SAP Response to the European Commission's White Paper on Artificial Intelligence - A European approach to excellence and trust

Executive Summary

Artificial intelligence (AI) will be a core driver of productivity and economic growth while it will also play a significant role in addressing critical societal challenges as it does now in the context of the COVID-19 pandemic. Europe must create an Ecosystem of Excellence for AI by boosting investments in AI research and innovation, fostering the adoption of AI across all industries and by the public sector and SMEs and to close the digital skills gap.

We fully support the European Commission's vision on creating Trustworthy AI systems for Europe that is built around a human centric approach. Europe needs an Ecosystem of Trust for AI – a harmonized and favourable policy framework in order to establish a single market for AI products and services, to provide legal certainty for AI developers and users, and to build consumers' trust in the technology across Europe.

To reach these objectives, we recommend the European Commission to first establish a dedicated programme across Directorate-Generals in order to complete the review of existing EU legislation potentially applicable for AI and make them fit for AI. Focus areas should include safety, liability, data protection, privacy, employment, anti-discrimination and relevant sector specific legislation. We believe that the concerns presented by applications of AI outlined in the White Paper could be addressed with guidelines and targeted amendments of existing horizontal and sector specific EU legislation.

We strongly recommend the European Commission not to rush into a horizontal AI specific legislation that would disregard the principle of technological neutrality and could lead to legal inconsistencies with existing EU legislation. Looking at the dynamic nature and fast-paced evolvement of AI, the implementation of an AI specific regulation could become challenging for AI developers and users and outdated after a short period of time. This hold true in particular for the definition of high-risk AI applications. There is also a fair risk that an uncertain regulatory environment and over-prescriptive rules will hinder investments in AI as well as the use of innovative AI solutions.

Against this background, the difference between purely technical applications of AI and AI having a direct impact on citizens/consumers must be taken into account. A potential EU regulatory framework for AI should make an emphasis on the protection of individuals and analysing risks from the perspective of the consumer. Therefore, if the European Commission deems to create a horizontal regulatory framework for AI, then the scope should be limited to high risks B2C AI applications, leaving B2B AI applications out of scope. Risks related to B2B AI applications can be addressed through contractual arrangements between business partners. This way, compliance with any AI regulatory requirements will be ensured throughout the supply chain by private contracts. This concept has already been recognized and applied in the NIS Directive, for medical devices and product safety.

Moreover, to reflect on the risk-based approach, we recommend setting up a clear and precise criterion for high-risk AI systems based on the probability of occurrence and consequences of the expected risk. To ensure legal consistency, the European Commission should rely on existing risk assessment processes and classifications defined in existing legislation.

We would caution the European Commission against the application of new ex-ante conformity assessments that could cause significant delays in releasing AI products and services to the European market. Instead, we suggest the application of existing self-assessment tools for Trustworthy AI

systems such as the Data Protection Impact Assessment (DPIA) under the General Data Protection Regulation (GDPR) that is built upon companies' existing practises.
We believe that a process -based certification scheme for high-risk AI systems should be applied instead of individual product or algorithm-based certifications in order to avoid "repeated assessments over the lifetime of AI systems" as suggested in the White Paper. Such certification scheme would focus on the effectiveness of the company or system wide processes that are applied to the ethical development, deployment and operation of AI systems. With process-based certification, one can provide the required insights into the best practises of AI Ethics applied to the development and deployment activities that each AI system undergoes.

Moreover, we can build on existing comprehensive legal framework for data, in particular for the processing of personal data under the GDPR that has a significant role in fostering digital trust that is essential for AI acceptance by consumers and both public and private bodies. Furthermore, we recommend that the DPIA should be expanded to an AI Impact Assessment that includes a process of balancing both concrete benefits and risks of AI if an automated decision is made by an AI system. We also recommend the applicability of the rights under Art. 22 GDPR to be extended to AI-supported assistance systems and the clarification on the application of rights of individuals under Art. 15 to 21 GDPR in the AI context.

