BSA RECOMMENDATIONS ON THE EU ARTIFICIAL INTELLIGENCE ACT

BSA | The Software Alliance ("BSA")[1] welcomes the opportunity to offer thoughts on the European Commission draft Artificial Intelligence Act (hereinafter the "AI Act" or the "Proposal"). BSA is the leading advocate for the global software industry before governments and in the international marketplace. Our members are at the forefront of software-enabled innovation that is fueling global economic growth, including cloud computing and AI products and services. BSA members include many of the world's leading suppliers of software, hardware, and online services to organizations of all sizes and across all industries and sectors. As leaders in AI development, BSA members have unique insights into both the tremendous potential that AI holds to address a variety of social challenges and the governmental policies that can best support the responsible use of AI and ensure continued innovation.

BSA supports the intention to structure the AI Act under a risk-based approach, and we strongly recommend that the EU co-legislators ensure that this approach is reflected in the final version of the AI Act. To this end, BSA would like to submit four recommendations to ensure that the proposal improves on and clarifies certain aspects that may limit this achievement.

- Clarify and refine the scope and definitions of the proposal
- Ensure that the obligations for AI providers and users are outcome and process-based and reflect the nature of AI as a service
- Allocate responsibility between AI providers and users in a manner that reflects the diverse AI ecosystem and ensures legal certainty
- Design a governance and enforcement system that fosters AI accountability without unduly burdening innovation

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry. Its members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernize and grow. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. Follow BSA at @BSAnews.
BSA's members include: Adobe, Akamai, Atlassian, Autodesk, Bentley Systems, BlackBerry, Box, Cloudflare, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, and Zoom.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

CLARIFY AND REFINE THE SCOPE AND DEFINITIONS OF THE PROPOSAL

In order to provide additional clarity on the AI that would be in the scope of the proposal, BSA recommends refining the definition of "Artificial Intelligence." **BSA recommends that the definition of AI aims more at ensuring its focus on software and processes commonly considered as AI, rather than risking encompassing those that would not constitute AI for the purposes of the Regulation, by further focusing the language provided for by Art. 3(1) and Annex I**. For example, some of the processes included in letters b) and c) of Annex I may include software that is not always classified as AI. Software and tools that are not AI, but that are used in the development of AI, should not captured by the definition of AI. The language in Art. 3(1) and Annex I should be modified to clarify that only software that is genuinely AI fits in the definition, to ensure that the Regulation achieves its objective of providing legal certainty for high-risk scenarios, without including other processes that are not traditionally considered AI.

BSA recommends reviewing some of the definitions of high-risk activities that would include AI in the scope of the proposal (i.e. Annex III), which may lead to including very broad sectoral services in the scope of the Regulation. Moreover, we urge the co-legislators to review the list of Annex III, taking into consideration the narrower requirements provided for by Art. 7(2), which explicitly mandate an in-depth analysis of the specific AI system, the sector of placement and a thorough risk-assessment before inclusion in Annex III. As provided under Article 7(2), the potential that the system has already caused harm to health and safety or adverse impact on fundamental rights should be a guiding criterion. As the AI Act seeks to regulate high-risk scenarios, and not sectors, it is fundamental to ensure that specific scenarios within a sector are clearly defined and delimited. In particular, the current definition of Employment, workers management and access to self-employment[2] would encompass a number of services that are not normally considered high-risk or would not be considered a concern for the public or customers. The current definition may be more sector than scenario-focused, as it would encompass many scenarios in the "employment sector" that would not pose particular concerns for fundamental rights (e.g. AI used for 'Task allocation' under the Employment section could be AI used for the routing of phone calls, predictive behavioral routing, which does not present any risks to human health or fundamental rights).

BSA also recommends that the involvement of industry stakeholders in the review of the Annexes to the proposal is sufficiently broad, to ensure that changes to the Annexes are informed by the most updated best practices and state of the art of AI research and development. In this context, BSA urges the co-legislators to include a review process of the Delegated Acts that would broaden the Annexes of the Act that involves all stakeholders.

