OPEN DIALOGUE

Building True Change Coalition Submission on the EU Proposal for a AML Regulation

Prepared by:
Lyudmyla Kozlovska
Bota Jardemalie

18 April 2024

The Open Dialogue Foundation (ODF) was established in Poland in 2009 on the initiative of Ukrainian student and civic activist Lyudmyla Kozlovska (who currently serves as President of the Foundation). Since its founding, statutory objectives of the Foundation include the protection of human rights, democracy and the rule of law in the post-Soviet area. In July 2017 the area of interest of the Foundation was expanded due to the rapidly deteriorating situation in Poland and other EU member states affected by illiberal policies implemented by their populist governments. The Foundation has its permanent representations in Brussels, Warsaw and Kyiv.

This Submission on behalf of the Building True Change Coalition (BTC Coalition) has been prepared by Lyudmyla Kozlovska and Bota Jardemalie. The Testimonials included within it are attributed to the individuals as described therein.

The Building True Change Coalition (BTC Coalition) composed of human rights defenders, political activists, Bitcoin entrepreneurs, and industry experts and coordinated by the Open Dialogue Foundation. The BTC Coalition aims to: (1) combat the abuse of Anti-Money Laundering / Countering the Financing of Terrorism (AML/CFT) within the wider range of transnational repression mechanisms; (2) promote financial inclusion in non-democratic and developing countries; (3) promote Bitcoin and stablecoins as tools to support human rights efforts and provide humanitarian aid worldwide; and (4) educate on the role of Bitcoin mining as an instrument to facilitate the adoption of renewable energy sources.[1]

Website: https://odfoundation.eu/ ; e-mail: odfoundation@odfoundation.eu

Twitter: @ODFoundation

Authors:

Lyudmyla Kozlovska	e-mail: lyudmylakozlovska@odfoundation.eu	X (Twitter): @LyudaKozlovska
Bota Jardemalie	e-mail: bjardemalie@protonmail.ch	X (Twitter): @jardemalie

OPEN DIALOGUE

[1] https://en.odfoundation.eu/projects-and-campaigns/combating-financial-exclusion-and-work-of-btc-coalition/

TABLE OF CONTENTS:

STATEMENT-COMMENTARY

During the April II plenary session, Parliament is due to vote on provisional agreements resulting from interinstitutional negotiations on the adoption of ***the Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing*** (the **AMLR**).[2, 3]

Since 2022, our BTC Coalition have conducted an advocacy campaign to prevent transnational repression in a form of politically motivated abuses of AML/CFT laws by dictatorial regimes and financial exclusion of humanitarian groups and vulnerable communities, including various classes of immigrants in the EU (such as dual citizens, refugees, and asylum seekers). Our advocacy led to the inclusion of key proposals in the European Parliament's previous draft of the AMLR voted last year, in April 2023 (the **EP AMRL draft**).[4] These crucial proposals have addressed the unfortunate realities of financial exclusion and weaponisation of banking data by the non-democratic regimes, both domestically and abroad.

Following the European Parliament's vote in April 2023, the Trilogue procedure led to the removal of all civil society recommendations, weakening the position of the only directly democratically-elected EU institution—the European Parliament. This has resulted in a considerable reduction of financial freedoms, increased financial exclusion, and heightened risks of abuse of the AMRL. This includes exposing EU citizens and residents to the potential misuse of their financial data by authoritarian regimes. These consequences for EU citizens and residents underscore the urgency and importance of civil society's call to reform the Trilogue negotiations, which are conducted behind closed doors and affect over 500 million people[5] with potentially drastic outcomes in the upcoming ALMR. Additionally, as the EU sets global financial regulatory standards, the negative language in the AMLR concerning privacy payment tools, such as self-hosted wallets and mixers, could lead to restrictions on financial freedoms in third countries and increase the potential for financial repression by illiberal regimes.

