SAP Position Paper: EU Artificial Intelligence Act

INTRODUCTION

- 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 a harmonized regulatory framework 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.
- Since there is a group of EU legislations covering AI directly or indirectly in their scope, it will be important to avoid legal inconsistencies with the proposed requirements of the Artificial Intelligence Act. As the European Commission is planning to propose a new liability and safety regulatory framework that will cover AI systems, we suggest building upon the provisions of the proposed AI Act and ensure synergies of these legislative files throughout the EU decision-making process.
- We appreciate the European Commission's efforts to propose a future-proof legislation that can stay up to date with the fast-paced evolvement of AI. However, we strongly advise against the application of secondary legislation (delegated acts) affecting core elements of the proposal such as the modification of Annex I on AI techniques and approaches and the modification of Annex III. Such significant changes should not be realized under the timeframe of a few weeks without leaving the possibility for industry to provide sufficient technical feedback. These modifications should be made with the involvement of the public through consultations and an independent expert group with technical knowhow. Such substantial changes implemented in a short timeframe will cause legal uncertainties for all impacted providers and users. Furthermore, it is not clear if those annexes are meant as complete lists and the national laws must stick to those lists or if they just meant as guidelines for the national lawmakers. Annex I has the character of a complete list while Annex III within the individual points remains rather exemplary.
- There is 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 overbroad and vague requirements could pose significant challenges for companies to implement operational and flexible processes and tools. Imposing an additional penalty regime for non-compliance under this regulation would double the risk of penalties for companies in addition to the GDPR[1] and other regulations. For this reason, the fundamental principles under the GDPR should be applied for the development/use of AI systems while the existing framework is expanded to include the necessary requirements for AI systems.

Overall, given the complexities of the AI value chain, we would need further clarifications from decision-makers with regards to the following:

Definitions

The objective of the AI Act is to prevent or significantly reduce any harm that high-risk AI systems can cause to the health, safety and fundamental rights of individuals. However, the definition of AI seems to suggest a scope that goes beyond what is commonly considered as AI technology. We have the following observations:

- Regarding the definition of AI in Annex I, we would like to call attention to (c) as it broadens the scope of the regulation to include common and traditional statistical methods and simple low dimensional problems that have already been in use for decades across many industries. It is our recommendation to focus instead on (a) and in particular (b) which highlight new situations that AI brings to the forefront and where either humans may not be required to provide input, verification or causality, or where humans are unable to easily comprehend the complexities and relationships within the data. Part (c) reflects neither. Accordingly, we are seeking clarification if the intention is indeed to regulate traditional statistical methods and simple low dimensional problems. If this was the case, even the simplest planning solution that is based on historic data would be considered AI, which in our opinion does not

[1] Such as providing a legal basis for processing, fairness, transparency but also concepts such as privacy by design and by default.

adhere to modern AI system definitions and is seen as counter-productive for the true promise of AI systems and depending services.

- We believe it is key to have a clear definition of the roles and separate between end user and user/intermediary. Particularly in the context of B2B AI, it is important to ensure that the Act appropriately differentiates between the different stakeholder and user roles and hence also the obligations of the AI provider (in this example SAP) and the company who is providing the AI to its end users (in this example, the SAP customer providing AI to its employees via an SAP product) as SAP is one step removed from controlling how AI is presented to the end users. In our opinion, as in other software usage situations, some of the obligations must also be placed on the companies purchasing AI in the B2B context. To give an easy example: a carmaker is not solely responsible for an accident of a car. The usage of the AI by an intermediary or end-user might lead to a different obligation. More fine-grained role specification and appropriate differentiation is needed e.g. for the design of the algorithm, the execution in specific hardware or repackaging of the technology in more complex solutions. This is seen as necessary as increasingly AI products and services (both for hardware and software) are integrated in more complex systems, which makes the need for clear roles across the whole lifecycle of these systems.
- In addition, end-users should be defined and specified in the proposal, as some of the requirements (e.g.: transparency and provision of information) should be concentrated on them instead of users explicitly. Existing definitions under the GDPR do not necessarily need to be repeated or should be at least aligned. We recommend that lawmakers further clarify and narrow the language in Annex III, considering the diversity of applications that may fall under some of the definitions.
- We would seek further clarification on Recital 11 to avoid varying interpretations with respect to scope and impact of the regulation. It would be clearer if *"using an AI system"* would be precisely defined and clarified how the regulation would apply to scenarios in which AI systems used outside the EU would affect the rights of European citizens.