Considering the liability related concerns, we believe it is crucial to identify gaps first in the current legal framework before assuming that existing insurance schemes, civil liability rules and tort law as well as contractual arrangements are not fit for purpose. In the context of strict liability, it is key to determine who has the economic or social benefit from applying the risk and deploying the technology and for what use was the technology foreseen. Overall should strict liability for high risk applications only be considered in very exceptional cases when life or health are concerned in a public space. A reversed burden of proof is a very sharp tool - as the as a general rule, the victim should continue to be required to prove what caused her harm. A reversed burden of proof should only be considered in limited cases – and context specific (if it was truly impossible/prohibitive for the victim to provide evidence) – and only apply to very high-level risk AI applications.

Ecosystem of Excellence

Europe must be at the forefront to reap the economic and social benefits of AI and to ensure future competitiveness and well-being. One area where Europe has the potential to actively compete and lead is the emerging AI business-to-business market. European enterprises generate a wealth of business data that can be leveraged to train algorithms. There is strong industry domain know-how in Europe that is essential for the creation of state-of-the-art AI solutions. Paris, Berlin and Amsterdam have become important AI start-up hubs with a strong focus on AI enterprise solutions. There are some mature and well-funded European AI companies in the field of data analytics. Similarly, there are several universities and institutes that are becoming leading research centers for AI enterprise applications.
In order to create an Ecosystem of Excellence, the EU must provide sufficient tools and resources to facilitate the uptake of AI by the public sector and SMEs, to close the digital skills gap and to invest vastly in AI related research & innovation activities.

Both the existing workforce and future talents must develop the skills to leverage the many job opportunities that AI and intelligent enterprises will offer. National governments, business leaders and educational institutions must join forces in order to ensure future employability and that industry can find the talents to exploit the potential of AI.

Develop AI forecasting skills: Closing the skills gap will have to be based on a solid understanding of the existing skills base and the skills needed in an AI environment in the future. National governments and industry must do their part to identify future skills needed for jobs undergoing transformation as well as skills required for new types of jobs that will be created through AI. The European Commission should have a greater role in gathering information and raise awareness about upcoming AI specific jobs and new roles such as “data scientist” or “AI auditor”.

Reform the education system: National governments will need to adapt the curricula to help students to obtain foundational knowledge in AI. They should also promote STEM (Science, Technology, Engineering and Mathematics) education that provide a good foundation for AI-related jobs. Educational institutions should emphasize the importance of creativity, critical and systematic thinking and social and emotional capabilities to strengthen human role in an AI environment. We recommend the establishment of a one stop shop for AI training materials and massive open online courses (MOOCs) to be accessible for professionals, school teachers and professors.

Up-skill existing workforce: Training materials should also be made available to employees, especially through MOOCs which offers instant access and are free of charge. Lifelong learning will become increasingly important in a dynamic AI environment. Companies should provide sufficient training opportunities. Business leaders must invest more in human capital and place skills development front and center in their corporate strategy.

While AI has experienced a massive momentum due to the research results of recent years, more basic and applied research must be conducted: AI models must become more robust, accurate and credible. Interpretability and traceability of algorithms should be improved so that users can understand results. Neural networks must procure accurate results with less data and strengthen their ability to learn from distributed data sets.

To this end, we encourage the European Commission to leverage existing AI research excellence centres that have already established dedicated AI research programs. Their activities now need to be scaled up and coordinated at European level. Europe needs to invest in test labs, where industry and universities can jointly develop innovative AI applications and test them in a real-life environment. Public funding is needed to encourage SMEs to participate and provide innovative use scenarios to these test centres. Therefore, we welcome the planned investment in AI specialized Digital Innovation Hubs. Moving forward, these Hubs should help accelerate innovation and the uptake of AI.

Furthermore, we encourage the European Commission to offer public funding directed at the application of ML and AI algorithms and methods with distinguished focus on start-ups, SME and large enterprises in the area of applied AI and the usage of controlled training data pools with an open-source approach.
As the Multiannual Financial Framework entails various funding programmes with different priority areas, the synergies between these programmes should be strengthened for the next 2021-2027 programming period to better support AI specific projects across Europe.