[2] Annex III(4) of the AI Act.

ENSURE THAT THE OBLIGATIONS FOR AI PROVIDERS AND USERS ARE OUTCOME AND PROCESS-BASED AND REFLECT THE NATURE OF AI AS A SERVICE

BSA recommends providing for obligations on AI development that are more process and transparency-oriented, rather than a rigid set of requirements that may create obligations that are impossible to fulfil (e.g. mandating "datasets free of errors and complete", [3] requiring the establishment of human oversight that enables the user to "fully understand the capacities and limitations of the AI system"[4]) and may involve tradeoffs with the objectives of fostering AI uptake and protecting citizens.

The proposal seeks to establish a common set of safeguards for two categories of AI that are fundamentally distinct: (1) AI systems that are high-risk in the context of safety and health and (2) AI systems that are high-risk from the perspective of safeguarding fundamental rights. Using the same requirements and market surveillance designed for product safety may not result in the protection of those rights. The distinct nature of the risks involves design and development choices of AI systems and is more dependent on the specific use. Thus, will also most likely affect the effectiveness of any conformity assessment. **BSA recommends fine-tuning the language in the obligations for AI Providers provided for by Chapter 2 of the AI Act, to ensure that the requirements reflect more the process of developing and perfecting a service such as AI, rather than a traditional product placed on the EU market.** As a way of example, the wording of Article 10(3) on Data Governance and Article 14(4) on Human Oversight would be more effective and technologically neutral if focused more on process and outcome. Moreover, several of these requirements are still topics of active research and concrete approaches for achieving these requirements might not be available depending on the specific AI technique. For example the use of the term 'state of the art' in the Proposal without any further clarification could prove problematic, as in a field which evolves as rapidly as AI does, there are many open debates about best solutions, which can change very over time.

In the context of AI that falls under Art. 6(1), the Proposal refers to the concept of "safety component" in the determination of the level of risk of an AI system. The proposed definition of what constitutes a "safety component" is and remains a source of uncertainty for the qualification of high-risk AI systems. To reduce this ambiguity, **it is important that the assessment of a "safety component" refers back to Union harmonized legislation to align with any relevant essential requirements**. In other words, that when assessing an AI system for the purposes of Article 6(1), a safety component is to be understood in the meaning of the relevant Union harmonization legislation listed in Annex II. The Proposal could clearly set out that AI requirements for "safety components" will refer back to Union harmonized legislation, whereas requirements for high-risk systems listed under Annex III are listed in the AI Act itself.

[3] Art. 10(3) of the AI Act.
[4] Art. 14(4)(a) of the AI Act.

BSA is strongly supportive of the decision to allow for self-assessment in most cases, as it ensures the ability for AI Providers to comply with the relevant obligations throughout the design and development process. To this end, it is important to note that the current definitions are not specific on the kinds of risk that must be considered for purposes of complying with the Article 9 requirement to maintain an appropriate "risk management system." As the type of risks can be manyfold (e.g. financial risks, risk of delays in development) and many of them are not relevant for this Proposal, a specific definition of the risks that have to be considered by this risk management system should be added. It would also beneficial to include additional language in Art. 9(2)(a) to reflect the need for more specificity for the risk-management obligations, by directly referring to the foreseeable risk *to the health and safety or fundamental rights of persons* associated with each high-risk AI system.

BSA also recommends ensuring that the AI Act obligations do not overlap with other EU legislation, in particular as they may create competing compliance requirements. For example, we recommend adding an explicit lawful basis in the body of the proposal for the processing of special categories of personal data under GDPR for bias monitoring of AI systems and datasets.

