TOWARDS A EUROPEAN AI FRAMEWORK

I. Context

Policy makers and regulators globally are increasingly focusing on the responsible and ethical use of data, in the context of Artificial Intelligence (AI). Mastercard welcomes the efforts made by the European Commission to develop a normative framework which ensures trustworthy AI and benefits European people and society. As a digital leader in the payments ecosystem that keeps data ethics at the heart of its approach to innovation (see our Data Responsibility Principles), we hereby provide our views on a framework that should underpin the development, deployment and use of AI.

II. Vision

To achieve trustworthy AI, a normative AI framework must be driven by respect for an individual's privacy and other fundamental rights. As such, it should take into account ***the impact that any AI development, deployment and use may have on individuals***. It also requires a principle based and flexible approach rather than a prescriptive one to ensure:

a. ***It is future proof and technology neutral*** so as to swiftly adjust to technological and societal changes
b. ***A level playing field*** to enable all participants across industries to compete and innovate
c. ***Consistency with other laws and regulations*** including the EU General Data Protection Regulation.

III. Normative Framework

A normative AI framework should take into account existing laws and regulations and must be based on the following key principles:

- **Human-centered -** Individuals must be placed at the center of the design, development, deployment and use of AI. AI technology must take into account its impact on human beings and the society. AI actors[1] must evaluate the risks and positive outcomes, in particularly related to:
  - safety and security
  - privacy, data protection and other fundamental rights
  - how AI can improve human capabilities and how it can benefit society as whole.
- **Transparency –** AI technology must take into account the principle of transparency, including:
  - *Knowing when it's AI* – AI Actors must take steps to communicate the existence, purpose and potential impact of AI technology.
  - *Understanding how it works* - The way AI technology arrives at its decisions and how it functions must be explainable according to the audience.
  - *Balancing the information shared* - Transparency as a cornerstone in trustworthy AI must be balanced with the need to ensure that proprietary information remains protected, and that malicious actors are not encouraged to bypass the AI system (e.g. a fraud prevention tool).

[1] All stakeholders that design, develop, procure, integrate, deploy and use AI.

- **Fairness -** AI technology must be designed, deployed and used in accordance with the principle of fairness, including:
  - *Bias* – AI actors must take technical, operational and organizational measures to identify and protect from biases in the input data, the process, or the output.
  - *Data Quality* – Taking into account the risk on individuals, AI actors must take steps to assess and improve data accuracy, reliability, completeness, diversity, as well as relevance.
  - *Human Oversight* – AI actors must provide a mechanism for individuals to have AI automated decisions reviewed by a human.
  - *Recourse* – Individuals negatively affected by decisions made by AI technology must have the right to challenge the decision and seek recourse.
- **Accountability –** AI actors must be responsible and must be able to demonstrate accountability, including:
  - *Assessment*, *Monitoring and Review* – The development, deployment, and use of AI technology must rely on *ex-ante* assessments which take into account potential risks and impacts on individuals, establishing controls and safeguards to mitigate those risks as well as trade-offs, when necessary. Regular monitoring, post-*facto* assessment of AI technology and uses as well auditability of AI results should also be implemented.
  - *Documentation* – The use of AI technologies (and the data used in connection with the technologies), the decision making process, and the identified risks and mitigations must be clearly documented.

IV. Mechanisms to foster compliance

To ensure consistency and legal certainty with respect to the normative framework, it is important to note that all principles above are enshrined in the General Data Protection Regulation ("GDPR"). Given that the GDPR establishes a good threshold for trustworthy AI, an AI normative framework, should not contradict or duplicate this, but rather build upon existing legislation (see Appendix for a concrete application).

Consequently, a normative AI framework could combine multiple regulatory options to both address the potential risks and capture the huge opportunities created by AI. While new legal instruments may be appropriate in some cases, there is a wide range of legal instruments which are already in place and should be leveraged. A normative AI framework should therefore focus on practical mechanisms to foster compliance with the existing principles, as well as accountability tools in line with the GDPR. A flexible approach could bring significant business, regulatory and societal benefits.

In particular, this should include:

- ***Accountability toolkit*** – The GDPR introduces tools for companies to demonstrate compliance, including (i) policies, (ii) data mapping ("records of processing"), (iii) appointment of a data protection officer, (iv) Privacy by Design, and (v) data protection impact assessment for high risk activities. Those tools could be leveraged and adjusted for AI purposes. This would allow both businesses and regulators to rely on one single "Accountability Toolkit" to demonstrate compliance with GDPR and AI obligations.
- ***Certification*** – Certification mechanisms serve to establish consumer trust in the use of technologies. Certification mechanisms could be established at EU level to allow AI actors to demonstrate their compliance with the AI normative framework. To maintain technology

neutrality, certification should focus on AI controls and safeguards, rather than certification of specific AI tools, solutions and/or personnel.