AI has the potential to improve public services. Advanced planning and personalization of services through AI could boost public service efficiencies, especially in administration, education, healthcare, and infrastructure. For that reason, European public authorities should become role models for AI deployment and demonstrate that the technology yields tangible benefits for citizens. Therefore, we encourage the European Commission to promote AI adoption in public services. This could include identifying suitable AI use cases in public services: addressing technical, cultural and legal bottlenecks for AI deployment and exchanging best practises.

SMEs are the backbone of the European economy. However, they are lagging behind when it comes to the adoption of new technologies, including AI. They lack the conceptual understanding of the technology and the means they are able to leverage its benefits and develop use cases which fit their business. They may have access to data requiring further efforts to structure in a way that it can be used for AI. Moreover, they do not have sufficient access to capital, high-quality data sets and find it difficult to attract and retain talents. Digital Innovation Hubs should have a significant role in addressing these bottlenecks and provide additional services to foster the uptake of AI by SMEs.

Ecosystem of Trust

AI Risk-based Approach and Regulatory Framework

Introduction

Europe needs a harmonized and favourable policy framework for AI in order to establish a single market for AI products and services, to provide legal certainty for AI developers and users, and to build consumers' trust in the technology across Europe.
SAP is of the opinion that concerns around AI needs to be addressed, but the context and purpose of AI systems will be key to determine the implications and relevance of the ethical and legal challenges that may emerge in specific use cases. We fully support the European Commission's vision on creating Trustworthy AI systems for Europe that is built around a human centric approach. The development of AI must respect European standards and values.

Make current EU legislation fit for AI

We believe that the concerns addressed in the White Paper and the objectives outlined above can be achieved with the revision of horizontal and sector specific EU legislation outlined in the White Paper. Therefore, we recommend the European Commission to establish a dedicated programme across Directorate-Generals with concrete timetables in order to complete the review of EU legislation potentially applicable for AI and make them fit for AI. Focus areas should include safety, liability, data protection, privacy, employment, anti-discrimination and relevant sector specific legislation. A holistic and comprehensive overview of identified legislative gaps is needed in order to address them through additional guidance or concrete amendments of existing EU legislation.

Refrain from horizontal AI legislation

We strongly recommend the European Commission not to rush into a horizontal AI specific legislation.

- Firstly, we believe that most common concerns presented by applications of AI outlined in the White Paper could be addressed by adapting existing horizontal and sector specific legislation at EU level.

- A specific AI regulatory framework could lead to legal inconsistencies with different EU legislation already covering AI directly or indirectly in their scope. We firmly believe that regulations should not be created in technological silos. It is important to stress that AI is constantly evolving and improving and should be treated equally with other technologies. Indeed, the definition of AI is itself challenging and adaptive techniques are already widely used in. The so-called 'technology neutrality' principle has already been recognized and applied at European level in key legislations such as the GPDR and the NIS Directive. Therefore, we strongly recommend the application of the technology neutrality principle when assessing the need for regulatory intervention on AI. This ensures that policy framework remains dynamic, adapting to the evolution of the technology.

- Considering the fast-paced evolvement of AI, the implementation of an AI specific regulation and the modification of high-risk AI use cases in a legislative annex could become challenging for AI developers and users and outdated after a short period of time.

- There is also a fair risk that an uncertain regulatory environment and over-prescriptive rules will hinder investments in AI as well as the use of innovative AI solutions, with severe implications for European competitiveness. Furthermore, the enforcement of such specified rules would pose significant challenges for companies to implement operational and flexible processes and tools.

AI Definition

If the European Commission proceeds with a regulatory intervention for AI, a clear and precise definition will need to be established for the sake of legal clarity, the effective enforcement of an EU regulation and having a common understanding of the technology.
We differentiate between two types of AI systems:

Rule-based AI systems are characterized by the fact that the behaviour of their components is fully defined by rules created by human experts. These systems are often described as symbolic or expert systems.

