Monero Policy Working Group (MPWG)
Date: 27/12/2020

Response to the consultation request from the European Commission regarding REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937.

Submitted by: Monero Policy Working Group
Authors: Jayson Benner, CPA, CA; Dr. F. X. Cabañas; Dr. J. Dubois-Lacoste;
Deanna MacDonald; Justin Ehrenhofer;
Dr. R. Renwick; Asst. Prof. Dr. A.J. Santos.
Contact: policy@getmonero.org

Introduction

1. The Monero Policy Working Group (MPWG) is a loosely formed quorum of individuals that contribute to the Monero[1] open-source project. Monero is a permissionless, privacy-preserving cryptocurrency network. The goal of MPWG is to work with regulators, policy makers, and the wider financial services sector to ensure broad understanding of Monero, and other privacy-preserving cryptocurrencies, is communicated. We have specific interest in interacting with entities so they may understand Monero's component technologies, especially with regards to evolving regulatory framework and compliance requirements. We thank you for the opportunity to respond to the proposed Regulation concerning Markets in Crypto-assets, and amending Directive (EU) 2019/1937. We give consent for our contribution to be publicly published in full.

2. We would like to take the opportunity to communicate our support for the Regulation concerning Markets in Crypto-assets (MiCA). We believe that clarity is required, and welcome harmonisation across Member States, echoing the sentiments of President-elect Ursula von der Leyen, to Vice-President Dombrovskis, in September 2019. We also welcome and support initiatives to regulate the Initial Coin Offering (ICO) market, especially in the interests of investor and consumer data protection. We also share common concerns regarding fraud, money laundering, and terrorist financing.

3. We support the views contained within the initial impact assessment conducted by DG-FISMA Unit B2, especially as they relate to the cost-benefit analysis for environmental impact, freedom of establishment within the Digital Single Market (DSM), and the protection of personal data of individuals. We also welcome clarity on the role of decentralisation in consumer protection, the role of open-source technologies for increased cybersecurity resilience, and we note the important role that self-custodianship plays in protecting the

[1] *see* The Monero Project, https://github.com/monero-project and https://getmonero.org.

individual from the increasingly malevolent activity conducted by unregulated custodians in the existing market place.

4. As a policy working group, we support any efforts by the European Commission, either directly or indirectly, to raise awareness and build relationships between the private and public sector - especially as related to the advantages and disadvantages of specific blockchain and distributed ledger applications from the perspective of data protection, security, and consumer and investor protection. We welcome efforts by the public sector to communicate and educate the general public on the advantages and disadvantages of crypto-assets, regardless of where they sit in the proposed taxonomy provided by DG-FISMA within the initial impact assessment. We feel that extending bridges to the private sector would increase harmony and foster conducive relationships between technologists, experts, and economists - ultimately creating cohesive trust between the previously bifurcated social groupings.

5. While we welcome clarity of the regulatory framework from the Commission toward the market for crypto-assets, **the Commission's stance on privacy-preserving crypto-assets is unclear**. We feel the lack of clarity on the question of privacy may, at best, cause uncertainty in the marketplace and, at worst, stagnate crucial innovation on Privacy Enhancing Technologies (PETs) and privacy-preserving technology, which will ultimately be to the detriment of privacy, as well as both personal, digital, and national security.

6. **We welcome additional guidance from the Commission with regards to the consideration of financially related privacy, as we feel it is an important tenet of a free and open society; crucial to self-determination, free will, autonomy, and congruent with both international[2] and European fundamental rights and values**[3]. We are also critically aware that transparent crypto-asset networks open very specific avenues for harm with regards to data protection and fundamental rights, and feel this should be explicitly stated by the Commission either inside this framework or by the appropriate bodies such as the European Data Protection Board (EDPB), the European Data Protection Supervisor (EDPS), or the European Fundamental Rights Agency (FRA). This is especially important given the increasingly powerful Artificial Intelligence (AI) and Machine Learning (ML) based identification and traceability techniques[4] [5] [6], which are being deployed

[2] The right to privacy in the digital age : resolution / adopted by the Human Rights Council UN. Human Rights Council (28th sess. : 2015 : Geneva), available at: https://digitallibrary.un.org/record/795309

[3] Charter of Fundamental Rights of the European Union, 2012/C 326/02, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.

