# AIOTI Additional Input to the Consultation on the White Paper on Artificial Intelligence - A European Approach

## Section 1 - An ecosystem of excellence

### 1.1 In your opinion, how important are the six actions proposed in section 4 of the White Paper on AI (1-5: 1 is not important at all, 5 is very important)?

### 1.2 Are there other actions that should be considered?

*Development of industrial AI must by design be strongly intertwined with cybersecurity and brought into the context of cybersecurity in a horizontal approach. This is intended for trustworthy AI, whose critical protection level meets the product requirements with a strong focus towards responsible AI.*

*Algorithms need to be protected and encrypted according to the level of security determined by the criticality of the application. The appropriate incentives must be established throughout Europe, including funding common projects that require strong collaboration between cybersecurity expert players and AI developing/using companies.*

*It is equally important to ensure that the proposed legal framework for high-risk AI applications provides legally certain, fully harmonised, future-proof, implementable and enforceable rules. This includes the development of a clear definition of AI as well as of a clear assessment-method of high-risk applications The follow-up actions should be designed to ensure a truly functioning and competitive EU Single Market for AI, avoiding fragmentation by each Member States developing their own rules.*

Revising the Coordinated Plan on AI (Action 1)

### 1.3 In your opinion, how important is it in each of these areas to align policies and strengthen coordination as described in section 4.A of the White Paper (1-5: 1 is not important at all, 5 is very important)?

### 1.4 Are there other areas that that should be considered?

*We support EU activities to build European data spaces taking sector specific industrial use cases as a starting point for specific industrial sectors. EU led activities should take into account ongoing national developments to strengthen the EU activities. Data ecosystems, based on contracts between companies of how to access and use data, will be a vital part of a future European Industrial and Services Ecosystem, enabling a European Cloud Service and Data Economy and supporting the mass adoption of AI.*

*EU Digital Single Market remains the main EU asset to deliver an environment of excellence and trust. The follow-up actions should be designed to ensure a truly functioning and competitive EU Single Market for AI, designed to ensure a truly functioning and competitive EU Single Market for AI, avoiding fragmentation by each Member States developing their own rules.*

A united and strengthened research and innovation community striving for excellence

1.5 In your opinion how important are the three actions proposed in sections 4.B, 4.C and 4.E of the White Paper on AI (1-5: 1 is not important at all, 5 is very important)?

1.6 Are there any other actions to strengthen the research and innovation community that should be given a priority?

*Europe needs to place focused investments in industrial AI, based on a combination of a wide range of technologies, including Machine Learning, semantics, NLP, vision, combined with domain know-how, in those domains where Europe plays a leading role. Europe should establish combined structures to bring skills and stakeholders together, in form of clusters, that can generate global leading innovations to achieve appropriate progresses in research and innovation on industrial AI.*

*EU should also focus on the regulatory requirements concerning the safety and compliance of products using AI, machine learning and blockchain technology while the innovation community should initiate and create the necessary harmonized standards supporting each relevant category of machinery/products; we clearly see the benefits to build on the existing NLF and expand this regulatory framework to AI*

Focusing on Small and Medium Enterprises (SMEs)

In your opinion, how important are each of these tasks of the specialised Digital Innovation Hubs mentioned in section 4.D of the White Paper in relation to SMEs (1-5: 1 is not important at all, 5 is very important)?

Are there any other tasks that you consider important for specialised Digital Innovations Hubs?

*Specialised DIHs where SME's are enabled to develop and test their use cases, should focus on domains where Europe plays a leading role: combining connectivity, Security, hardware solutions, automation, semantics, edge computing, data analytics, explainable and data scarce AI, achieving to take the efficiency of industrial infrastructures (factories, power, transportation, etc.) to the next level, but also to give an answer to European societal challenges using the Digital Europe Program.*

Section 2 - An ecosystem of trust

Chapter 5 of the White Paper sets out options for a regulatory framework for AI.

2.1 In your opinion, how important are the following concerns about AI (1-5: 1 is not important at all, 5 is very important)?