Learning-based AI systems are differentiating themselves by the fact that their initial configuration made by humans is only the basis for the final form of their functions. With the help of data, they train how to solve a problem and continuously adapt their function in this process. For learning-based AI systems, humans define the problem and the goal, but the behaviour rules and relationships required for the solution are learnt in an automized way.

Definition of high- risk AI systems should exclude B2B applications

Given the identified legislative gaps, if the European Commission deems that a regulatory intervention for AI is necessary, we support a principle-based framework limiting the scope to high risks arising in B2C context impacting consumers directly. B2B AI applications should be left out of scope with B2B matters handled by the supply chain effect (i.e. B2C players cascade their requirements through the supplier network).

Firstly, clear distinction shall be made between AI frameworks providing a set of technical approaches (which have individual technical challenges e.g. in regards of accuracy and explainability) and AI solutions created and used by human developers and users (being responsible for their created systems and their actions). Accordingly, difference between purely technical applications of AI and AI having a direct impact on citizens/consumers must be taken into account.

A potential regulatory framework for AI should make an emphasis on the protection of individuals and analysing risks from the perspective of the consumer. Therefore, we suggest an additional criterion to the definition of high-risk AI systems focusing on fundamental rights, consumer rights and safety-related harms of AI products or services offered by B2C actors (for example a risk to life, health or privacy).

For most B2B AI use cases, AI Ethics concerns are often not the primary relevant concern in the B2B context as they are in B2C. Given the contractual arrangements in the B2B sector, the compliance of AI providers with a potential AI regulation will be indirectly ensured throughout the supply chain.

This has already been recognized and applied in the NIS Directive, medical devices, product safety and similar approaches.

Therefore, the B2B sector should not be disrupted with new rules that could significantly slow the adoption of AI and could hamper innovation. Given that a developed AI model could be deployed in various context and areas, the different bilateral contractual freedom of B2B operations should be maintained in order to specify the application area of companies' AI models, products and services. Potential risks can be addressed in private contract ensuring a fair allocation of risks among developer and deployer.

For the sake of legal clarity, the definition of consumers, B2C and B2B shall be interpreted in line with Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services and Regulation (EU) 2018/302 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market:

'Consumer' means any natural person who is acting for purposes which are outside his or her trade, business, craft or profession';

'B2C' means any private individual acting in a commercial or professional capacity or any legal person offers goods or services to consumers for purposes relating to its trade, business, craft or profession;

'B2B' means any natural person or any legal person, irrespective of whether privately or publicly owned, who is acting, including through any other person acting in the name or on behalf of the trader, for purposes relating to the trade, business, craft or profession of the trader.

To further reflect on the risk-based approach, it should be noted that there is no one-size-fits-all approach when it comes to AI systems. We welcome the European Commission's risk-based approach where the most pressing risks should be addressed with targeted actions limited to highly critical applications of AI. To this end, we recommend setting up clear and precise definition and criteria for high-risk AI systems based on the probability of occurrence and consequences of the expected risk. To ensure legal consistency, the European Commission should rely on existing risk assessment processes and risk classification defined in existing legislation.

We believe that the scope of the exceptional instance outlined in the White Paper is too broad in its current form that could create legal uncertainty in the future. The European Commission should focus on setting up a future-proof criteria for high-risk AI systems and should avoid using exceptional cases that could make the risk-based approach less robust and effective.

Mandatory Requirements

In order for Trustworthy and Ethical AI regulation to be effective and able to be implemented and enforced there are several mechanisms that should be taken into consideration by EU decision-makers. First and foremost, there should be a common understanding on the concept and meaning of ethical principles (i.e. fairness) before they are being transformed into concrete processes. It will be crucial to clarify these concepts in order to set up operational requirements for businesses as they should not be in a position to interpret ethical concepts that often have several subjective meanings.

