Monero Policy Working Group (MPWG)
MoneroPolicy.org
Date: 28/11/2021

Response to a Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information accompanying transfers of funds and certain crypto-assets (recast)

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 a 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 in the context of evolving regulatory and compliance requirements.

2. We would like to take the opportunity to acknowledge the proposed package. It is far reaching and substantially developed, and we welcome the ability to respond to five concurrent public consultations on the matter.

3. We would also like to thank the Commission and DG-FISMA for the ample consultation time. It allows a multitude of stakeholders to provide opinion, perspective, and expertise on such intricate and wide-ranging legislative changes. Of course, the consultation phase also allows for due consideration of potential impacts, risks, the weighing of proportionality and necessity, as well as providing for a general level of transparency and accountability fitting of the industry.

4. We would like to draw attention to the fact that we have provided a response to four of the five public consultations. Our responses, though partitioned, should be read in aggregate and considered - where applicable - as a congruent whole.

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

Preventing money laundering and terrorist financing – traceability of crypto-asset transfers

5. It is noted within the legislative package that a core driver for the amendments is because 1% of GDP is currently involved in "suspect" activity. Simultaneously the legislative body admits legislative changes are required due to gregarious actions of *licenced entities*.[2] While we do not discount the severity of criminal activity in this regard, we feel that the balance of legislative change within this recasting impacts primarily on the *citizen* and their normal economic behaviour. Given this, we question the proportionality[3] of several articles within the proposed "REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information accompanying transfers of funds and certain crypto-assets (recast)".

6. We would like to first draw attention to the explanatory memorandum. The document provides references to recommendations from FATF, "See in particular Recommendation 15 of the Financial Action Task Force (FATF) on new technologies as modified in June 2019."[4] We would like to formally acknowledge our disagreement with the proposed broad interpretation of the FATF definition of VASP - mainly as we feel it disproportionately affects projects that are permissionless, decentralized, and open source by nature. Below we repeat our recent response to the FATF, as they sought public consultation on their *updated Guidance for a risk-based approach to virtual assets and VASPs:*
    a. The provided definition of VASP requires more in-depth consideration. It seems to state that a VASP may be "any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:...". We support the need to define what constitutes a VASP, but strongly disagree with recommendations of a broad interpretation. When interpreted broadly, as suggested, we do not feel there is a reasonable or proportional boundary of what constitutes 'non-covered activities'.
    b. We urge clarity to ensure that jurisdictions acknowledge that the private ownership, use, and interaction with blockchain networks (including validating transactions, interacting with multisig transactions as a minority key holder, as well as methods known as liquidity provision, staking, voting, and algorithmic design) distinctly do not fall under the definition of VASP activity.
    c. We would like to highlight that any movements to include natural persons acting on their own behalf would seem to alter the perceived mandate of the FATF, in a manner best described as 'Scope Creep'. Acknowledging this would be beneficial, so the public, national bodies, competent authorities, and regulatory bodies are aware of the evolution of the mandate bestowed to an international harmonisation body purported to be tasked with regulating obliged entities, in the traditional sense.

[2] FinCen files, available at: https://www.bbc.co.uk/news/uk-54226107
[3] https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf
[4] p.3

7. We welcome the strengthening of data protection rights included within Recital 17 of the recasting, but question how 'further processing' could be identified by a regulator as being conducted with any degree of certainty by VASPs. Transaction data on non-privacy-respecting crypto-asset ledgers is held on publicly viewable records. Little effort is required to conduct an analysis on data subject transaction patterns once a wallet address of a data subject is known. Further to this, non-privacy-respecting crypto-assets pose a substantial risk to consumers, given that VASPs could reasonably create highly accurate profiles of their customers using publicly available data sources. We question whether this is sufficiently accounted for within the current recasting. We urge the Commission to consider this, and provide comment (either directly through this legislative package, or through appropriate bodies such as the EDPB/EDPS) - as it may potentially have far reaching implications for both the economy and society that have not yet been considered adequately.

8. Further to the above, we would like to remind the Commission that public keys (in the form of addresses) may be viewed as personal data - especially if it is reasonably likely that a data subject can be identified using supporting information (such as an adjacent travel-rule database). In this case, it would be advisable that a public key is not directly maintained on a publicly viewable ledger, given potential data protection implications. Consequently, it is imperative that obliged entities are not explicitly required to record a public key on a publicly viewable ledger, or be prevented from dealing in a crypto asset where the public key is not immediately discernible from the publicly viewable ledger.

9. We welcome the minor note on fundamental rights on p.9 of the proposed recasting, but urge the Commision to further fortify the relation between fundamental rights and data protection. In the context of crypto-asset transfers we believe that required 'travel-rule' information (as recommended by the FATF) should, under no circumstances, be maintained on structures that do now allow for the actioning of data subject rights, such as deletion and rectification. We urge the Commission to state this explicitly, in order to ensure VASPs do not append 'travel-rule' information to the transfer of crypto-assets themselves (e.g. maintained on an immutable ledger). Further to this, the proposed recasting should specifically forbid travel-rule information being appended on public ledgers. To support this, we propose the amendments:
    a. Within Recital 33 the wording is presented as: *"It should not be required that the information is attached directly to the transfer of crypto-assets itself, as long as it is submitted immediately and securely, and available upon request to appropriate authorities"*. We believe this should be amended to: *"Information required should not be attached directly to the transfer of crypto-assets, but submitted immediately and securely, and available upon request to appropriate authorities within a separate data transfer mechanism",* or something to that effect.
    b. Within Article 14(4) we propose the following amendment from the current: *"The information referred to in paragraphs 1 and 2 does not have to be attached directly to, or be included in, the transfer of crypto-assets."* to *"The information referred to in paragraphs 1 and 2 should not be attached directly to the transfer of crypto-assets."*

We welcome the opportunity to provide suggestions in this regard, and would be concerned if they were not undertaken, especially as appending transfer-rule information (whether directly or in pseudonymised form) directly on ledger would seem in violation of data protection rights, currently in force.