2.2 Do you have any other concerns about AI that are not mentioned above? Please specify:

*AI algorithms for deep learning should be based on design and should include cybersecurity with a high priority to safeguard these algorithms according to the level of (cyber) security determination by the criticality of the application. "not always accurate" is not inherent to AI. It strongly depends on the specific technologies and applications, their development, their real technical advancement, deployment, and environment/context of AI use. Explainability will always be difficult ("black box") for complex, deep learning algorithms. We also note that a vast range of AI technologies do not pose any concern. This is why we support the approach to focus on the specific use of AI technologies - and not on AI technologies per se – as well as on high-risk applications.*

*It must be underlined that the concerns mentioned above are linked to the potential risks of AI in critical use cases. There are plenty of applications where AI does not raise any concern.*

2.3 Do you think that the concerns expressed above can be addressed by applicable EU legislation? If not, do you think that there should be specific new rules for AI systems?

Other, please specify

*We believe there is no need for totally new legislation of AI algorithms. Most industrial applications (up to 90%) do not need new regulation, because already sufficiently covered by existing one (GDPR, EU Machinery Directive). It is necessary to separate between the vertical markets, because "one-size-fits all" approach is not applicable and would benefit the European industries. The use of sandboxes to test new concepts (e.g. autonomous driving) within a delimited, regulation-flexible and innovation-friendly space supports these developments. Further the free flow of data and support for contract-based solutions for sharing B2B data as a general principle boosts the European industries in a positive way.*

*For high risk AI applications, we notice a fragmented approach, multiple and sometimes various policies and rules across Member States. This creates legal uncertainty and fragments the EU Single Market to develop and market AI technologies in Europe. This is not helping trustworthy, investment and innovation-friendly environment in the EU. Given applicable EU legislations as well as the need for Single Market, the EU regulatory framework should complement, and not overlap with, existing rules. This requires a careful analysis of regulatory gaps, the development of a clear definition of AI, as well as of a clear assessment-method of high-risk applications. In this context, we support the approach to introduce specific rules for specific uses.*

### 2.4 If you think that new rules are necessary for AI system, do you agree that the introduction of new compulsory requirements should be limited to high-risk applications (where the possible harm caused by the AI system is particularly high)?

Other, please specify:

*Vast range of AI technologies do not pose any concern and are well regulated by existing EU laws (e.g. GDPR). We agree that the introduction of new compulsory requirements should be limited to high-risk applications. Legal certainty and a transparent methodology to distinguish between high-risk and non high-risk AI application is essential.*

If you wish, please indicate the AI application or use that is most concerning ("high-risk") from your perspective:

*AI in IIoT applications where personal privacy or where life & limbs are at stake are critically evaluated in a case-by-case approach. The risk level must be objectively determined by the criticality of the application itself.*

### 2.6 In your opinion, how important are the following mandatory requirements of a possible future regulatory framework for AI (as section 5.D of the White Paper) (1-5: 1 is not important at all, 5 is very important)?

### 2.7 In addition to the existing EU legislation, in particular the data protection framework, including the General Data Protection Regulation and the Law Enforcement Directive, or, where relevant, the new possibly mandatory requirements foreseen above (see question above), do you think that the use of remote biometric identification systems (e.g. face recognition) and other technologies which may be used in public spaces need to be subject to further EU-level guidelines or regulation:

Please specify your answer:

*Existing policy framework and legislation (like GDPR) is sufficiently covering the use of biometric ID systems. Permanent human oversight of all AI activities is not needed, it depends on the criticality of the application; a clear definition of the objectives of the AI application by humans must be sufficient.*

*By complying with the future EU regulatory framework, we would expect remote biometric identification solutions would benefit from:*
- *Increased trust and acceptance by users, customers, and society at large;*
- *Legal certainty;*
- *A level playing-field to provide competitive and innovative solutions on the EU market.*
- *Market access to procurement contacts (e.g. border control management systems at airports).*

*No further requirements are necessary. However, we would welcome European Data Protection Board (EDPB) guidelines on video recording for data processors.*