[4] Sun Yin, H. H., Langenheldt, K., Harlev, M., Mukkamala, R. R., & Vatrapu, R. (2019). Regulating cryptocurrencies: a supervised machine learning approach to de-anonymizing the bitcoin blockchain. Journal of Management Information Systems, 36(1), 37-73.

[5] Zola, F., Eguimendia, M., Bruse, J. L., & Urrutia, R. O. (2019, July). Cascading Machine Learning to Attack Bitcoin Anonymity. In *2019 IEEE International Conference on Blockchain (Blockchain)* (pp. 10-17). IEEE.

[6] Toyoda, K., Mathiopoulos, P. T., & Ohtsuki, T. (2019). A novel methodology for HYIP operators' bitcoin addresses identification. *IEEE Access*, 7, 74835-74848.

by the advertising technology (Ad-tech) and related industries to extract information and profit from consumers, without their knowledge - or informed consent. We believe that this is of great importance as society increasingly conducts a larger proportion of its economic activity online. **Protecting consumers from targeted advertising (based on actual spending patterns), behavioural manipulation, and price discrimination is of critical importance to fundamental rights and consumer protection as we venture deeper into the 21st century**. This line of thinking is supported by views from within the Commission as has been communicated with the recent: Request for Services in the context of "Framework Contract for the provision of Evaluation and Impact Assessment services to DG CONNECT" - SMART 2019/0024, Lot 2 - Exploring, documenting and analysing digital policy issues. Ref: Study Privacy and Economic Impact of Adtech - VIGIE 2020-0663.

7. The relationship between financial privacy and potential harm to individuals has been previously communicated by the Commission, within its Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR[7], which clearly states **the considerable risks that may befall the data subject if correct and proper monitoring and regulation are not put into place regarding payment services and payment service providers.** We believe that appropriate monitoring and regulatory frameworks also need to be deployed within the market for crypto-assets, especially with regards to violations of GDPR data subject rights. Considerable privacy and data protection harms may befall the data subject through the combination of transparent crypto-asset networks and the increasingly powerful chain-analysis techniques available to the marketplace. These tools allow disproportionate levels of information to be garnered about individual transactions, and (of greater concern) their related chains of transactions and transacting parties, that continue beyond the scope of a business relationship. We are of the opinion that **financial transactions (whether exercised through the use of crypto-assets or not) often include 'sensitive personal data'[8]; including information about religious beliefs, political affiliation, and/or information regarding gender and sexual preferences.** Despite the importance of these matters, the right to financial privacy in the context of the protection of sensitive personal data as it pertains to financial transactions is notably absent from this proposal, and has not been explicitly addressed by the Commission nor included within the scope of consumer protection, as it is currently defined. The MPWG is of the opinion that this matter is of critical importance to the regulation of markets in crypto-assets, and is furthermore a crucial component to the Commission's stated priorities "to make Europe fit for the digital age and to build a future-ready economy that works for the people[9]".

8. Considering the above point, we would like to clearly state that some provisions of the Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR should be addressed in the context of the MiCA proposal, in particular:

[7] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202006_interplaypsd2andgdpr.pdf.
[8] Recital 51, Regulation (EU) 2016/679 (General Data Protection Regulation).
[9] A Europe Fit for the Digital Age, available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en.

a. "Where a data breach involves financial data, the data subject may be exposed to considerable risks. Depending on the information that is leaked, data subjects may be exposed to a risk of identity theft, of theft of the funds in their accounts and other assets. Furthermore, there is the possibility that the exposure of transaction data is related to considerable privacy risks, as transaction data may contain references to all aspects of a data subject's private life. At the same time, financial data are obviously valuable to criminals and therefore an attractive target[10]."
b. "The processing of personal data by payment service providers may entail 'profiling' as referred to in Article 4 (4) of the GDPR. For example, AISPs could rely on automated processing of personal data in order to evaluate certain personal aspects relating to a natural person. A data subject's personal financial situation could be evaluated, depending on the specifics of the service. Account information services, to be provided as requested by users, may involve an extensive evaluation of personal payment account data[11]."