BTC Coalition is calling Members of the European Parliament to vote against proposed numerous provisions in the current draft of the AMLR, including, but not limited to, the following:

1. The post-Trilogue **AMLR expands its scope to include all types of crowdfunding platforms (see Exhibit hereto, Article 2), including based on crypto-assets and serving humanitarian purposes, designating them as intermediaries.**

   In the post-Trilogue draft, **crowdfunding platforms are considered as a high-risk ever-evolving Money Laundering and Terrorist Financing (ML/TF) channel, without regard to the increased the broader negative societal impacts leading to hinder social, entrepreneurial, and humanitarian initiatives.** This expansion could create potential consequences such as increased administrative and operational costs, reduction of the donor base due to invasive due diligence processes and reduced financial inclusion of smaller entities and projects that traditionally rely on crowdfunding.

   This unreasonable and disproportionate expansion, without any exceptions, in effect, devastates fundraising efforts for civil society organisations. In times of crisis, such as natural disasters, military conflicts, like the latest in Ukraine, or emergencies, crowdfunding becomes a rapid and effective means for civil society to gather resources.

[2] https://data.consilium.europa.eu/doc/document/ST-6220-2024-REV-1/en/pdf
[3] https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/760419/EPRS_ATA(2024)760419_EN.pdf
[4] https://www.europarl.europa.eu/doceo/document/A-9-2023-0151_EN.html#_section6
[5] "Trialogues involve a series of informal inter-institutional dialogues between the European Parliament, the Council of the European Union and the European Commission, wherein the institutions attempt to agree on a piece of EU legislation. Despite not being mentioned in the EU treaties, trialogues have become the mechanism of choice to circumvent parts of the ordinary legislative procedure, with the number of trialogues increasing very rapidly since the entry into force of the Lisbon Treaty." https://edri.org/our-work/trilogues-the-system-that-undermines-eu-democracy-and-transparency/

The proposed expansion of the AMLR to categorize all crowdfunding platforms as risky channels echoes existing de-risking practices that have already shown devastating impacts on vital humanitarian efforts.

For instance, as **president of human rights NGO Open Dialogue Foundation, a human rights defender, Lyudmyla Kozlovska,** explains, a significant precedent occurred during the Ukrainian crisis beginning in February 2022. Despite the urgent need for humanitarian aid following the Russian invasion, Ukrainian and pro-Ukrainian NGOs and volunteer groups saw their crowdfunding capabilities severely hampered. Services like GoFundMe, Patreon, Wise, and PayPal, alongside major banks, suspended numerous accounts without clear justification, citing internal policies against transactions related to "armaments, military goods, and services"[6, 7] These actions, taken under existing regulations, illustrate the potential for greater harm and hinderance to social, entrepreneurial, and humanitarian initiatives that the new expansion threatens to formalize and intensify.

For instance, **Roya Mahboub, one of the first Afghan female CEOs, living in the US, CEO of the Digital Citizen Fund, and a Fellow of Executive Education from Stanford University**, details the devastating effects of restrictive fundraising practices in the West.[8] Since August 2021, services like Western Union and MoneyGram halted in Afghanistan, worsening food and housing crises. At the same time, all major Western crowdfunding platforms have blocked fundraising for Afghan causes due to compliance issues. In contrast, Bitcoin has become an essential tool, allowing Roya's organization to directly pay Afghan women for coding and digital skills work, circumventing financial and social barriers.

The post-Trilogue AMLR requirements could do more than just slow down such humanitarian efforts; they might even halt them, adversely affecting the timely delivery of humanitarian aid and support to those in need. The broad application of the AMLR to all crowdfunding platforms could also create a chilling effect on civic engagement, where NGOs and civil society organisations will scale back their activities due to such negative consequences or self-censor to avoid the complexities and risks associated with compliance.