ALLOCATE RESPONSIBILITY BETWEEN AI PROVIDERS AND USERS IN A MANNER THAT REFLECTS THE DIVERSE AI ECOSYSTEM AND ENSURES LEGAL CERTAINTY

The European Commission's AI White Paper correctly stated that legal requirements for high-risk AI applications "should be addressed to the actor[s] who is [are] best placed to address any potential risks".[5] BSA recommends that this principle should be more explicitly reflected in the final version of the proposal. As currently drafted, the AI Act creates uncertainty about what actor will bear responsibility for complying with key legal requirements in many circumstances. This is especially true where an AI developer would make available a general-purpose AI system that can be used in a variety of contexts, and potentially customized by an AI deployer in a manner that would transform it into a high-risk system. In such circumstances AI developers will not be in the position to know whether the technology is being deployed by an end-user in a manner that meets the definition of high-risk.

The regulatory requirements for the various entities responsible for designing, developing and deploying AI should account for the unique roles and capabilities of the entities that may be involved in an AI system's supply chain. Any obligation (and associated liabilities) should fall on the entity that is best positioned to both identify and efficiently mitigate the risk of harm that gave rise to the need for a regulation. We continue to support an AI legislation that promotes accountability for both AI developers and deployers, as each entity in the design, development and deployment of AI should have clear responsibilities and obligations.

[5] European Commission White Paper on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65

In this context, while BSA is strongly supportive of creating different obligations for AI Providers and AI Users, we would caution that the current formulation of Article 28 may not clearly assign appropriate roles and responsibilities in the event of actions taken by one stakeholder in the value chain.[6]

We advise to establish a clearer distinction and corresponding obligations between deployers of AI system and developers of AI systems, to ensure the necessary clarity and proportionality with regards to the obligations for risk management of AI. **The guiding principle should be that the entity that determines the purposes and means by which an underlying model is trained and/or used should bear greatest responsibility for ensuring compliance with the AI Act**. The Act currently focuses more extensively on the responsibilities of AI Providers (commonly referred to as developers) and less on AI Users (commonly refer to as deployers) [7]. BSA recommends ensuring that the deployers/users are further included in the management of risks stemming from AI, and the related obligations. Furthermore, it is important to consider that - especially in the B2B space – AI is often developed to the specifics of the customer needs (who is almost always the User), and therefore the responsibilities on how it is deployed are not exclusive to the developer. Additionally, BSA recommends including a definition that distinguishes more clearly between users as deployers and users as individual end users (which is often the case in the B2B space), which would be a fundamental step in ensuring that all entities involved in the AI deployment phase receive clear and proportionate obligations.

The uncertainty on allocation of responsibilities is particularly important in the case of so-called general purpose AI (i.e. an AI that is not developed for a single specific purpose or sector in mind, but which instead is designed to be versatile and give customers the chance to innovate), which would not be clearly covered by the abovementioned Art. 28. In many cases, such AI is developed before knowing its market placement, and **BSA recommends ensuring that the AI Act obligations would be assigned to the user that may place the general purpose AI in a high-risk use**. Currently, the proposal seems to require AI developers developing general purpose AI to either comply with all the requirements of the Act, regardless of whether the AI may classify as high-risk, or to contractually bind AI users not to place it in a sector covered by the Act. Moreover, it is unclear whether an AI developer who offers general-purpose AI system could become retroactively subject to the obligations for high risk systems in the event that their customer integrates the technology into a high-risk use case. In this context, we would **recommend clarifying that an AI developer of a general purpose AI is not considered an AI Provider as per the definition of the AI Act**, as the AI is not developed originally and specifically for deployment in a high-risk scenario. In this context, the deployer would be considered the AI Provider once the AI is deployed in a high-risk scenario as defined by the AI Act. Recital 60 of the Proposal indicates that Providers need to cooperate with Users to support them in their compliance efforts, which seems to imply that when a User develops a general purpose tool into an AI system for a high-risk intended use, it is up to the User to comply with the requirements for high-risk systems – as it would be considered a Provider as per the Proposal. The articles of the AI Act

[6] We would suggest to consider adapting the language to the commonly used terms, so that no confusion occurs. It is common to speak about AI 'models', i.e., individual models typically performing a single function, and an AI 'system', describing a broader system that may comprise multiple models and other processes. Customers may integrate text analytics models as part of a customer management system that the customer assembles and deploys. Suppliers of such AI models are merely mentioned in recital 60. Deployers of AI are those that 'use' individual AI models directly and those combining them to build broader AI systems. We believe the term 'deployer' better reflects the decisive role that this entity plays in choosing the intended use and wider context into which a model or system is deployed.