- ***Codes of conduct*** – While an AI normative framework should have pan-industry reach, sector-specific codes of conduct could be encouraged to provide guidance on industry-specific use cases.
- ***Enforcement*** – Several EU Data Protection Authorities ("DPAs") already assess AI and its impact on privacy and other fundamental rights. This is in line with the resolution of Data Protection and Privacy Commissioners during their International Conference in 2019 to safeguard privacy, data protection but also other fundamental rights more broadly[2]. The European Data Protection Board as well as some DPAs separately have also developed significant expertise and published guidance on the development and use of AI in recent years[3]. There is a risk that having multiple authorities involved in supervising and enforcing AI could lead to legal uncertainty, market fragmentation and ultimately undermine consumers' trust in AI. It could ultimately undermine the objective of setting the European Union as a world leader in responsible and trustworthy AI. In this context, the Data Protection Authorities will need to play an important role in ensuring the effective implementation and enforcement of the AI normative framework.

- ***Research and Development*** - To foster the design, development, deployment and use of trustworthy AI, it is essential to invest in research and development in key areas, such as Privacy Enhancing Technologies ("PETs"). In particular, investment on anonymization methodologies can preserve the value of datasets by generating non-personal data insights. It is key to keep in mind that data is contextual, which means that even non-personal data can become personal, for instance when combined with other datasets. There is currently legal uncertainty as to what it takes for companies to anonymize data in the light of the GDPR. Such PETs may include homomorphic encryption, synthetic data and differential privacy, as well as a solutions provided by expert anonymization providers like Truata (co-founded by Mastercard and IBM: https://www.truata.com/).
- ***Education and university curricula*** - Education of workforce and university curricula on AI and on how to use PETs is key. Private-public sector partnerships that promote knowledge transfer between academia, industry, Small Medium Enterprises and public authorities should be encouraged in order to ensure upskilling in a way that will ultimately benefits the digital economy and European society. This will create AI "literacy", jobs and incentives for AI professionals to stay in Europe.

---

[2] https://icdppc.org/wp-content/uploads/2019/10/Resolution-on-the-Conference-Strategic-Direction-2019-2021-FINAL.pdf

[3] https://www.cnil.fr/en/algorithms-and-artificial-intelligence-cnils-report-ethical-issues
https://ico.org.uk/media/2615039/project-explain-20190603.pdf
https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

International Conference of Data Protection and Privacy Commissioners (ICDPPC), Declaration on Ethics and Data Protection in Artificial Intelligence

V. Application of the Normative Framework and Mechanisms

We have set out a use case in the Annex which provides a description of how the normative framework and the mechanisms could potentially apply.

ANNEX – USE CASE

According to the latest European Central Bank (ECB) report[4], the total value of fraudulent transactions annually amounts to €1.8 Billion, making the need for fraud prevention services greater than ever. Apart from credit card fraud, fraudsters have moved to new areas such as account fraud, phony merchant debit cards and prepaid cards, fraudulent reward programs and malicious takeover of mobile phone accounts.[5]The report notes that 73% of the value of card fraud resulted from card-not-present (CNP) payments, which occur when a fraudster deploys malicious means (e.g. malware) to steal a cardholder's data and then uses it to make unauthorized payments.

Mastercard offers Smart Authentication (**Smart Auth**), a solution designed to mitigate such risks by improving transaction authentication and reducing fraudulent transaction risks. Smart Authentication is a solution to help card issuing banks (**Issuers**) comply with the requirements introduced under the revised Payment Services Directive (PSD2), in particular, to perform transaction risk monitoring and transaction risk analysis.

When a cardholder makes a purchase with a merchant online, the merchant initiates an authentication request to confirm that the individual is the legitimate holder of the payment card. The merchant sends the individual's information to the Issuer through Mastercard's network. Mastercard Smart Authentication is the solution which, based on the EMV 3-D Secure industry standard[6], helps the Issuer identify fraud in authentication messages sent from the merchant.

Smart Auth is supported by algorithmic models which provide insights on fraudulent authentication patterns. Algorithmic models have proven to be extremely valuable in this context. Detecting fraudulent patterns is usually based on large multi-country data sets, as fraudsters will use similar methods from one country to another and then attempt to take them globally. While human logic would be slower or unable to identify such complex patterns in the first place, AI makes this process more efficient and effective. As a result, with Smart Auth, when a new authentication request comes in, the models immediately attribute a risk score and reason code to each payment transaction.

How the GDPR applies in practice

The GDPR is a legal instrument with broad application to AI. The definition of personal data which includes any information relating to an identified or identifiable natural person includes authentication data which would be processed as an input to AI, as well as the AI outcome (e.g. Smart Auth assessment of a transaction and/or risk profile).