Consistency with existing financial markets - Fees

9. In addition to the overarching concerns communicated above, the MPWG welcomes additional clarity from the Commission regarding crypto-asset transaction fees. Transaction fees fall under two general categories: (1) on-chain "network transaction fees" mandated by the crypto-asset protocol, and (2) fees charged by trading platforms and other entities that custody or transmit crypto-assets ("withdrawal fees"). Network transaction fees are, at times, more transparent in crypto-asset networks than the incumbent card-based payment system counterparts, including within privacy-preserving crypto-assets where the fees applied to transactions remain public. However, certain networks may require, as a part of their consensus rules, that a certain portion of transaction fees must go to a specific entity other than the one who verifies the transaction. These are often called "developer rewards" or "founder rewards"; wherein a portion of every transaction fee is redirected back to the crypto-asset founders, with no reasonable choice, opt-out, or consent mechanism on behalf of the consumer. This is especially of concern given the inherent centralising force of such mechanisms. Regarding withdrawal fees, the MPWG believes that **crypto-asset trading platforms should make a reasonable effort to provide their customers with a fair and reasonable cost for withdrawing crypto-assets from their platform**. In cases where the total withdrawal fee exceeds a fair and reasonable network transaction fee, customers should be presented with the additional amount, and the distinction between the two should be clearly communicated.

10. The MPWG also welcomes open communication from the Commission with regards to how transparency and fairness should be achieved regarding transaction fees in the crypto-asset sector, especially how they will be regulated, overseen and, more specifically, the

[10] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202006_interplaypsd2andgdpr.pdf, para. 68.
[11] ibid, para. 79.

application of network transaction fee algorithms by both trading platforms and custodial crypto-asset wallets. We are not certain how these issues are viewed by the Commission, and we believe it to be a considerable avenue for potential harm, misuse, and a distinct threat to consumer protection and market integrity. **We believe the transparency of network transaction fees and withdrawal fees should be treated with due care and diligence by the Commission.**

Article 4

11. While the Regulation provides clarity on the obligation of crypto-asset founders, it is unclear what obligations are required of open-source project contributors and developers. We believe **it is of utmost importance to provide certainty and protection to software developers who are working on projects that are directed towards serving the public good, or towards the development of open, permissionless ledgers**. In fact, within the Regulation, Article 4 has no provision for an issuer wherein the founder, or current developers, are not identifiable, as is often the case for open-source and decentralised projects such as Bitcoin and Monero. It is unclear whether this is merely an oversight by the Commission, or strategic. If the latter, we welcome clarity on the matter through official communication. We strongly believe in the democratisation of crypto-asset network creation and believe that open-source methodologies provide an avenue for both governance and participatory inclusiveness. We also believe that **decentralisation is a core element of security, whether viewed from the perspective of availability, integrity, or resilience (and/or combination thereof).** On this matter we would point to existing guidance on "De-Centralized Virtual Currencies" as provided by the United States Department of the Treasury and Financial Crimes Enforcement Network[12]. This guidance defines a "De-Centralized Virtual Currency" as having the following properties:

    a. has no central repository and no single administrator, and
    b. persons may obtain by their own computing or manufacturing effort.

    This working group believes that founders, developers, and maintainers of crypto-asset networks who make a reasonable attempt to ensure the crypto-asset network remains decentralised and/or permissionless in terms of verification, block or transaction signing, and custody of funds, **should be given a specific exemption to the requirements listed in Article 4**.

Article 68(1)

12. We would like to draw particular attention to Article 68(1), which states: "the operating rules of the trading platform for crypto-assets shall prevent the admission to trading of crypto-assets which have inbuilt anonymisation function unless the holders of the crypto-assets and their transaction history can be identified by the crypto-asset service providers that are authorised for the operation of a trading platform for crypto-assets or by competent authorities.[13]" In this regard, **it is unclear what an "inbuilt anonymisation**

[12] https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.
[13] MiCA, Article 68(1).

function" means, so we would welcome clarity. As of the publication date, there is no national, European, nor international definition of such phrase that we are aware of. We believe that complete anonymisation is technically and practically impossible to achieve, so this group does not understand how a trading platform can make a fair assessment of what an "anonymisation function" is without a clear definition, framework for assessment, or prior guidance.