[7] BSA Policy Paper "AI for Europe", please find it at AI for Europe (bsa.org)

should mention this clearly and be more explicit regarding this allocation of responsibilities when it comes to general purpose tools.

For these reasons, BSA recommends including an additional category in Art. 28 to address instances in which an AI user or other third party uses, trains or modifies a general-purpose AI system in a manner that would render it a high-risk AI system. In such circumstances, the user or other third-parties should be considered the AI Provider under the Act. This should include also the further training of an existing AI system, and when a user or third-party develops AI off of general purpose tools or APIs. As mentioned above, **the guiding principle for compliance obligations with the legislation should be the identification of who is defining the actual intended purpose of the AI system and who determines its parameters**. Also, third parties, and notably the ones involved in the sale and the supply of software, software tools and components, pre-trained models and data, or providers of network services should not be considered Providers for the purposes of this Regulation.

Additionally, BSA recommends clarifying the obligations for AI that is not currently in the scope of the proposal, but may be included following the review process competence granted to the Commission. In such cases, we advise the EU co-legislators to include time-periods for "new" AI included in the scope of the Act to ensure that AI Providers and Users are able to comply properly with the obligations of the Act. It is also important to clarify the threshold for AI to have to be requalified and reassessed after system updates.

DESIGN A GOVERNANCE AND ENFORCEMENT SYSTEM THAT FOSTERS AI ACCOUNTABILITY WITHOUT UNDULY BURDENING INNOVATION

BSA is strongly supportive of a cohesive and efficient system of governance and enforcement of AI. The AI Act includes very diverse sectors in its scope, and would involve several market surveillance authorities and enforcement bodies and agencies. **BSA recommends ensuring that the competences and powers of each body remain proportional and clearly defined**. In particular, it is important to ensure that overlapping competences between different authorities are avoided, so that compliant AI Providers and Users have a clear understanding of which body is competent for their activity. In this context, it is important to note that each Member State has an accreditation body referred to in Regulation (EC) No 765/2008. These organizations are well defined and governed. The accreditation bodies are an essential pillar of the market surveillance and conformity assessment system of the European Union. We recommend designating the national accreditation bodies as the notifying authorities. Such an action will discourage the fragmentation of certifications which may result in country-specific requirements that can become barriers to trade between Member States especially for small or medium-size enterprises.

BSA would caution against applying purely product safety principles to AI, which is much more akin to a service. In the context of enforcement, there is a risk of severe market fragmentation depending on how Member States will allocate competences, in addition to the significant possibility that different authorities, sometimes cross-border, will have overlapping competences which would not be easily solved – and would hinge on a first-come-first-judge basis whereby there would be a rush

for authorities to establish as broad competences as possible, oftentimes with extraterritorial effects.

BSA would strongly caution against including the possibility to access source code of AI. The AI Act currently provides for rather broad powers for market surveillance authorities to request access, and does not clarify how companies may seek remedies, or how such requests would be issued and justified by the issuing body, and possibly reviewed by the competent judiciary authorities.

BSA is strongly supportive of the Commission's intention to support the creation of Codes of Conduct related to the obligations stemming from the AI Act, and of the current objective of establishing an Expert Group for monitoring and guiding the implementation and enforcement of the Act. In this context, we would suggest ensuring broad inclusion of diverse stakeholders, building upon and broadening the membership of the High-Level Expert Group on AI. Moreover, BSA strongly recommends including the abovementioned Expert Group in the EU AI Board, to ensure full representation of all AI stakeholders in the deliberations of the Board. The AI Act should include a provision to that purpose.

For further information, please contact:

Matteo Quattrocchi,
Senior Manager, Policy – EMEA
matteoq@bsa.org