Furthermore, it is imperative to involve AI practitioners who have experience outside of a purely research or small-scale operation throughout the decision-making and implementation process. This concept of appropriate involvement will also extend to those authorities who are put in charge of the day to day oversight and enforcement of any new rules on AI as great skill will be required in order for regulations to have the appropriate and intended impact. As we have pointed out, we feel that the concerns outlined in the White Paper could be addressed by the revision of existing EU legislation and therefore, it is necessary to have a clear delegation of duties between different authorities so that AI providers are not responsible for managing the overlap or gaps between various authorities.

Training Data

We are in the fortunate position within the European Union that we already have the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("**GDPR**") in place that sets a solid foundation for the free flow of personal data within the European Union and the protection of personal data as a fundamental right. We encourage the European Commission to build upon that foundation while also allowing for measures that will help promote trustworthy artificial intelligence. If the European Commission proceeds with training data related requirements it will be important to create synergies with the relevant articles of GDPR.

Addressing bias at each step of an AI system's lifecycle is crucial but it is also important to note that all data potentially has bias (e.g. in case where the training data reflects previous discrimination, or the training data has imbalances). Often this bias is irrelevant for the application or can be mitigated technically. Furthermore, bias only becomes a concern that goes beyond general system quality, when it leads to unfair discrimination i.e. a system that systematically interprets a letter o as zero is biased but maybe still provides meaningful value. It is important to detect unfair discrimination at output level and then address it via technical or other means including the robust testing of any anti-discrimination measures on an ongoing basis.

It is also important to acknowledge that the more restrictions that are put on training data, the more difficult it will be for organizations to get broad, representative data. Broad representative data is essential for not only accuracy but also in order to mitigate the impacts of bias in data. Further requirements on training data will also complicate the use of data that was collected before a new AI regulatory framework. We also urge the concept of 'sufficiently representative' to be defined more clearly by the European Commission and that policies are then written in order to support achievement of this new concept of 'sufficiently representative'.

Data and Record Keeping

We agree with many of the requirements that are outlined in the AI White Paper about data and record keeping that should be based on necessity and proportionality principle, bearing in mind the resources needed to document the AI systems' datasets, decisions, and processes. We strongly suggest that all data and record keeping requests are implemented in such a way as they can meet the requirements within the GDPR. This is especially important for any requirements to maintain data sets or for auditing of data sets or performance over time while allowing for retention and deletion (especially right to be forgotten) of personal data in line with GDPR.

Information to Be Provided

One of the leading principles of the GDPR is the principle of transparency; transparency includes an obligation to inform the individual about their rights and enable them to exercise those. In the case of automated decision-making in the meaning of Art. 22 GDPR they even have the right to receive

meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. Therefore, any new information provision requirements should be in line with Art. 22 GDPR when it comes to processing of personal data by the AI system. Under a new AI regulatory framework, it will be important to clarify which elements of an AI systems needs to be documented and shared with which actors, especially the data subjects and for what purposes.
It is also important to note that challenges around transparency and explainability in the case of sophisticated machine learning models is an area of active research. Therefore, it would be important to accelerate this area of research with sufficient public funding and interpret its findings into operational and technical standards. Where explainability is deemed to be too challenging to achieve in the case of some AI models, documenting the reproducibility of outcomes should be considered as a solution.
We acknowledge the importance of transparency and explainability especially in case of AI systems directly engaging with end-users. We further suggest differentiating requirements between B2B and B2C AI applications as the greater the impact on the individual (e.g.: in the area of healthcare), the greater the required explainability and transparency should be, allowing individuals to understand the reasons for the decision and challenge it when appropriate.
However, we strongly advise against excessive information provision obligations and disclosure of technical features that would not necessarily be informative for users. Furthermore, such disclosures would create risk for intellectual property rights, security, and companies' contractual arrangements with customers.
As a B2B company, we support our customers with products able to explain the reasoning behind intelligent system proposals in context and at the right time for end-users. These are empowered with a feedback loop in order to allow end-users to provide feedback on the output of the algorithm that we can further evaluate and incorporate into the re-training of the algorithm.