13. We welcome boundary work to be undertaken that establishes clear guidelines on the role that anonymisation and de-anonymisation techniques have in both the public and private spheres in the context of protecting privacy while fulfilling regulatory requirements. **Without this, it remains distinctly unclear how the Commission delineates between critical privacy and security features, as detailed in specifications, standards, and technical reports, such as those produced by ISO TC307 - Blockchain and Distributed Ledger Technologies[14], and said "inbuilt anonymisation functions."** Does the Commission view these as one and the same? If so, this seems to suggest that the Commission does not advocate for basic privacy to be afforded to the data of users engaged in trading of crypto-assets. This appears inconsistent with Article 88 of this same Regulation and, of even greater concern, seems at odds with guidance and opinion provided by the European Data Protection Supervisor, and advisory bodies, such as the EDPB. Therefore, we would urge the Commission to provide clarity on this matter, either through DG-FISMA, the EBA, or through appropriate bodies, such as DG-JUST, the EDPB, or EDPS.

14. Without clear technical definitions and boundaries this group is concerned about the potential for an overly broad interpretation of the terms "anonymisation function", "holders", and "transaction history". This vagueness could lead to inconsistent interpretation of the Regulation. For example, in the case of Bitcoin, an address that is created from a randomly-generated private key could be considered an "anonymisation function," because the user has the ability to accept funds without these funds being directly tied to the user's identity. Additionally, the use of Schnorr signatures in Bitcoin for multi-signature wallets could also be viewed as an "anonymisation function", because it makes multi-signature transactions less distinguishable from other transactions. Furthermore, computer code is often written for a variety of purposes. Many features that improve transaction privacy in practice may also have other purposes, such as improving transaction efficiency or user security. **The MPWG recommends that the Commission provide guidance on this matter to ensure clarity and consistency.**

15. In view of the possibility of inconsistent interpretation, trading platforms may be inclined to drop support for any crypto-asset that can be viewed as having an "anonymisation function" entirely out of an abundance of caution. This would potentially have a negative impact on anti-money laundering and counter terrorist financing efforts. EU investigators could face a reduction in their oversight powers as European residents might seek out platforms in less-regulated jurisdictions, or opt for decentralised trading platforms. The MPWG believes trading platforms should be explicitly reassured that offering services related to privacy-preserving crypto-assets is permissible**.**

[14] https://www.iso.org/committee/6266604.html.

16. With regards to the ambiguous terms "holders" and "transaction history", **there is a danger that Article 68(1) may, in its current form, be read as meaning all crypto-asset holders and the entire history of transactions from the very first block mined, to the current user**. This broad understanding is not only technologically infeasible for privacy-preserving crypto-assets, it would, in effect, create a presumption of illegality for those simply maintaining some semblance of financial privacy. An all-encompassing reading of these terms would severely restrict the trading of privacy-preserving crypto-assets to the extent that it could lead to a violation of property rights.

17. **Individuals have proprietary interests over crypto-assets**. Under Article 1, Protocol No. 1 of the European Convention on Human Rights[15], people have the right to the peaceful enjoyment of their property. The right to use and dispose of one's property is also enshrined in Article 17 of the Charter of Fundamental Rights[16], where it is reiterated that individuals have the right to own, use, dispose, or bequeath his or her lawfully acquired possessions. The concept of "possessions" is not only limited to physical goods, ownership rights can extend to intangible assets[17]. For instance, trademarks[18], patents[19], and copyright[20] are considered possessions. Similarly, crypto-assets are non-physical assets with economic value and various rights and obligations are attached to this class of property. When a crypto-asset is held in a non-custodial wallet, users maintain exclusive possession and control over cryptographic keys to the exclusion of all others. Moreover, tax liabilities may arise when a crypto-asset is obtained by way of mining, staking, gift, or purchase from a trading platform, and subsequently transferred for payment of a good or service, or sold. The digital asset can be pledged as collateral, deposited into an interest bearing account, or even destroyed by "burning". Thus, crypto-assets are "possessions". As such, **any interference with the use of crypto-assets must be fairly balanced with the public interest, proportionate, and necessary**. Although there is a margin of appreciation, and courts generally do not question the wisdom of one policy over the other[21], regard must still

[15] see The Convention for the Protection of Human Rights and Fundamental Freedoms, https://www.echr.coe.int/Documents/Convention_ENG.pdf

[16] *see* Charter of Fundamental Rights of the European Union, EUR-Lex - 12012P/TXT, https://eur-lex.europa.eu/eli/treaty/char_2012/oj.

[17] It should be highlighted that Article 3(3) of Directive (EU) 2015/849, on preventing the use of the financial system for money laundering or terrorist financing (4th Anti-Money Laundering Directive) defines 'property' as "assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets." Ownership interests in a crypto asset can be proven by electronic means with cryptographic keys.