### 2.9 Do you have any further suggestion on a voluntary labelling system?

*Voluntary labelling of an industrial AI application (in the B2B area) is not bringing any extra information and will only provoke an extra admin burden for companies (especially for SME's and startups). A B2B relationship is by definition based on trust between partners (supplier - user) and based on mutual contractual agreements (specifications) which should always be respected.*

*Any successful voluntary labelling system requires a trusted and sound governance, enforcement and public recognition. However, we question whether such label should only be available on compliance with high-risk requirements. Any future EU regulatory framework may want to refer to relevant widely accepted international standards.*

### 2.10 What is the best way to ensure that AI is trustworthy, secure and in respect of European values and rules?

Please specify any other enforcement system:

*Extensive exchanges with all stakeholders across the AI chain will be necessary to discuss further the appropriate compliance and enforcement mechanisms. Combination of ex-ante assessment & ex-post surveillance and enforcement mechanisms would be purposeful, in particular in light of the positive experiences with the EU product safety legislation following the so-called "New Legislative Framework / NLF". This will allow flexibility providing necessary measures depending on the subject. For high-risk applications, the evaluation of AI systems (incl. deep learning engines) for conformity assessment by 3rd party would need to be conducted with respect to:*

*- the intellectual property of the AI systems developer / integrator / vendor;*
*- cost efficiency - in today's highly competitive environment, market operators cannot suffer unjustified administrative burden, delays, and costs to introduce innovative AI solutions on the EU market;*
*- specific AI technologies deployed: 3rd party certification body must be selected on the basis of demonstrated knowledge and authority in its field.*

*For non high-risk applications, we think that AI systems should benefit from existing EU regulatory framework for conformity assessment of new products placed on the EU market.*

### 2.11 Do you have any further suggestion on the assessment of compliance?

*A trustworthy AI should be ensured by a combination of ex-ante compliance and ex-post enforcement with existing mechanisms of conformity assessments. Harmonized software defined safeguards can help to provide a balanced flexibility for AI deployment considering products and services. Industry would be in favour of a risk assessment against technical requirements set through harmonized standards.*

## Section 3 – Safety and liability implications of AI, IoT and robotics

### 3.2 In your opinion, are there any further risks to be expanded on to provide more legal certainty?

*In our view, the current EU product safety legislation (e.g. Low-voltage Directive, Machinery Directive, General Product Safety Directive,) is so- called "total-safety" legislation and covers all risk that arise or can arise from covered products and related technology. There is no need to expand on further risks in the text of the Directive. Clarification of aspects such as relating to risk coverage or safety concepts should be done through guidelines, where necessary. from an industry perspective we support the expansion of the NLF to AI through a revision of the Machinery Directive to include AI covering the essential requirements for health and safety while all machine specifics should be covered through a harmonized standard for each corresponding product platform.*

### 3.4 Do you have any further considerations regarding risk assessment procedures?

*The risk assessment process and the principles of safety integration for risk mitigation according to the EU legislation on CE marking have proved their effectiveness and have been successfully implemented. Today almost all industrial sectors carry out risk assessment and implement risk reduction measures according to processes that were required by the safety legislation. Therefore, the iterative process of risk assessment and risk reduction measures does not need further considerations for AI.*

*When the scope of the AI application changes, like a new purpose, the risk assessment should be re-assessed. This should be considered within the life-cycle of AI applications to ensure they are out-of-scope of the risk assessment procedure and this helps innovation.*

*In the machinery directive, for instance, AI-induced changes are already covered by the concept of "substantial change". Whether or not a change is based on AI is irrelevant. The conformity assessment procedures are suitable.*

### 3.7 Do you think that the current national liability rules should be adapted for the operation of AI to better ensure proper compensation for damage and a fair allocation of liability?

Please specify the AI applications:

*In specific applications, the liability could be introduced for an autonomous system and its owner. The owner means the one who use the system, where life & limbs are at stake or personal/material damages could occur.*

### 3.8 Do you have any further considerations regarding the question above?

*In specific applications, there could be strict liability standards should exist to allow the claim compensation from the owner of the autonomous system, who should be able to bring these claim up to his insurance.*