Robustness and Accuracy
It will be important for AI developers and deployers to get a better understanding on the intended application, the impact of the use case and discuss adverse outcomes, unusual patterns and the means they could be prevented and mitigated.
However, it should be noted that 100% accuracy cannot be ensured during the entire life cycle of an AI system. Machine learning techniques are based on approximation where training a model has the goal to minimize the error rate. Despite the fact that software code aims to be 100% error free, also rule-based programming cannot guarantee the absence of errors in most cases.
Any mandatory requirements to ensure safe and accurate outcomes of high-risk AI systems should be reasonable and be adapted to the specific context and use case.
Companies' existing practises should be taken into account to improve model accuracy and efficiency such as analysing the feedback of end-users, monitoring the performance of the model and documenting any negative and unforeseen impact and failed testing with their parameters.

Human Oversight
To define the necessary and proportionate level of human involvement for a high-risk AI system, determining its objective will be a first crucial step. Firstly, we strongly recommend the European Commission to ensure any new rules to be consistent with the existing rules of Art. 22 GDPR. Any oversight mechanism should be adapted to the specific risks, the level of automation, and context of the AI system. For example, in case of autonomous cars detect a potential accident and decide to use the break, there is no sufficient time to consult with a human first. The European Commission should further clarify at which stages and to what extend human involvement/oversight is needed for high-risk AI systems.

Voluntary Labelling Framework

A voluntary labelling system could serve as a flexible and market-driven solution to develop and deploy Trustworthy AI systems. However, its acceptance and added value will highly depend on the overall scope of high-risk AI systems, the operational nature of its requirements and governance structure.
It will be important that such framework is industry driven, supervised by the European Commission and endorsed by all EU Member States in order to serve as a gold standard within Europe and across the globe. The AI Ethical Guidelines created by the AI High-Level Expert Group could serve as a foundation for the voluntary labelling system to develop two set of requirements addressed to AI developers and users. Such a scheme should have a steering group to work on the requirements with AI auditors involved to ensure effective implementation. Enforcement could be on a voluntary basis accomplished by self-assessment by AI developers or deployers and by third-party certification obtaining a 'Trustworthy AI' certification/label. This framework could also be required by B2C companies' procurement policies towards their suppliers in order to ensure the ethical development and deployment of AI products and services.

Enforcement and Governance

We would caution the European Commission against the application of new ex-ante conformity assessments that could cause significant delays in releasing AI products and services to the European market. The administrative burden coming with extensive testing and audits will deter companies, especially SMEs from developing AI products that could result in the decline of AI adoption and could reduce overall competitiveness of Europe.

Instead, we suggest the European Commission to consider the application of existing self-assessment tools for Trustworthy AI systems such as the DPIA under GDPR that is built upon companies' existing practises.

The lack of expertise on the evaluation of algorithms and models will also need to be addressed within a harmonized European approach in order to ensure an efficient and uniform enforcement of any rules.

Standardization will have a significant role in enabling a flexible and innovation-friendly regulatory framework at EU level. The EU should instruct a European standardization body to develop a standard with concrete obligation to implement a potential AI regulatory framework addressed to high-risk AI system plus a certification scheme.

We believe that a process -based certification scheme for high-risk AI systems should be applied based on the EU AI Ethical Guidelines that already process-based instead of individual product or algorithm-based certifications in order to avoid "repeated assessments over the lifetime of AI systems" as suggested in the White Paper.
Such a certification scheme would focus on the effectiveness of the company or system wide processes that are applied to the ethical development, deployment and operation of AI systems. With process certification, one can provide the required insights into the best practises of AI Ethics applied to the development and deployment activities that each AI system undergoes. Therefore, it would enable new product versions without the need to re-assess AI systems throughout their lifetime each time.

This will require defining the criteria and a methodology for evaluation. Following this approach, a process-based certification scheme could serve as the baseline across industries that will provide a transparent and effective processes to develop and deploy Trustworthy AI systems.