The challenges of current AML/CFT regulations on humanitarian efforts are already apparent. As **Andrii Kavetskyi, a Ukrainian representative of the Canadian charitable foundation SGA and former Reporting Officer for a USAID project**, has experienced that in Ukraine, beneficiaries of financial humanitarian aid have to wait for months for "urgent support". He had to switch from ways of raising funds to using Bitcoin and Tether for crowdfunding and delivering promptly financial aid. This situation illustrates the potential for even greater difficulties once the post-Trilogue AMLR requirements extend their reach to all crowdfunding platforms, potentially exacerbating delays and restricting the agile response capabilities essential for effective humanitarian assistance.

There is a **serious concern that NGOs and civil society groups engaged in crowdfunding for their non-financial activities could be wrongly scrutinised or penalised by obliged entities under the AMLR**, especially in the current compliance-driven environment, when fewer and fewer banks in the EU are willing to accept NGOs as clients. This can result in a regulatory environment that is unnecessarily restrictive and stifling for civil society activities and impact fundamental freedoms, such as the right to freely express and associate. It might limit the ability of individuals and groups to mobilise resources for advocacy, political campaigns, or social movements.

2. **The BTC Coalition is deeply concerned that, following the outcomes of the Trialogue, the AMLR no longer includes regulatory safeguards to prevent unwarranted de-risking, ensure non-discrimination, and promote financial inclusion. The deletion of Recital (32a) and Article (41a) in**

[6] https://ain.ua/2022/08/09/wise-zablokuvav-rahunky-fondiv-yaki-dopomagaly-ukrayini/
[7] https://vctr.media/ua/ne-takyj-j-idealnyj-chomu-ukrayinczi-vzhe-skarzhatsya-na-paypal-132476/
[8] https://en.odfoundation.eu/a/723329,submission-to-fatf-tools-to-prevent-abuse-of-aml-cft-laws/

Chapter III of the AMLR, as described below, represents a significant step backward in the efforts to create a balanced and equitable financial regulatory environment.

In the post-Trilogue draft of the AMLR, **all provisions in Recital (32a) (see Exhibit hereto) concerning the financial protection of vulnerable communities, including all classes of immigrants (dual citizens, refugees, and asylum seekers, among others) have been deleted.** Recitals are an integral part of any EU regulations, providing essential context, clarification, and guidance for the interpretation and application of the law.

In the EP AMLR draft, Recital (32a) was crucial for civil society since it promoted financial inclusion and emphasised the importance of not unduly denying access to financial services, **especially for vulnerable groups such as refugees, asylum seekers, human rights defenders, and NGOs**. Financial inclusion is vital for these groups to participate in economic and social life, enhancing their stability and integration into society.

The previous version of Recital (32a) advocated for due diligence measures based on individual risk assessments, which could prevent blanket denials of service and ensure that measures would be proportionate to the actual risks presented by these specific customer categories. Currently, financial institutions routinely adopt a risk-averse approach, leading to increased financial exclusion of vulnerable groups. The absence of this Recital (32a) would mean less regulatory emphasis on the need for financial institutions to adopt the risk-based approach, proportionate and effective measures to manage and mitigate risks linked to these clients. **Without this previous version of Recital (32a), the explicit connection between financial inclusion and the effective fight against money laundering and terrorist financing is weakened, reducing the incentive for financial institutions to work towards more inclusive services.**

As **Ismail Mesut Sezgin, a Turkish opposition political commentator residing in the UK and a victim of AML/CFT mechanisms abuse listed by the Turkish authorities among the FETO[9] members**, testifies: "To fight any dissent, the regime in Turkey routinely labels innocent people as terrorists. This has had a detrimental effect on my business and has caused immense stress. Every financial institution, even in the West, like Wise and Western Union, blocked my business accounts and started treating me as if I were a terrorist. The same situation occurred with TSB Bank when I inquired about a possible mortgage. The mortgage expert said she would look into my case in light of the notes in my report but admitted that it would be very difficult to process a successful application in my case. So, right now, I cannot continue with my studies, work as a self-employed entrepreneur, or have access to regular financial products such as a loan or a mortgage."[10]