Providers responsibilities

- **Reporting of serious incidents and malfunctioning**: Article 62 requires providers to report "any serious incidents and malfunctioning of high-risk AI systems" that could breach fundamental rights to respective national market surveillance authorities. We recommend including specific parameters to assess the impact of serious incidents and malfunctioning. They would improve legal certainty significantly. At EU level, various legislations (GDPR, Cyber Security Act, ePrivacy Directive, NIS and NIS2) require notification of incidents to different authorities under different thresholds. In order to avoid additional processes, put on providers, we recommend streamlining notification processes at EU level, also to ensure that confidentiality of customer data is respected. We suggest integrating the incident notification into the EU AI centralized database where providers could directly report them to the European Commission and national competent authorities. We also need a clear one-stop notification recipient in case of cross-border incidents. The seat of the company or, in case of a non-EU company, a registered entity in the EU must be able to provide notifications for all EU countries to avoid duplication.
- **CE marking**: We believe that the proposal should entail further details on the process of affixing the CE marking and the placement of the CE marking in case of software. It will be crucial for the AI Act to create uniform rules on the requirements and process as it is the first time that the CE marking will be a requirement for software.
- Article 64 requires providers to give access to training, validation, and testing datasets[2] through APIs or other technical means and the source code of the high-risk AI system to market surveillance authorities. Firstly, we would need further explanation from EU decision-makers about the potential added-value of the source code with regards to addressing potential risks of an AI system. Granting access to the source code could be challenging when the AI system is just one component of a complex software. Such disclosure would heighten risks for safeguarding intellectual property rights, trade secrets, privacy, cyber security, and companies' contractual arrangements with customers. The possibility of security incidents is especially high if data access happens via publicly available APIs. In addition, possible conflicts such as the need to keep data for the audibility of the algorithm with the

[2] Datasets could be from customers for the sole purpose of SAP's use. This could pose additional legal challenges from a confidentiality point of view.

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.

High-risk AI systems

- We believe that *"the management and operation of critical infrastructure"* currently defined as a high-risk category is too broad and against the objective of focusing only on well-defined areas of risk. Such a broad category could entail a wide range of back-office AI solutions (with regards to procurement, invoicing, payments etc.) in the scope that do not cause any harms to the safety of individuals. Instead, we recommend narrowing down the high-risk category to a complete list of affected sectors and affected operational areas excluding commercial and administrative departments that are not related to the underlying risks.
- Based on the definition of remote biometric identification systems in the proposal, it is not clear whether unlocking devices or having remote access to machines, systems with the usage of biometric data would be considered as high-risk AI systems. We believe further clarification in this high-risk category will be essential as not all remote biometric identification systems in all contexts pose a risk to the fundamental rights and safety of individuals. Also, not all biometric identification systems are AI systems. This would lead to a different (legal) treatment for some biometric identification systems falling under the regulation and others not, depending on which underlying technology they use.
- The high-risk category of *"access to and enjoyment of essential private services and public services and benefits"* was left very broad that could include the identification of a wide range of AI use cases used in the private and public sector. The future extension of this category could have detrimental effect on AI adoption in the public services. We would recommend EU decision-makers to narrow down the category to concrete use cases based on the classification of high-risk AI systems outlined in the proposal.
- With regards to the revision and extension of the high-risk AI systems list (Annex III), we recommend the further clarification of the overall process for the sake of legal certainty. We believe that clear criteria for the evaluation of the definition of a High-risk AI system are essential for implementing privacy by design and for designing enhanced technologies to meet the high level of protection of the fundamental rights of concerned individuals rather than listing certain AI systems.
- Currently, the legislation does not provide any information on who could initiate the extension process, the potential involvement of industry, a transition period for providers and users to comply with the changes, the role of the EU AI Board and an independent Expert Group to provide technical input. We believe that all these details should be explicitly included in the proposal. The process to periodically review the list of high-risk AI systems should be clear, transparent, based on evidence and take place in consultation with involved stakeholders.

Mandatory Requirements

- For the Artificial Intelligence Act 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 several ethical principles (i.e. bias). Also, they should only be included in the act if there is a concrete idea of how they can be enforced through a regulatory process. 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 valid subjective meanings, even between the various EU member states.
- When it comes to the operationalization of mandatory requirements, we strongly support the European Commission to work with standardization bodies instead of focusing on the preparation of technical specifications. This will enable engagement by public and private sectors to develop a flexible and innovation-friendly regulatory framework at EU level and to define the most appropriate standards for the current technology and markets. For the sake of legal certainty, to drive innovations and to ensure competitiveness of companies it will be essential to establish a timeline for the set-up of standards.

Data Governance

- We encourage the European Commission to build upon existing EU legislation while also allowing for measures that will help promote trustworthy AI. In case of data governance related requirements, it

will be important to create synergies with the relevant articles of GDPR to avoid uncertainty and complexity. Data governance practices shall be defined for the development of AI systems in general, outlining additional principles for high-risk AI systems.