Re-training algorithms in a specific location will not necessarily guarantee AI systems with higher quality and a different output. Relying solely on European trained algorithms and European data sets could also cause challenges with regards to the diversity of datasets. We need to have a global focus to ensure a diverse and fair user experience and avoid burdensome requirements for European based companies who serve markets across the globe.

Finally, regardless of the specific structure of the enforcement mechanism, the European Commission must continue to involve industry in discussions in order to realize an effective and operational framework for Trustworthy AI systems.

International Cooperation on AI

The emerging global market for AI products and services will provide tremendous business opportunities for the European industry but it is important to note that they are developed with the combination of both European and non-European components. Governments around the globe are creating distinct ethical and policy frameworks for the development and use of AI.

Therefore, we strongly recommend the European Commission to take a leading role on the international governance of AI and promote a shared understanding and joint approach on the ethical development and use of AI in platforms such as the OECD and G20. The EU should also have a greater coordinative role to shape the development of international standards for Trustworthy AI in cooperation with for example International Organisation for Standardisation (ISO) and International Electrotechnical Commission (IEC) to harmonise the technical requirements of AI. This will ensure a level playing field globally and open AI markets for European industry worldwide.

AI & GDPR

1. **Build on the existing legal framework at a European level, in particular the GDPR**
    - We can build on our existing comprehensive legal framework for data in the European Union, in particular for the processing of Personal Data under the GDPR.
    - The trustworthiness of AI is built on three pillars (1) lawful by respecting all applicable laws and regulations, (2) ethical by respecting ethical principles and values and (3) robust by both from a technical perspective while taking into account its social impact. For the pillar "lawful" the processing of Personal Data under the GDPR is a crucial key for a legal and transparent processing because AI requires access to extensive sets of data, in many cases, sensitive data including data on race, ethnicity, gender and other sensitive attributes.
    - Building on the GDPR is a major step to foster a digital trust that is essential for AI acceptance by consumers and public as well as private bodies. Possible conflicts such as the need to keep data for the audibility of the algorithm with the right to deletion of the data subject (or the so-called right be forgotten) must be solved and balanced with the framework of the GDPR.
    - The GDPR requires that the processing of Personal Data happens in a fair and transparent manner; in many instances AI is discussed in the context of ethical principles and even if the processing is already not legally permitted under the provisions of the GDPR.

2. GDPR has the roadmap for accountability to ensure product and business compliance

- One of the cornerstones of accountability, particularly when technology such as AI is involved, is the documented DPIA by the controller. In the context of a DPIA a "risks – benefits balancing test" is essential.
- The DPIA should be expanded to an AI Impact Assessment that includes a process of balancing both concrete benefits and risks of AI if an automated decision is made by an AI system.
- A "risk-benefits" balancing test is essential because there could be a high risk related to a specific AI system that may be overridden by compelling benefits to individuals and society at large. In any case, if the GDPR applies, Art. 32 ensures the security of processing on a level of technical and organizational measures appropriate to the risk.
- Further, explore and promote sector-specific risk assessment, inter alia whether AI is used in the private or public sector and also whether the use of AI is in a risky sector like healthcare, policing or judiciary.

3. AI transparency - meaningful information about the logic involved

- GDPR provisions that are squarely aimed at AI state "the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." (Art. 22 and Recital 71).
- According to the GDPR, a distinction can be made between (i) AI systems which, as assistance systems, support people in their decisions ("AI-supported assistance system") and (ii) AI systems which make decisions independently, so-called systems for Algorithmic Decision Making ("Algorithmic Decision Making").
- Art. 22 GDPR only covers the case of Algorithmic Decision Making when a decision is based solely on automated processing which produces legal effects or similarly significantly affects the data subject. The applicability of the rights under Art. 22 GDPR should be extended to AI-supported assistance systems.
- GDRP already provides for a general obligation of transparency including an obligation to inform the individual about their rights and enable them to contest their decision and even seek redress. Also noteworthy are Art. 13 and 15 which state repeatedly that data subjects have a right to "meaningful information about the logic involved" and to "the significance and the envisaged consequences" of automated decision-making.