A post-Trilogue of Recital (32a) is more limited compared to the previous version as it focuses more narrowly only on civil society organisations that conduct charitable or humanitarian work in third countries, without explicitly mentioning the broader range of vulnerable groups. It lacks the strong emphasis on financial inclusion, individual risk assessments, and the specific measures financial institutions should take to avoid denying services to legitimate customers. The latest version of Recital (32a) provides less detailed guidance on the implementation of the risk-based approach to ensure financial inclusion and combat ML/TF effectively. **The post-Trilogue version does not adequately address the nuanced balance between mitigating financial crime risks and ensuring financial inclusion for all vulnerable groups.**

For instance, **president of the Organisation for Economic Inclusion, a global coalition comprising youth leaders, industry experts, and policymakers, and an economist at IESE Business School, Jorge Jraissati,** testifies: "We advise MEPs to vote against this proposal, as it fails to address the most significant problem concerning AML/CFT: the fact that these laws create considerable unintended consequences for citizens, leading to the financial exclusion of millions of people. This

[9] https://spcommreports.ohchr.org/TMResultsBase/DownLoadFile?gId=33729
[10] https://en.odfoundation.eu/combating-financial-exclusion-and-work-of-btc-coalition/ismail-mesut-sezgin/

not only violates rights but also majorly constrains growth for Europe's single market. As of today, immigrants frequently face problems accessing financial instruments, such as the right to a basic payment account. This includes individuals with legal status in the country, a formal employment offer, and even dual EU citizenship. This occurs because most immigrants come from countries classified as "high-risk" by financial institutions, which elevates compliance costs and nudges banks to avoid onboarding these individuals."[11]

In addition to changing Recital (32a) and deleting the regulatory guidance on financial inclusion, the deletion of Article (41a) "*Unwarranted de-risking, non-discrimination and financial inclusion*" (see Exhibit hereto) in the post-Trialogue version of AMLR has significant negative implications for civil society and NGOs, particularly those representing vulnerable communities that already face unreasonable de-risking and discrimination by banks and other financial institutions in the EU.

The entire Article (41a) was introduced by the European Parliament in 2023 as a result of the BTC Coalition's human rights advocacy campaign. **Article (41a) was intended to prevent unwarranted de-risking by ensuring that credit and financial institutions have controls and procedures in place to avoid unjustified refusal or termination of business relationships with certain categories of customers.** It aimed to prevent these decisions based on broad characteristics like profession, country of residence or origin, or the type of business, advocating for decisions based on individual risk assessments instead. Article (41a) promoted financial inclusion and ensure that due diligence requirements do not lead to indiscriminate exclusion.

Without Article (41a), there is a heightened risk vulnerable communities and NGOs will face increased difficulties in accessing financial services. The explicit requirement for institutions to consider mitigating measures before rejecting customers based on ML or TF risks is removed, as well as the obligation for these institutions to adjust their services on an individual and risk-sensitive basis, and to avoid undue exclusion of non-profit organizations based on geographical risk, is no longer explicitly mandated. The BTC Coalition believes that in practice, vulnerable groups, activists, and NGOs may find it even harder to establish or maintain banking relationships. This exacerbates the issue of financial exclusion and undermines the efforts to ensure fair treatment and access to financial services for all EU residents and entities.