[18] *Anheuser-Busch Inc. v. Portugal*, ECHR, 11 Jan 2007 (Application No. 73049/01).

[19] *Smith Kline and French Laboratories Ltd v. the Netherlands*, ECHR, 4 Oct 1990 (Application No . 12633/87).

[20] *Neij and Sunde Kolmisoppi v. Sweden*, ECHR, 19 Feb 2013 (Application No. 40397/12).

[21] *James and Others v. United Kingdom*, ECHR, 21 Feb 1986 (Application No. 8793/79); *Koufaki and Adedy v. Greece*, ECHR, 07 May 2013 (Application No. 57665/12 57657/12).

be given to the possibility of other measures that can be reasonably resorted to in weighing the proportionality of a measure[22].

18. **The prohibition of disposing of privacy-preserving crypto-assets on regulated trading platforms is an interference.** State-sanctioned trading platforms are likely to have higher liquidity and offer better consumer protection, which would greatly affect the commercial value of non-admitted assets[23]. Denying admission of assets that have an "anonymisation function" would interfere with a widely accepted characteristic of crypto-assets — that being a medium of exchange. European merchants would be less inclined to accept privacy-preserving crypto-assets given the restriction on trading.

19. **The public interest objective can be achieved by more proportional means.** The aim of combating money laundering and the financing of terrorism can be met by requiring higher-risk users on trading platforms to disclose private viewkeys and/or signed key images that "decrypts" privacy-preserving crypto-asset transactions at the wallet level. With this private information, trading platforms would have the ability to audit outgoing transactions, prove wallet balance, and together with information that is already required to be disclosed by users in compliance with AML/KYC regulations (such as AMLD5[24]), keep a record of user identity, origin, and transfer of assets. It is also possible for users to self-declare their identity and transactions to designated authorities on a voluntary basis. These methods of disclosure would be more proportional than a blanket ban of privacy-preserving crypto-asset admission on regulated trading platforms. **This working group maintains that in most lower-risk cases, entire transaction histories are not necessary to reduce risks to an acceptable level.**

20. Therefore, MPWG recommends that **Article 68(1) should include text clarifying that "holders" means customers interacting directly with crypto-asset service providers and "transaction history" ought to be limited to platform-customer level transactions as opposed to all transactions, such as customer-customer where the trading platform is not a party to the transaction**. Where a trading platform operator finds that there are circumstances with a particular consumer that calls for Enhanced Due Diligence in accordance with risk-based AML procedures, there should be text in the Regulation on how disclosure of public keys is handled. We believe that **the anonymity of the public key is a necessary precondition for the privacy of the user of a crypto-asset.** This was understood as far back as 2008, in the Bitcoin whitepaper[25]. To the degree that the public key is anonymous to an outside observer, the privacy of the user is

---

[22] *OAO Neftyanaya Kompaniya Yukos v. Russia*, ECHR, 20 Sep 2011 (Application No. 14902/04); *Vaskrsić v. Slovenia*, ECHR, 25 Apr 2017 (Application No. 31371/12).

[23] In *Yaroslavtsev v. Russia*, ECHR, 2 Dec 2004 (Application No. 42138/02), applicant complained that the State refusal to register his car, which was purchased from an unidentified seller in Belarus, greatly diminished the commercial value. Court held that the refusal amounted to an interference with the owner's rights under Article 1 of Protocol No. 1.

[24] Directive (EU) 2018/843 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (5th Anti-Money Laundering Directive), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843.

[25] *see* Bitcoin Whitepaper, sec. 10, pg. 6, https://bitcoin.org/bitcoin.pdf.

protected. However, this does not require the anonymity of the individual user, and there exist circumstances where the anonymity of the individual user may not be desirable. In these circumstances, in order to maintain proportionality and data minimisation, strict protocols and boundaries are required to ensure the confidentiality of the public key.

21. **Moreover, the Commission should indicate in the Regulation that requests for personal data shall be reasonably aligned with user behavior, and the associated AML risk levels tied to a specific customer.** Trading platforms should collect only information that is absolutely necessary to comply with applicable AML/KYC regulations. Further, the MPWG believes that the requirements imposed on regulated entities rely too heavily on the surveillance of public transaction histories. Public transaction histories may not be available for many legitimate and defensible reasons and when they are available proprietary association methods are used, often through companies with explicit financially vested interests, which in turn may impact on any number of components; affecting impartiality and fairness in the investigation process.

