

## Consultation response

# AmCham EU's response to the White Paper on Artificial Intelligence

Supporting document to the public consultation launched by the European Commission



AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and U.S. positions on business matters. Aggregate U.S. investment in Europe totalled more than €3 trillion in 2019, directly supports more than 4.8 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

## Introduction

There is no doubt that artificial intelligence (AI) will transform every aspect of our society and economy, and in many ways, it already has. AI is commonly used in our daily actions with features that make our lives safer, more convenient and productive. Digital technologies improve connectivity in rural areas, support environmental sustainability and peoples' health, safety, mobility and overall quality of life. Breakthroughs in areas such as vision, speech, translation and knowledge sharing, have all proven AI is a transformative technology that has unprecedented potential.

Currently, we find ourselves in the context of a global health crisis. The COVID-19 pandemic has presented an uncertain international environment. The immediate priority has been, and remains, to tackle this health emergency. However, as we look to move forward, we will need to balance health responses with the broader social and economic aftershocks of the crisis. New challenges will emerge and the road to the economic recovery will be long as we lay the foundations for what is to come next.

We believe that the digital sector is playing, and will continue to play, a crucial role for both the health and economic recovery strategies. Technology, especially AI, underpins critical products and services that global communities, governments and healthcare organisations depend on every day. It has played a vital role in helping tackle the health crisis, but it has also meant more businesses across the EU have embraced technologies, including AI, as a means of adapting and injecting more digital resilience into their business models. Trusted technological solutions have enabled us to sustain social, economic, healthcare and educational interactions, as well as information flow and research. Now, the forward-looking digitisation of industries and public services can not only help return us to what we had, but also build a new, more resilient and sustainable economy.

AmCham EU was pleased to see the approach taken by the Commission in their White Paper proposing a risk-based, use case specific approach focused on high-risk AI applications. Therefore, we look forward to providing our detailed contribution to this public consultation. We believe Europe has a unique opportunity to become a global leader in AI, and that industry has a crucial role in promoting its responsible development. AI developments will and can help to solve some of society's most pressing challenges, which is why it is important we advance innovation while simultaneously building trust in technological advancements that work for people.

The ambition in forthcoming legislature should be to facilitate the uptake of AI development and to increase research funds, public-private partnerships, skills and education, and to leverage technological innovations that make positive changes and accelerate global capabilities. Strong cooperation between government, business and civil society will be essential. The EU and the US will remain important partners in setting global standards, and AmCham EU and our member companies stand ready to do our part.

## 1. Ecosystem of excellence

AmCham EU supports the Commission's view that AI can flourish in Europe if the right conditions are in place, both through an 'ecosystem of excellence' to strengthen the foundations of the AI market, and an 'ecosystem of trust' to accelerate the responsible production and the adoption of AI in Europe. In our view, the ultimate objective in building an ecosystem for AI in Europe is to stimulate demand and promote the development and uptake of responsible AI solutions by the private and public sectors.

Regarding the 'ecosystem of excellence', the Commission has identified the right priorities in its White Paper: investing in research and innovation programmes, upskilling and reskilling the workforce, coordinating national initiatives, fostering adoption by both the public and private sectors and building strong public-private partnerships are essential elements of this ecosystem. We would also highlight the need for an inclusive adoption of AI so that small and medium-sized enterprises (SMEs) and public services in disadvantaged areas can also overcome barriers to access these technologies.

Out of all the priorities we would like to particularly highlight:

- The need for enabling a strong involvement of the private sector in building the ecosystem of excellence. Participation in public-private partnerships should be open to all companies regardless of the location of their headquarters. Rather than making a company's origins a criterion, we believe that participation should indeed be open to all actors which can provide technical capabilities, and which comply with European regulations and values;
- The importance of significant investments in education, life-long learning and reskilling to ensure our workforce is ready for the jobs of tomorrow. Vocational training and apprenticeships will continue to play their role, but we also need to better align education with in-demand skills like science, technology, engineering and mathematics (STEM) skills and competences. AI will require multi-disciplinary skills, which will require the development of systems for workers to signal their applied skills beyond classic education institutions;
- The need to build technical expertise within public institutions and oversight bodies, to ensure civil servants are familiar with the technology and its implications, and that anyone using AI systems to provide public services is fully and regularly trained. The public sector faces many challenges in adopting AI (eg, antiquated internal processes – administrative and organisational, heavy reliance on physical paper, poor digital infrastructure, siloed IT applications, lack of interoperability and poor user experience with digital public services). Existing EU funding streams, such as the European Regional Development Fund (ERDF), the Cohesion Fund (CF) and the Digital Europe Programme should be used to address these challenges. A follow-up to the Tallinn Ministerial Declaration on eGovernment should also be envisaged to increase the exchange of good practices among governments;
- It is fundamental to make non-sensitive public sector data available for research to boost data available for training AI systems, as well as to support the creation of AI ecosystems and public-private partnerships; and
- The need to build on existing research organisation and to promote multidisciplinary and cross domain collaborations.