For instance, Syrian, Belarusian, Venezuelan, and Russian nationals who legally reside in the EU have encountered problems accessing the banking sector in some Member States. These individuals are sometimes effectively excluded from the financial system solely because banks associate their passports or countries of origin with higher risks and increased compliance costs. **The deletion of Article (41a) removes a critical layer of protection that helped to balance security concerns with the need for inclusivity and fairness in the EU financial system.**

For instance, the case of **Open Dialogue Foundation (ODF), a human rights NGO registered in Belgium, provides a vivid example of financial exclusion**.[12] ODF defends political activists and victims of torture and political persecution, and also exposes severe human rights violations and the misuse of international cooperation mechanisms by authoritarian regimes. ODF became a target of politically motivated persecution, legal harassment, and disinformation and smear campaigns, which falsely alleged that ODF was engaged in money laundering. These persecution, harassment and smear campaigns were organized as retaliation by three illiberal regimes. Consequently, all of ODF's bank accounts in Belgium, as well as those of its employees, volunteers, accountants, lawyers were closed due to these public smear campaigns. Despite these challenges, over the period of 7 years, ODF has won all its court disputes, including multiple libel cases, and has successfully disproven all allegations against it.[13] Moreover, the Chamber of Basic Banking Services in Belgium intervened, mandating a major Belgian bank to provide a basic bank account

[11] https://en.odfoundation.eu/combating-financial-exclusion-and-work-of-btc-coalition/jorge-jraissati/
[12] https://en.odfoundation.eu/a/723329,submission-to-fatf-tools-to-prevent-abuse-of-aml-cft-laws/
[13] https://en.odfoundation.eu/foundation/attacks-on-the-open-dialogue-foundation/

to ODF. However, without providing a written refusal or justification, the bank orally refused to open such an account for ODF. Unfortunately, the existing EU legal framework does not promote financial inclusion, nor does it offer effective and efficient solutions for preventing unwarranted de-risking or restoring bank accounts.

When adopted, the AMLR will set regulatory standards not only for Member States but also for EU membership candidates. Even existing EU AML/CFT requirements have led to significant challenges for NGOs in some EU membership candidate countries, particularly illustrated by experiences in Ukraine. According to **Tetiana Pechonchyk, head of the Human Rights Center ZMINA (Ukraine)**,[14] the regulatory measures introduced in Ukraine upon recommendations of the EU and FATF, ostensibly aimed at preventing money laundering and terrorist financing, have inadvertently led to unnecessary overregulation and operational impediments for NGOs. Ukrainian banks blocked the accounts of prominent civil society organizations like the Institute of Mass Information and the Civil Network OPORA for not being able to comply with new AML requirements. The lack of precise definitions for ultimate beneficial owner (UBOs) in NGOs and the absence of accessible guidance and practical submission options have made compliance difficult and led to financial exclusion. The EU and FATF must consider a more balanced approach to regulation that does not unduly burden civil society. Civil society organisations should be involved more in the regulatory process to avoid these negative impacts and ensure regulations serve their intended purpose without harming vital non-governmental activities.

3. The post-Trilogue AMLR **specifically targets self-hosted wallets and pear-to-peer (P2P) transactions, overlooking the fact that these are the only payment and fundraising instruments used by millions of civic and human rights activists suffering from financial exclusion or various forms of financial oppression**. Self-hosted wallets are deemed high-risk and suspicious, essentially labeled as significant facilitators of money laundering and terrorist financing.

   For instance, **a human rights defender, NY-qualified lawyer, and political refugee in Belgium, Bota Jardemalie,**[15] testifies: "While I was under legal protection in Belgium, and the Belgian Federal Police were investigating a criminal conspiracy to kidnap me from Belgium, my brother was taken hostage, arrested, and tortured by authorities back in my home country of Kazakhstan. In parallel, influenced by an online smear campaign orchestrated by the Kazakh regime, Belgian banks proceeded to de-risk me and closed all my bank accounts. Furthermore, my banking data was illegally transferred to Kazakhstan, based on fabricated allegations of money laundering by the regime. Unfortunately, my case has not been an exception, with increased compliance requirements, more and more legal residents in the EU face unwarranted de-risking and abuse of banking data, without any legal remedies. In situations like this, without a bank account, one can only rely on cash or crypto-assets, such as Bitcoin, and self-hosted wallets."