TITLE VI: Prevention of Market Abuse involving crypto-assets

22. Preventing market abuse is a crucial component of financial stability and proper functioning. It is also critical to ensuring fair market practice by entities in position to benefit from information asymmetries. However, we believe that **the MiCA Regulation has failed to consider the implications for potential market abuse that may (and already does) occur in the market with regards to transparent, non privacy-preserving crypto-assets**. Open, public ledgers allow for market abuse as information typically considered "insider" or "confidential" is posted on a publicly-accessible record. The MPWG questions the overarching wisdom of TITLE VI: Prevention of Market Abuse involving crypto-assets that does not account for the above. More specifically, Article 78(1) states: "no person shall use inside information about crypto-assets to acquire those crypto- assets, or to dispose of those crypto-assets, either directly or indirectly and either for his or her own account or for the account of a third party." We question how any market abuse could be traced back to illicit activity if the only information required to 'front-run' a market are specific public key addresses (and their associated incoming and outgoing transactions). Watching these addresses from any terminal worldwide would allow a malevolent actor to know, in real time, when a large deposit or withdrawal from a particular entity, or to a particular platform, is performed. This allows third parties to observe sensitive financial data from a particular trader, or more generally allows front-running of large orders about to be made. **This seems to be a persistent failing of the vast-majority of non privacy-preserving crypto-assets, and a fundamental risk to market stability, market fairness, market integrity, consumer protection, as well as a fundamental centralising force.** We believe that specific due consideration should be made by the Commission to this point.

Regulation 2016/679 and crypto-assets

23. It is the opinion of the MPWG that **transparent crypto-asset data structures pose considerable risks to data subjects, especially considering that many have been**

deployed by legal persons (i.e., registered entities, companies, and/or foundations) with seeming disregard for Regulation 2016/679 (GDPR). The GDPR is considered an important European level regulation supporting the protection of fundamental rights. In the context of crypto-assets, the nature of data transfers and the underlying architectures, a number of considerable concerns are yet to be addressed[26]. Indeed, there is yet no published Data Protection Impact Assessment that we are aware of for a crypto-asset architecture even though it has been a legal obligation of GDPR, Article 35 since its enactment in 2018. We welcome clarity from the Commission in this regard.

24. The MPWG is of the opinion that privacy-preserving data structures are one of the few manners through which a crypto-asset architecture and its founders may remain compliant with the legal obligations of GDPR. This is due to the implementation of cryptographically based technical measures to ensure the protection of personal data. Specific mechanisms ensure that the public key of the data subject remains off-chain, with a series of privacy-preserving techniques applied as technical measures, to maintain data subject (and personal data) privacy. **These techniques have been outlined in ISO TC 307 TR 23244 - Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations[27]**. Critically, this privacy affordance does not mean that regulated entities are not able to comply with specific crypto-asset related AML/CTF requirements when offering related services, as information may be sent off-ledger between parties if required by appropriate entities, regulators, and/or financial investigation units. We believe these off-ledger mechanisms should be the de-facto arrangement for such information transfer, whilst the appropriate bodies ensure that the legal obligations of GDPR are maintained by entities, as required by law.

Conclusion

25. As a policy working group, the MPWG supports the establishment of MiCA and welcomes harmonisation across Member States. We also considerably support efforts by the European Commission to raise awareness and build relationships between the public and private sectors in the context of blockchain and distributed ledger applications from the perspective of data protection, security, and consumer and investor protection. However, the Commission's stance on privacy-preserving crypto-assets is insofar unclear within MiCA, and key terminology used throughout the document has yet to be defined. If left unchecked, this lack of clarity could have profound, and adverse implications, specifically upon Privacy Enhancing Technologies, privacy-preserving crypto-assets, and privacy in the European Union. As a technical expert committee, and stakeholder, in this policy process, the MPWG is available for any further consultation with the Commission, and welcomes the opportunity to provide opinion and perspective upon request.

[26] EPRS, Blockchain and the General Data Protection Regulation Can distributed ledgers be squared with European data protection law?, Foresight Unit (STOA) PE 634.445 – July 2019, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.
[27] https://www.iso.org/standard/75061.html.