barrier for investing in the development of AI systems and subsequently hurt EU competitiveness in the long term.

Our proposal: *Adapt compliance process and cost to match SMEs operations.*
As DIGITAL SME, we would like to ask the co-legislators to ensure that SME competitiveness and their innovation-potential remain centre stage. A highly regulated environment, and mandatory conformity assessments, may benefit larger companies and organisations that issue conformity assessments, but

[6] 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
[7] Ibid. p. 69
[8] https://www.ceps.eu/clarifying-the-costs-for-the-eus-ai-act/

strongly limit smaller companies. Proposal 1: If the regulator decided to proceed with the approach taken in this piece of legislation, special provisions for SMEs should be included such as free of charge support (i.e., AI certification advisors) to ensure compliance should be made available to SMEs, awareness raising activities, specialised training, and support programmes, European DIH support programmes to SMEs, among others. Proposal 2: However, we strongly recommend reconsidering this approach altogether.

5. While standardisation will play a key role in the AI Act, SMEs are largely under-represented in key institutions.

Conformity assessments will be based on standards, but SMEs are often not included in the standards-setting as they are under-represented in standardisation organisations. Oftentimes, this leads to standards which are written in a way that is non-practical, prohibitively expensive, and not applicable for SMEs. As standards are usually behind pay-walls, SMEs have no means of assessing them, checking them for suitability, and to develop pathways towards adoption.

For example: *Even widely recognised standards are not applied in practice.*
For example, in the area of cybersecurity, Common Criteria schemes are only applied to about 1500 products worldwide[9]. The most wide-spread and popular ISO/IEC 27001 certificates have been issued 32,000[10] times worldwide, although adoption is rising (figures from 2017). However, there are about 25 million SMEs in the EU, and about 190 million companies worldwide, which shows that the adoption rate of well-recognised schemes and standards is very low. Also, even essential standards are hidden behind pay-walls.

Our proposal: *Strengthen SMEs' participation in standardisation processes, including AI standardisation, and access to standards.*
1) Active participation in standards-setting: We strongly advise that standards should be written with the active participation of SMEs (ensuring an inclusive approach), and to avoid a "one-size-fits-all" approach, often defined and adopted by research organisations, large companies, and legal and ethical experts. 2) *Accessibility of standards*: Standards should be openly accessible without any pay-wall, and a tiered approach to certification against standards would be advisable (e.g., the UK's Cyber Essentials are a good example of a low threshold approach, accompanied by a "readiness" assessment tool)[11]. This is especially important for start-ups, which may not focus on ensuring process-based standards-compliance, but rather focus on developing their product and idea before considering other aspects.

6. The concepts of liability and "placing on the market" do not to reflect how AI products are developed.

Given the complex nature of AI solutions, 3rd party developers are often involved in developing solutions for deployers (B2B customers) who ultimately provide the technology to their end users (internally or externally). Moreover, 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

[9] https://www.commoncriteriaportal.org/products/
[10] https://www.itgovernance.co.uk/blog/iso-27001-certification-figures-increase-by-20

(e.g., when still in a Proof-of-Concept stage), costs of experimentation could increase significantly, hindering innovation.

For example: *Unclear liability for software developers and final users.*

AI software today is often developed based on academic and open-source software (OSS). The openness in AI-related coding is a fundamental driver of AI-innovation. 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".

For instance, a business develops a natural language processing API to de-gender job adverts. They build this solution using training data that's available to them. Developers then integrate the API into HR SaaS platforms and other solutions. The B2B customers then using the feature, would expect the liability for the feature to be with the HR SaaS developers, whilst the developers would seek follow on claims against the NLP solution creators. Other examples may include multiple entry points on the market for AI development (ex. OSS, but also more complex supply chains). Further points of discussion are data collection and processing of data and how these approaches will be combined with GDPR and Data Act.

Our proposal: Increase legal clarity around responsibility (e.g. on complying with the regulation, e.g. who has to do the monitoring of a solution, etc.), liability and "placing on the market" for developers and deployers, in addition to the current roles mentioned in the proposal such as Users and Providers, and ensure that innovative and open development processes are not limited.

7. Ensure sandboxes address the needs of SMEs.

While the current proposal foresees sandboxes, those are not mandatory. Sandboxes can help innovative companies to try out their solutions without risking infringing legislation. Sandboxes are therefore very important to ensure that companies will experiment with AI. However, even beyond sandboxes, SMEs may require additional support that can help them comply with the requirements of the AI Act. In additional, sandboxes are not necessarily adequate for each part of the supply chain. Different tools, such as, e.g., questionnaires, may be needed to allow for different AI solutions according to the level of AI development.

For example:
The set-up of the AI Act is highly complex as it refers to the existing New Legislative Framework. More guidance is needed for providers to be able to classify AI systems in practice. The ability to determine the risk class of a product or part of a product will have an impact on whether companies have to undergo conformity assessment. AI systems rarely have the exact same application as described on paper, making it difficult for providers, esp. for SMEs without access to a team of in-house lawyers, to determine if an application would be considered high risk or not. For example, the current regulation would apply to machinery products or medical products. If one component of the product was to rely on software that may feature some AI-based software (according to the definition, including ML techniques or some statistical analysis), the product would have to undergo conformity assessment also with regards to meeting the requirements formulated in the AI Act.

Our proposal: *Set up facilities to allow SMEs confirm the classification of specific use cases.*
Clear criteria and a possibility to officially confirm the classification of specific use cases should be set up for SMEs via the sandboxes. SMEs should have the possibility to be advised on whether the product

they are developing, potentially as a component of a product, would fall under the Regulation, and who would be responsible for ensuring conformity, and at what stage of the development process. This could be a service offered free of charge 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.

Further detailed comments, e.g. about aspects related to *data quality*, are available in DIGITAL SME's Position Paper on the AI Act.

About DIGITAL SME

The 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.

Why this fact sheet?

The European DIGITAL SME Alliance welcomes a European approach to regulating Artificial Intelligence (AI). For instance, a harmonised approach can help provide more opportunities for SMEs to scale and the EU's vision for ethical AI may be able to set Europe apart in global competition. Yet, 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.

For questions about this Fact Sheet, please contact:

Ms. Annika Linck
Policy Director
a.linck@digitalsme.eu