## 2. Ecosystem of trust

### Risk-based approach

We have long called for a risk-based approach to AI regulation and fully support the view that AI legislation must be targeted and focused on problems which are not already covered by existing legislation. We therefore agree with the Commission that any additional regulation should be focused on high-risk applications, which arguably would be those applications endangering safety. Potential risks to user safety are indeed the key concern, which could justify regulatory intervention. As for some of the other concerns identified by the Commission, these are either already covered by existing legislation (eg, privacy, fundamental rights, liability), or do not seem as relevant (eg, 'AI is not always accurate'). If companies must strive to mitigate inaccuracy, there is no such thing as a technology or human that is always 100% accurate.

We would suggest to the Commission to undertake a thorough analysis of existing legislation (including sectoral legislation) that is applicable to AI, before introducing new legislation. It would be helpful to all stakeholders involved (eg, researchers, SMEs, businesses, individual users) to have a 'body' of AI law at their disposal to clarify compliance. It will also make it easier for the Commission to positively and confidently identify the gaps in legislation it needs to address. Finally, in order to avoid over-regulation, we would encourage the Commission to propose a narrow definition of AI systems which would focus strictly on AI high-risk applications (and not expand to AI applications other than high-risk, or software in general). AI policies should define AI in a way that avoids legal uncertainty, fragmentation and an uneven playing field. Regular knowledge-sharing of what AI is and is not between policymakers, industry, and academia is required to ensure AI policies define it clearly and consistently.

## Ethics and trust

It is also important that we build trust between society and technology, as an understanding of technologies will be necessary for them to be accepted, trusted and used by citizens. Initiatives should be developed which aim at mitigating the risks of unethical use of AI.

## Risk assessments

Although we are generally supportive of the 2-level risk-based approach (low/high risk), we would recommend some adjustments to ensure regulation is proportionate, targeted, and provides legal certainty.

Any risk assessment (or indeed rules/prohibitions) must take account of the context when assessing risk since an AI application used for the same purpose will pose different risks depending on the way it is integrated into business operations. The focus should always be on the specific use case, not on the broad class of application or technology. As such, risk assessments must reflect the probability of harm and not just the severity of harm. Therefore, we recommend developing both a risk grading system and the list of possible requirements for high-risk applications together with experts and the private sector based on quantifiable and predictable risks.

The 'exceptional instances' clause to classify entire sectors as high-risk is too open-ended and creates legal uncertainty. Also, the reference to 'immaterial damages' in the risk definition is vague (and not an established legal concept) and the spirit behind it is already covered by other laws (eg, data protection, non-discrimination, freedom of expression). It would be far better to align it with the phrasing of the Product Liability Directive, which defines damage as death, personal injury or damage to property.

AmCham EU members are investing significant efforts in the mitigation of bias in AI so as to reduce discrimination. The quality of training data and using sufficiently representative data sets are important elements in creating and using AI in a responsible and ethical way, understanding the difficulty in obtaining perfectly representative data sets and ensuring it is completely free from any bias. The Commission should encourage companies to strive for high data quality and bias mitigation by making reasonable efforts, rather than imposing overly prescriptive requirements based on unattainable objectives. The emphasis should be on testing output, not on training data quality. Rather than putting requirements on training data, it would be better to have requirements based on testing model performance using benchmark data sets, to make sure that the outputs are within an acceptable range, since it is the model output that ultimately determines the real-world impact of an AI system.

Stringent requirements on AI applications that are trained on 'European data' could lead to lower quality AI outcomes. While the stage of training AI with data is important, simply focussing on the origin of the data and not what it creates as a result of that data is illogical. AI systems that are not trained on universal data, but only on 'European data', risk delivering outcomes that are skewed and take a form of bias that is unwanted. Non-European data could bring different results when compared to European data, due to behaviours, habits, cultures or conditions, and this should not mean that it will be non-compliant with Member State or EU law (eg, GDPR). Therefore 'complete data sets', rather than data sets with only pre-selected European data as the training fuel for AI-systems, ultimately yield more comprehensive outcomes.