10. Further to the above, Article 14 states that the following information is required to be transferred along with any crypto-asset transfer:

    a. originator's address
    b. official personal document number
    c. customer identification number or date and place of birth
    d. the name of the beneficiary
    e. the beneficiaries account number (where such an account exists and is used to process the transaction.

We would like to make two points regarding this obligation. Firstly, we believe this not to be proportional to the obligation to provide information found within Article 5 or Article 6 - especially since the Regulation does not prohibit information being transferred directly on-ledger. We are also unsure of why such data points are being requested, given relevant guidance from bodies such as the EDPB[5] and EDPS[6], as well as consultations received from data protection authorities[7] concerning the balance and application of privacy and data protection rights.

Secondly, we would also like to draw attention to the high-level implications of such an obligation, should it be enacted. Article 3 provides definitions for 'wallet address' and 'account number' These are referred to in Article 14 (3) wherein an obliged entity is required to record certain data points regarding the originator and beneficiary. We believe this course of action may, depending upon the crypto asset, require an obliged entity to record a public key on a publicly viewable ledger, or be prevented from dealing in a crypto asset where the public key is not discernible from the publicly viewable ledger. While we recognise the intention of the above rules, we feel they lack clarity and effectiveness, and would be cause for litigation, if not amended.

---

[5] Statement on the protection of personal data processed in relation with the prevention of money laundering and terrorist financing, available at: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-protection-personal-data-processed-relation_en

[6] EDPS Opinion on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC, available at: https://edps.europa.eu/sites/edp/files/publication/17-02-02_opinion_aml_en.pdf and Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, available at: https://edps.europa.eu/sites/default/files/publication/20-07-23_edps_aml_opinion_en.pdf

[7] GENERAL FEEDBACK for PUBLIC CONSULTATION on GUIDELINES for AML, CP128, available at: https://www.centralbank.ie/docs/default-source/publications/Consultation-Papers/cp128/data-protection-commission-response-to-cp128.pdf

11. We have pointed to the definitions provided within this recasting, specifically those provided for 'wallet address' and 'account number'. We urge the Commission to consider the clarity of these, both technically and editorially. If the recasting is adopted, we do not feel that these definitions will add the required degree of certainty. We also feel that certain interpretations would render them factually incorrect. We would perhaps draw attention to the use of the term "unique transaction identifier", as detailed in Article 5, to support any clarification in this regard - especially with regards to information required to be available upon request to designated authorities.

12. Further to the above we suggest the following wording for Article 14(3):

> "By way of derogation from paragraph 1, point (b), and paragraph 2, point (b), in the case of a transfer not made from or to an account, the crypto-asset service provider of the originator shall ensure that the transfer of crypto-assets can be individually identified, and record the originator and beneficiary (if different) unique transaction identifiers provided by the distributed ledger."

13. We welcome the provisions for data retention limits within Recital 40 and Article 21, as it seems congruous with existing data protection legislation, such as Regulation 2016/679. However, we also understand that national legislation may provide for derogations. With this in mind, we would like the Commision to ensure that the proposed EU Anti-Money Authority (AMLA) would include review of such Member State derogations on a regular basis. We would also propose that obliged entities are mandated to maintain a record of data deletion activities in order to present to the relevant authorities, or data protection authorities, regardless of any Member State derogation clause. This would support the enactment of certain data subject rights, afford appropriate regulatory bodies avenues for investigation into data protection activities, and also ensure there are the appropriate evidential chains should specific rights of redress be required, or litigation occur.

14. Broadly, we would like to question how this suite of proposed legislative changes align with the recently proposed (and consulted on) "Declaration of Digital Principles – the 'European way' for the digital society."[8] As we have pointed out within Paragraph 5 of this response (and elsewhere), there remains concern regarding the overarching proportionality, appropriateness, effectiveness, and legality of the proposed amendments. We would like to understand how this suite of proposed changes (and the implications of such) impact on Europe's ability to align itself with the stated Digital Principle goals of:

    a. Protection of personal data and privacy
    b. Protection of consumers online
    c. Non-discrimination

Conclusion

[8] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13017-Declaration-of-Digital-Principles-the-%E2%80%98European-way%E2%80%99-for-the-digital-society_en

15. We thank you for the opportunity to respond to the Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information accompanying transfers of funds and certain crypto-assets (recast). We hope you will consider the points we raise in an open and transparent manner. We give consent for our contribution to be publicly published, and are at your disposal through the email address provided above, should we be required to clarify any aspects of this response.