EDiMA

EDiMA Annex to European Commission's AI White Paper Online Questionnaire

As the European trade association representing the online platform ecosystem, EDiMA would like to thank the European Commission for the opportunity to provide feedback on its White Paper on Artificial Intelligence (AI).

AI-powered analysis offers the European Union a range of opportunities in a broad variety of economic sectors and society in general. EDiMA's members are fully committed to maximising the benefits of AI for Europe, while keeping its potential risks to the bare minimum. EDiMA therefore supports the Commission's goals of promoting investment and innovation in trustworthy AI.

Due to the limited space available in the online questionnaire and the nature of some of its questions, EDiMA has opted to use this paper as an annex in order to elaborate, and where necessary clarify, some of the responses provided.

As a general remark, EDiMA would like to point out that certain questions in the questionnaire seems to include many presumptions, which we do not have the opportunity to address or question. We hope that the explanations can provide the context and nuance that we believe is vital for the European Commission to consider when assessing responses to the questionnaire more generally.

Section 2 – An ecosystem of trust

Regarding the questions posed on chapter 5 of the White Paper that sets out options for a regulatory framework for AI, EDiMA would like to clarify the following:

- Concerns about AI are all important and legitimate, they should by no means be discounted. Developments on AI are advancing quickly and will have a transformative impact on our societies.
- The vast majority of AI applications do not carry high risks for human beings and risks vary based on multiple parameters. AI and Machine Learning are software tools to help classify information, make recommendation and support optimization in ways that support organizational efficiency and human decision-making. Some AI applications are only linked to industrial processes and do not affect individuals.
- All concerns highlighted in the questionnaire's table are taken into account by companies during the development of AI applications, in order to ensure high-quality of products and services they offer consumers. Having strong processes in place can help to minimise risks - for example by checking the quality of the datasets within the model used to train it and by performing rigorous testing, though these processes must be flexible in order to adapt to widely different applications of AI.
- In this context, it is important to bear in mind that it is not possible to audit the quality of a dataset independently from the model being used to train it. It is essential to place the emphasis on having internal processes to audit the level of risk of using a particular data

source as training data for various tasks. The quality of datasets is not inherently high or low - they are either well- or ill-suited to be used to train AI models for certain tasks. To give a concrete example, a dataset of images of human faces that contained 70% male faces may yield a high quality face detection model but a gender-biased gender detection model. There is no way to audit the quality of the dataset independently from the model it is being used to train.

- Context and prevalence matter. Without knowing the purpose for which AI is used, who could be impacted, the scale of the risk or likelihood of harm, the relative importance of factors such as discriminatory outcomes or AI inaccuracies is difficult to assess.
- Similar to many other technologies, AI development is complex and unintended consequences can happen during the process. Even with datasets well suited to be used to train AI models for certain tasks and strong internal processes, something unintended can happen depending on the type of AI technology used. Over time, automated systems may stop functioning within their designed constraints. But there are processes such as audits, testing, monitoring, reviews, employee training etc. that can be put in place to mitigate that risk.
- Such good design practices are adopted by companies in order to win their customers' trust and thereby deliver the most appealing and competitive products to their customers. The need for regulatory oversight over such practices should solely focus on applications that carry the highest risk for users, bearing in mind the possible negative consequences for innovation and the administrative burden that could result in a broader set of applications being regulated.
- As with many other products and services offered in the marketplace that have complex supply chains, every AI product and service can be associated with a person or business entity that can be held liable. There is nothing inherently different about AI that would make it more difficult for a person to find a party liable and seek compensation accordingly.
- On the potential for AI to result in "discriminatory outcomes", we make our submission based on our understanding that the term is intended to mean "negative discriminatory outcomes". It ought to be kept in mind that the standalone term "discriminatory" could otherwise mean differentiation or indeed positive discrimination, which can be used to correct unintended bias in AI for example.

On whether some of the concerns about AI expressed in the questionnaire can be addressed by applicable EU legislation, EDiMA would like to make the following specification:

- Most of the concerns raised by AI applications are addressed through already existing legislation, for example GDPR on biometric data, the recently adopted P2B Regulation and consumer law as recently revised on transparency requirements for ranking guidelines.
- A one-size-fits-all approach will not work when it comes to AI as it carries the risks of being too rigid, it could become quickly outdated and could stifle innovation. There needs to be space left for tests and innovation, via sandboxing for example.
- EDiMA is not opposed to new legislation in principle, but it needs to be targeted and focused on the AI applications that pose the greatest risk of harm to human beings. Such applications

may already be covered by sectoral legislation, such as in health or financial services, so any new regulatory initiative should build on existing regulatory framework.
- The potential gaps identified could be filled by appropriate guidance and definitions coming from the European institutions. Such guidance should be sector specific. It would prevent fragmentation across the different Member States while allowing for flexibility to adapt to the rapid developments observed when it comes to AI applications.