Furthermore, data flows from one location to another in a heartbeat. It is extremely complex to allocate one specific geography to data or a particular data set. Often enough data sets are a mix of data coming from various geographies. It would be overly burdensome for businesses to filter out non-European data from the data sets they use to (re)train their AI applications.

Minimising the potential for businesses in Europe to choose different data sets around the globe or force them to 'retrain' AI systems on European data would actually be self-defeating and risk greater discrimination and produce lower quality AI outcomes. If we want to foster greater trust, it is crucial that AI in Europe is trained in accordance with quality standards and that the outcomes are the focus of regulation.

Finally, there is no ‘one-size-fits-all’ approach to ensuring safety, robustness and accuracy of AI systems. It is important to retain flexibility in the legal interpretation and to collaborate with practitioners to draft rules that are workable from a technical perspective.

### **Biometric identification systems**

Biometric identification systems should be allowed, but guidance is needed to give people confidence in them. Requirements for remote biometric identification systems should follow the Commission’s risk-based approach, with specific requirements applying only to high risk applications. We would welcome further consultation with industry on this point.

### **Voluntary labelling**

A label might be helpful to increase trust in AI systems, however at this stage the proposal is vague and it is difficult to see how this would be implemented in the near-term. The proposal raises a lot of questions: which authority would assess and issue the labels? What would happen in case a low-risk AI application presents problems after obtaining the label? Would it create de facto blanket conformity requirements for all AI systems? The suggestion to use the High-Level Expert Group (HLEG) self-assessment could be a first step, although it needs to be shortened and made more practical for companies to use. Overall, a lot more work needs to be done in a multi-stakeholder setting to get to a place where all parties feel confident about labelling.

### **Conformity assessment and compliance**

We would support a combination of ex-ante self-assessment by entities using high-risk applications, followed by ex-post market surveillance. Ex-ante conformity assessment models can hold back innovation from reaching the market and add a huge amount of burden to businesses such as delays and red tape, which would deter companies, in particular SMEs, from developing and launching new services in Europe. A more balanced approach is to make the expectations clear for risk assessment processes, and allow for self-checking prior to launch, with ex-post investigations carried out where problems are suspected. Some lessons can be learned from self-assessments in regulated industries such as in the area of medical equipment.

### **Governance**

It is essential for the governance framework to enforce any future rules on AI in a coordinated, harmonised and simple way. In order to achieve this objective, we strongly recommend further consultation with the private sector regarding the establishment of the governance framework. We tend to think that, and as is the case in highly regulated sectors such as medicines, air transport and financial services, the existing regulatory bodies are best placed to make ex-post conformity assessments.

## **3. Liability and safety**

The use of AI systems, and therefore any resulting liability, is context-specific. Therefore, the focus of risk should lie on a specific application and the context of its use. There is often a complex chain of various producers and intermediaries involved, for example, various producers (eg, software developers, hardware, component or end-product manufacturers who embed the software in their products), back-end operators (who train the AI system) and front-end operators using the system. This is why having more than a single operator who is liable or introducing joint liability would not be workable, and it would not make sense for anyone involved in making an AI system to be liable for problems they had no awareness of or influence over.

In a business-to-business (B2B) context, contractual liability is working well as parties can negotiate for a more efficient allocation of risk which consider each specific context and use. It is impossible to define a general and holistic liability regime applicable to AI technologies, and we strongly advise against the aim to assign liability via a regulatory framework and suggest leaving such issues to contractual arrangements. Any changes to the liability framework should be consistent with the scope of the Product Liability Directive.

We disagree with the idea of expanding the definition of ‘product’ in the Product Liability Directive to include software. One could wonder in what cases stand-alone software would result in property damage, bodily injury or death. Usually, this will be caused by hardware or by the use of the software by a human being. Generally

speaking, services will still require a physical infrastructure in their execution, therefore physical products remain the basis for the guidance and application of the Directive. In most cases the relationship between provider and end-user is covered by a contractual relationship, while services that are inherently dangerous or pose specific risks are already regulated and subject to insurance (eg, healthcare or legal services).