- Addressing bias at each step of an AI system's lifecycle is crucial. Here, it is also important that the bias contained within data should be treated differently than the bias that may result from the outcomes produced by an algorithm. Though they can certainly be related, a bias in the data does not automatically result a biased output. We urge to focus on the biased outputs because this is where potential damage occurs, and it gives the incentives to develop techniques to train unbiased systems on biased data. Based on Article 10 paragraph 3, we also urge the concept of *"relevant, representative, free of errors and complete"* datasets to be defined more clearly as it won't be possible to guarantee such features with technical means. Indeed, part of the job of a true data scientist is to work with the errors in a data set and make sure they are appropriately controlled for.
- **Record keeping requirements** should be based on the necessity and proportionality principle, bearing in mind the resources needed to document the AI systems' datasets, decisions, and processes especially in the case of small providers. We strongly suggest that all data and record keeping requests are implemented in such a way that they can meet the requirements within the GDPR considering data protection by design and by default. 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.
- **Under the transparency and provision of information requirements** (Article 13), it will be important to clarify which information will be shared with which actors and for what purposes, while taking into account those scenarios that equally may prove impossible to provide such information or involve a disproportionate effort. We strongly advise against excessive information provision obligations and disclosure of technical features that would not necessarily be informative for end-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 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.
- **Human oversight**: Firstly, we strongly recommend the European Commission to ensure these requirements are consistent with the existing rules of Art. 22 GDPR. The degree of oversight should be adapted to the specific risks, the level of automation, and context of the AI system[3] to avoid hindering automated processes. It will be important to note that bias could also occur and be introduced by human developers. Therefore, in case human bias is the root cause for discrimination in a high-risk AI system, the added value of human oversight measures should be re-considered instead of promoted in the proposal. Furthermore, we would strongly recommend specifying which human oversight approach (human-in-the-loop, human-on-the-loop, or human-in-command) and at which step of the high-risk AI system's lifecycle should be adopted.
- **Robustness and accuracy**: It is more advisable that the regulation enforces providers of AI system to upfront define the purpose of the system, the intended way of using the system and define suitable performance criteria according to these. Using *"accuracy and robustness"* general criteria in the regulation does not work, simply because for many use cases accuracy cannot be defined e.g. chat bots or other systems with generative components. Also the approach we propose acknowledges the fact that it is always about finding trade-offs between different criteria, that not all criteria are suitable for all use cases and that actual performance of a system highly depends on the way of using a system. Companies' existing practices should be considered in the legislative proposal to improve model accuracy and efficiency such as analyzing the feedback of end-users, monitoring the performance of the model and documenting any negative and unforeseen impact and failed testing with their parameters. Requirements on robustness and accuracy should be reasonable and based on the particular context and high-risk use case.
- **Cyber security requirements** based on Article 15 should be in alignment with existing rules such as the NIS Directive, or the proposed NIS2 Directive.
- Article 52 sets **transparency rules for certain AI systems** that are intended to interact with natural persons unless it is obvious from circumstances and the context of use. We believe that such an

[3] These should ideally be specified to avoid misinterpretation.

exception creates legally a grey area as it is not clear from whose standpoint the obvious context or circumstance will be determined.

Enforcement

- It is necessary to have a clear delegation of duties between different national authorities so that AI providers are not responsible for managing the overlap or gaps between various authorities. The lack of expertise on the evaluation of algorithms and models will also need to be addressed with a harmonized European approach to ensure an efficient and uniform enforcement of rules and conducting audits.
- Based on Article 43 paragraph 4, high-risk AI systems should undergo a new conformity assessment every time they are subject to substantial modifications. The definition of substantial modification in the proposal entails changes with regards to the intended purpose or changes affecting the compliance of the AI system with the mandatory requirements (Title III, Chapter 2 of the proposal). We would recommend providing a more specific definition that includes specific details whether such modification will entail retraining, changing the weights of the model or updating the model in general. These details again raise issues around the definition of AI in the proposal that does not define the component parts of AI systems. Repeated conformity assessments will bring forward excessive administrative burden and costs for providers, specifically for smaller companies that might not have the necessary resources to cover such repeated assessments. It will also have the unintended consequence of disincentivizing product improvements or continuous development cycles (agile processes to make many small improvements over time) that are currently a key approach in which AI products are typically developed. Furthermore, this proposal does not sufficiently account for self-learning, transfer learning or reinforcement learning processes when used in providing continuous improvement or feedback to algorithms based on performance. Such continuous and collective learning approaches are expected to be an integral element of future AI systems, which goes beyond traditional cycle-based software development practices and therefore needs to be well-considered in this proposal. Eventually, the extensive testing and audits will deter companies from developing AI products that could result in the decline of AI adoption and could reduce overall competitiveness of Europe. On the other hand, the volume of requests to repeat conformity assessments will need to be managed by the respective notified bodies that will impact their operation and resources significantly.
- **Expert Group**: include explicitly in the proposal to ensure a direct role for industry, clarify its mandate, composition, responsibilities.
- Article 83 paragraph 2 determines the application of the regulation for high-risk AI systems already placed on the EU market or put into service. Such existing AI systems will have to comply with the regulation in case they are subject to significant changes in their design or their intended purpose from the application date of the regulation. Firstly, the Article does not define the application of the regulation to non-high-risk AI systems subject to transparency requirements that already have been placed on the EU market or put into service. Secondly, the legislation does not provide a legal definition for significant changes in design that will cause legal uncertainties for companies. We believe the application of the regulation to existing high-risk AI systems in the EU market should be clear and simple going forward to ensure legal certainty for providers and users in order to carry out the necessary compliance work.