4. Foster data sharing in the Digital Single Market

- AI depends on an ability to use large data sets and the EU needs to fully leverage its Digital Single Market to enable responsible use and access to such datasets in order to develop its AI capabilities and strengthen the AI industry.
- This includes B2B sharing but also between business and government.
- To foster such a data sharing GDPR tools should be developed further, for instance
  - Reduce uncertainties regarding pseudonymization and anonymization; e.g. the conditions under which datasets containing personal data are considered as anonymous in specific contexts need to be respectful with the GDPR.
  - Less stringent legal requirements for a permissible processing of pseudonymous data should be encouraged e.g. to process pseudonymous data for legitimate interest in the context of developing AI to ensure quality of datasets

5. **Importance of a coherent and modern interpretation of GDPR by the data protection authorities**
    - As the GDPR embeds the risk–based approach precisely to allow for consideration of risks and harms, we believe it would be crucial to further explore possibilities under Art. 89 GDPR how the GDPR applies to processing of personal data for research purposes by the private sector. Especially, if AI technology is trained where the risk is lower meaning that there are no direct legal effects or similarly significantly effects for the data subject.
    - An additional authorization criterion should be introduced allowing the processing of particularly sensitive data (special categories of personal data under Art. 9 GDPR). The added value for the data subjects as well as for society should be taken into account, especially if the rights of a data subject are only slightly affected meaning that there is no direct legal effect or similar significant risk for the data subject.
    - Besides the general need for a clarification of the access right under the GDPR, there should be a clarification on the application of rights of individuals under Art. 15 to 21 GDPR in the AI context, especially, if AI technology is trained and possible limitations of data subject rights, where they could render algorithmic training impossible.

Liability Framework for AI

Legislation in the field already exists to a large extent. We believe it is crucial to identify gaps first in the current legal framework before assuming that existing insurance schemes, civil liability rules and tort law as well as contractual arrangements are not fit for purpose.

There is no one size fits all: diversity of emerging digital technologies (and the diversity of use and application) – leads to a diverse range of risks, which makes it very difficult to come up with a single solution suitable for the entire spectrum of risks. AI should not be viewed as a single technology but rather as supply chain matter. It is very important to identify who has what responsibility and who could control which risk.

In the context of strict liability, it is key to determine who has the economic or social benefit from applying the risk and deploying the technology and for what use was the technology foreseen. Overall should strict liability for high risk applications only be considered in very exceptional cases when life or health are concerned in a public space.

For the business to business sector it is essential to preserve private autonomy (Privatautonomie) to -within borders - freely negotiate contractual relationships or partnerships. This remains a key principal under civil law and needs to be preserved as far as possible – not least to restrict use contractually. Service and technology provider can't be held responsible or liable to a use or application of technology/software that wasn't agreed or even explicitly excluded contractually.

In some digital ecosystems, contractual liability or other compensation regimes will apply alongside or instead of tortious liability. This must be taken into account when determining to what extent the latter needs to be amended.

A reversed burden of proof is a very sharp tool - as the as a general rule, the victim should continue to be required to prove what caused her harm. A reversed burden of proof should only be considered in limited cases – and context specific (if it was truly impossible/prohibitive for the victim to provide evidence) – and only apply to very high-level risk AI applications. Where a particular technology

increases the difficulties of proving the existence of an element of liability beyond what can be reasonably expected, victims could be entitled to facilitation of proof.

It should be considered that logging documentation and track records for exculpation can create an enormous bureaucratic burden. Potential overlap with existing legislation like the GDPR which also provides for extensive documentation requirements, must be avoided.

It is not necessary to give devices or autonomous systems a legal personality, as the harm these may cause can and should be attributable to existing persons or bodies.
In situations where a service provider ensuring the necessary technical framework has a higher degree of control than the owner or user of an actual product or service equipped with AI, this should be taken into account in determining who primarily operates the technology. It is still necessary to determine who has the benefit from deploying the risk and who controls the overall process.