Mastercard's response to the EU Commission AI White Paper

Mastercard welcomes the opportunity to provide feedback to the European Commission on its White Paper: "On Artificial Intelligence – A European approach to excellence and trust" (the "**White Paper**"). The present document, together with Mastercard's own AI White Paper ("Towards a European AI Framework"), aims to provide further context to Mastercard's responses to the public consultation on the White Paper.

The present document focuses on the following topics, following their order of appearance in the White Paper:

1. International cooperation in the context of AI
2. The mandatory requirements of a possible future regulatory AI framework
3. The regulatory oversight and the authorities competent for such regulatory framework

1. International cooperation

Mastercard welcomes the European Commission's aim for international cooperation on AI, as outlined in Section 4.H of the White Paper. As technology and data are key elements of an increasingly borderless global economy, it is essential that any policy in relation to AI takes into account this international dimension and aims for compatibility with approaches taken in third countries. Any ban or restrictions on the use of technology developed outside the EU risks disadvantaging EU organizations compared to organizations in third countries. It should be considered that several EU organizations that have the capability to develop AI in the EU, may rely on non-EU suppliers for parts of their IT support model (e.g. hosting and cloud capabilities, AI components).

We therefore believe that the scope of application of any AI regulatory framework should be based on where the service involving AI is being delivered, ensuring that any services provided in the EU have to comply with similar rules, irrespective of whether an AI model, algorithm, service or product has been developed in the EU or in a third country.

2. Mandatory requirements for high-risk AI applications

Section 5.D of the White Paper (Question 2.6 of the Public Consultation) lists the following mandatory requirements of a possible future regulatory framework for AI:

1. The quality of training data sets
2. The keeping of records and data
3. Information on the purpose and the nature of AI systems
4. Robustness and accuracy of AI systems
5. Human oversight

6. Clear liability and safety rules

While we agree that all these principles are important in an AI context, we consider most principles (1-5) already covered by mandatory requirements in the existing legal framework such as the General Data Protection Regulation ("**GDPR**") when personal data is involved. For purposes of legal certainty, any processing of personal data in the context of AI should remain fully subject to GDPR.

Sector-specific regulation covers some of the above-mentioned requirements as well. For instance, the Directive on payment services ("**PSD2**") requires robust governance arrangements for payment services and establishes payment service providers' liability for unauthorized payment transactions, including when AI is relied on for such services.

Therefore, any further mandatory requirements on the above-mentioned principles should not lead to conflict with and/or duplication of GDPR and other existing regulations (e.g. PSD2). Organizations should have the possibility to implement a holistic risk assessment methodology for AI, regardless of the type of data used or the sector they are active in. Rather than having to perform several types of risk assessments, they should be able to perform a consolidated risk assessment which takes into account the GDPR as well as additional considerations specific to AI, for instance in relation to bias, explainability and auditability. Questions on safety, infrastructure stability and social impact could be considered as well.

In addition, it is interesting to note that the GDPR does not strictly prescribe how organizations should comply with the different data protection principles, which are also relevant in the context of AI. Pursuant to Article 5(2) of the GDPR, organizations shall be responsible for, and be able to demonstrate compliance with the data protection principles (i.e. the "accountability" principle). Article 24(1) of the GDPR further concretizes this accountability principle by stating that organizations shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. Yet it is not exhaustive and does not specify what those measures should look like in practice.

Therefore, any further mandatory requirements for high-risk AI applications should not be too prescriptive given that not all requirements or principles may be relevant in all circumstances. Rather, the mandatory requirements should follow a principle-based approach and provide the necessary flexibility to allow organizations to adopt measures that are "appropriate" to the particular circumstances. For example, accuracy is an important principle to consider in AI applications. Yet, aiming for maximum accuracy of an AI system is not always appropriate. In the financial sector, for instance, reducing accuracy on purpose in order to increase false positives, and thus flag more payment transactions as potentially risky, allows for extra due diligence steps in assessing fraud. Whereas, in in the abstract, reduced accuracy would be perceived as problematic or risky, in certain circumstances it can be a conscious trade-off to achieve an important benefit. Organizations should have the flexibility to make these trade-offs and decide which measures are appropriate for their given AI use case.

In light of the above, companies should be able to leverage their Data Protection Impact Assessment or other risk methodology to document AI-specific risks and benefits, as well as mitigating measures and potential trade-offs.

3. Regulatory oversight & competent authorities

The success of a possible future regulatory framework for AI is dependent on the efficiency of its regulatory oversight and enforcement.

According to Section 5.H of the White Paper, oversight and enforcement of a future AI regulatory framework will take place through a European governance structure in the form of a cooperation framework of national competent authorities, sectorial networks and regulatory authorities (e.g.

data protection authorities, financial regulators, etc.). There are no questions in the Public Consultation covering this topic.

To ensure smooth regulatory oversight or enforcement and to reduce unnecessary burden on an AI application under the future regulatory framework, we believe it is critical to have one authority taking the lead and operating as single point of contact towards the organization concerned. For purposes of legal certainty, the data protection authorities ("**DPAs**") should retain general competence over AI applications involving the processing of personal data, including where such applications have a potential impact on individuals' fundamental rights and freedoms, in accordance with Article 1 GDPR. As such, they should be in a leading position and single point of contact for the organization for oversight of any AI application involving personal data processing, but with the possibility to collaborate with other authorities where necessary. For instances where AI does not involve the processing of personal data (e.g. AI used for manufacturing processes), it could be envisaged that the authority with the most relevant expertise (e.g. because of the sector in which the AI is deployed) takes the lead and cooperates with other authorities where needed.

Ensuring effective cooperation between different authorities should however not be underestimated. Article 63 of the GDPR puts forward the consistency mechanism, according to which the EU DPAs must cooperate with each other and, where relevant, with the Commission in order to contribute to the consistent application of the GDPR. However, since the entry into application of the GDPR, it has proven difficult and burdensome for the different DPAs to put this consistency mechanism into practice and collaborate in an efficient way. This has led to diverging opinions and interpretations, which runs counter to the GDPR's initial objective of harmonization.

A cooperation framework for AI should learn from the experience with the GDPR consistency mechanism and build further on its (limited) achievements. Any AI regulatory framework should therefore clearly spell out how a cooperation of different authorities at different levels must work in practice. We further believe thorough consideration is needed on what authorities should be included in the cooperation framework in order to avoid ineffective enforcement which would undermine EU citizens' trust in AI and the digital economy.

Mastercard thanks the European Commission for the opportunity to provide these comments to the White Paper.