[4] https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1809_fifth_report_on_card_fraud.en.html
[5] https://www.forbes.com/sites/tomgroenfeldt/2019/03/18/credit-card-fraud-is-down-but-account-fraud-which-directly-hurts-consumers-remains-high/#5ded226820bf
[6] EMVCo 3-D Secure is an industry standard designed to help merchants and issuers authenticate card-not-present transactions. EMVCo is a standardization body overseen by six member organisations—American Express, Discover, JCB, Mastercard, UnionPay, and Visa—and supported by dozens of banks, merchants, processors, vendors and other industry stakeholders.

AI Principle	*GDPR Requirement*	*What Mastercard is doing*
Human-centered	Under Recital 4, the GDPR is designed to serve the mankind. Therefore, the protection of personal data is one of the fundamental rights and freedoms that it is meant to protect. This is confirmed throughout the GDPR (Articles 6, 33-36 and Recitals 75, 84) where the data controller[7] must assess whether the activity creates a risk to the rights and freedoms of individuals.	To follow the letter and spirit of the GDPR, Mastercard places the individual at the center of its product development with its Privacy by Design process. It means that we embed safeguards and controls in the design of every product, solution and technology, to protect people's data and human rights. Regarding Smart Auth, in particular, Mastercard not only assessed and documented the impact of this AI innovation would have on cardholders' data protection but, also, on other fundamental rights, such as privacy, autonomy, equal treatment. We also looked at what the impact could be on society as a whole.
Transparency	Under Article 5 (1)a of the GDPR, personal data shall be processed in a transparent manner. Recital 58 of the GDPR introduces the principle of transparency, requiring information addressed to individuals to be concise, easily accessible and easy to understand, as well as communicated in clear and plain language.	Smart Auth is a solution offered to Issuers and not to individuals directly. To comply with the transparency requirement under the GDPR, Mastercard has developed technical controls which explain the input, output and logic of the algorithm. These controls are included in documentation which is offered to Issuers on a confidential basis so they can take informed decisions when using Smart Auth, i.e. when they authenticate a cardholder. This documentation contains technical information about how the model was developed and can be helpful to understand how it generates outcomes. However, it is not appropriate to share information broadly with cardholders, given it is too technical and reveals business confidential information that fraudsters could use to "game" the authentication process.
Fairness	The principle of fair processing is introduced in various places within the GDPR, including as a core principle in Article 5§1(a). Under Recital 71, the Controller must implement	To comply with the fairness requirement under the GDPR, Mastercard has put in place technical and organizational controls. In particular, Mastercard takes steps to evaluate and improve data quality in the data sets used for the AI models developed for Smart Auth under Article5§1(d) GDPR. In addition, to protect

[7] The entity which determines the means and purposes of data processing.

AI Principle	*GDPR Requirement*	*What Mastercard is doing*
	technical and organizational measures in order to minimize risks and prevent discriminatory effects of profiling and data processing.	Smart Auth from bias and discrimination, we built technical controls to monitor our AI models in order to identify drift and report significant change within the model behavior. We also developed auditability tools to support Issuers when cardholders seek recourse.
Accountability	Articles 24, 30 and 35 require data controllers to be able to demonstrate compliance by implementing organizational measures. In particular, by performing impact assessments, keeping records of data processing, and generally ensuring accountability, incl. allocating liabilities.	Mastercard performed an impact assessment for Smart Auth and has documented it in internal documentation and records of data processing. Mastercard also developed network rules which function as the contractual basis to allocate liabilities when necessary. Going further, Mastercard appointed a Chief AI Officer in addition to its Chief Data Officer and Chief Privacy Officer, and established an AI Governance Framework as well as an AI Governance Council which is consulted each time the use of AI involves medium or high risk.

Mechanisms to foster compliance

Certification – There is currently no certification mechanism to allow Mastercard to certify that its AI processes specifically comply with industry standards and existing laws. A voluntary certification scheme could help encourage the uptake of AI solutions in the market, as it may reduce the time required for due diligence and customer negotiations. It would also increase corporate customers and eventually consumers' trust in AI.

Code of conduct – The GDPR includes industry-wide technology neutral rules on transparency, accountability, fairness and liability. It also establishes a good threshold for a future AI normative framework. The financial sector may benefit from establishing a voluntary code of conduct to specify how this framework works in practice.

Supervisory authority – The DPAs would be likely to consider themselves competent when case specific issues arise with regards to the principles highlighted in this paper, as demonstrated by the International Conference of Data Protection and Privacy Commissioners resolution concerning the conference's strategic direction[8] . To avoid the risk of legal uncertainty, the DPAs could supervise and enforce the AI normative framework.

[8] https://icdppc.org/wp-content/uploads/2019/10/Resolution-on-the-Conference-Strategic-Direction-2019-2021-FINAL.pdf