Reflecting on whether there is a need for new compulsory requirements being limited to high-risk applications (where the possible harm caused by the AI system is particularly high):

- EDiMA believes a risk-based approach is important, and agrees that low-risk applications should not be subject to a regulatory burden. The concept of establishing cumulative criteria to easily identify high-risks applications is workable provided such indicators are clear and proportionate, and sufficiently nuanced to take into consideration the large diversity of AI applications.
- In this regard, we believe adjustments are needed, for instance, in order to ensure that regulation is proportionate and appropriately targeted in order to provide legal certainty. Thus, the Commission should consider the opportunity cost of not using AI, emphasise the need for proportionality, remove open-ended clauses that create legal uncertainty, e.g. “exceptional instances” such as impact on consumer rights and remove the reference to “immaterial damages” in the risk definition.
- Furthermore, in order to ensure high levels of legal certainly, the process to decide whether new sectors should be added to the list of ‘high-risk sectors’ must be robust and transparent, taking into consideration the views of relevant experts and with extensive consultation with industry. The decision to add a sector to the list should be followed by reasonable transition period to ensure preparedness for AI developers.

On the use of remote biometric identification systems or RBIS (e.g. facial recognition) and other technologies, EDiMA would like to clarify its response on its use in public spaces only in certain cases or if certain conditions are fulfilled:

- As the use of RBIS in public spaces are currently being experimented all over the world (incl. the EU), they remain a matter of concern in the public debate as they touch upon very sensitive personal data, e.g. facial features in the case of facial recognition.
- In particular, the use of RBIS in public spaces by national governments, law enforcement agencies and private entities could have very important negative effects on fundamental rights. Fear of mass surveillance is a legitimate concern.
- It is important to emphasise that the Law Enforcement Directive and the GDPR are applicable to the use of RBIS. Under the latter, biometric data is considered a special category of personal data and its processing is in principle prohibited unless a legitimate exception applies.
- Ultimately it is up to governments to decide on particular approaches to further regulation of these technologies. However, some important factors that governments should consider

include: whether these technologies are required for public security; if they have been pre-approved as being reasonable and proportionate use; and whether there is a practical way of achieving the same ends without the use of such sensitive data.
- It is important to point out that RBIS in public spaces can be used for good, for example to help find missing children.
- However, most of these systems still feature a very high rate of error and lack of accuracy.
- A public debate is necessary on the place RBIS should have in our societies, and to what extent their use can be compatible with EU values.

On whether voluntary labelling systems would be useful for AI systems that are not considered high-risk in addition to existing legislation, EDiMA would like to further explain why it answered in the negative (i.e. “rather not”):

- The introduction of a voluntary labelling system when it comes to non-high risk AI applications could face many limits in practice.
- If the goal is to introduce one single labelling system, it will have to be flexible enough to accommodate the diversity of AI applications.
- EDiMA does not believe that a simple list of cumulative criteria to get the label will be useful: companies should be able to choose the most effective measures fitting their product or service. This is crucial if we want the voluntary labelling system to have any uptake, especially across SMEs and start-ups.
- In addition, this labelling system would have to be adaptable enough to keep-up with the fast-moving pace of innovation in AI.
- A labelling system that is not flexible enough could quickly become outdated and provide false assurances to consumers, ultimately undermining their trust in AI applications.

On the best way to ensure that AI is trustworthy, secure and in respect of European values and rules EDiMA believes another enforcement system is needed. Ex ante conformity assessment requirements do not strike the right balance. A combination of ex-ante risk self-assessment and ex-post enforcement for high risk AI applications would likely achieve similar results much faster and without risking unduly stopping innovation and creating unnecessary burdens. This would also build on existing industry practices, including the ethical, legal and due diligence practices that guide the responsible and trustworthy development of AI.

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

On whether there are any further risks to be expanded on to provide more legal certainty:

- EDiMA would like to emphasise that the safety of users is a top priority for EDiMA members. It is essential that consumers feel confident that they will find a comprehensive offer of safe and reliable digital services in the online environment.
- EDiMA believes that current product safety legislation continues to be an adequate tool in light of new technological developments, including AI and other emerging digital advancements such as IoT.

Regarding risk assessment procedures:

- Due to the great variety of digital products facilitated by AI, an approach that takes due account of the specificities and lifetime stages of the products, including the levels of risk involved, is essential. A differentiated risk-based approach will allow Europe to remain an attractive destination to invest in digital innovation.
- The current EU liability framework is a stable framework that incites investment, innovation and smart risk-taking. EDiMA expects these values to be maintained.

As to whether 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:

- EDiMA believes that while the current national liability rules do not contain liability rules specifically applicable to damages resulting from the use of emerging technologies including AI, the harmful effects of the operation of emerging digital technologies should primarily be addressed by the ethical and safety frameworks and can additionally be compensated under existing laws on damages in contract and extra-contractual liability rules.