   The AMLR does not recognize that self-hosted wallets are crucial for transferring funds for humanitarian purposes to numerous non-democratic, war-torn, or failed states where traditional financial systems are either non-functional or serve the interests of ruling regimes. Such transfers often expose senders, donors and recipients — typically oppositionists, their supporters, or those in need of humanitarian aid — to various forms of repression, including transnational repression, due to the dictatorial regimes' abuse of AML/CFT laws (e.g., in Belarus, Kazakhstan, Turkey).

   During the Trialogue, Recitals (20) and (21) were revised and Article (31b) in CHAPTER III Article 31b "*Measures to mitigate risks in relation to transactions with self-hosted address*" was added (see Exhibit hereto), targeting self-hosted wallets/addresses. The practical implication of the post-Trilogue AMLR focus on self-hosted wallets is likely to be an increase in operational and compliance costs for obliged entities, which could influence their business strategies and client relationships. **The additional compliance checks for self-hosted wallets/addresses will make the**

[14] https://en.odfoundation.eu/combating-financial-exclusion-and-work-of-btc-coalition/tetiana-pechonchyk/
[15] https://en.odfoundation.eu/a/723329,submission-to-fatf-tools-to-prevent-abuse-of-aml-cft-laws/

process of converting crypto-assets to and from fiat currency more challenging, if not impossible, for activists and members of civil society who are already experiencing increasing financial exclusion from traditional financial institutions.

For instance, **Anna Chekhovich, financial director of Alexei Navalny's Anti-Corruption Foundation (FBK),**[16] testifies: "The Anti-Corruption Foundation (ACF), founded by Alexei Navalny, was recognised as an extremist organisation by the Russian government in 2021 and was forced to leave Russia. We have moved to the EU countries, where we registered a legal entity to continue our activities. However, we have been facing problems in opening a simple bank account in the EU due to banks' AML compliance, and our bank accounts get closed without any explanation. Western banks treat Russians in exile as potential money launderers, and their transactions are often treated as suspicious. This leads to living without bank accounts which is impossible in the modern world. At some point, donations were available to us only in form of cryptocurrency, but European banks refused to conduct transactions related to cryptocurrency. Paysera payment system closed the organisation's account. Many of our donors from all over the world want to support our work in the EU by donating in Bitcoin and other crypto-assets, but we cannot open a KYC wallet in the EU due to the prejudicially hypervigilant treatment by financial entities and crypto-asset service providers. For example, recently, the exchange platform Crybex froze the money of the ACF (19k EUR) when we tried to exchange Bitcoin to fiat. They don't make a refund because we are Russian citizens."

The increased due diligence requirements of new Article (31b) will also result in financial exclusion for those users who value the privacy of crypto transactions. Smaller clients with self-hosted wallets, who, due to the new Article (31b), will present a higher perceived risk relative to the financial benefits that they generate to the business of the obliged entities, will be deprioritised or even excluded from services. This is because the cost of compliance per transaction will be higher for smaller accounts, making them less economically viable for the financial institutions. As it has been happening already with NGOs, financial institutions tend to focus on larger clients or those with lower risk profiles to maintain cost efficiency in their operations.

For self-hosted wallet users, increased scrutiny and the obligations of Article (31a) to disclose more information compromise their legitimate rights to privacy, exposing them at physical risk of being identified and attacked for fund extortion if their information is disclosed.

The potential for overregulation might lead to market concentration, where only large crypto-assets service providers can afford to comply with the stringent measures. This concentration could reduce competition in the EU new digital market, leading to higher costs and less innovation in the long term. In practice, such approach will be an effective ban on members of civil society to use self-hosted wallets and will drive otherwise legitimate crypto-assets transactions into the shadows, meanwhile hindering the identification and reporting of suspicious activities. Thus, ensuring access to regulated financial platforms, including for the self-hosted wallets, is crucial for effective AML/CFT efforts.

4. Moreover, in the post-Trilogue version, **Recital (94a) (see Exhibit hereto) was deleted, which will have negative impact on the society and economy**. Recital (94a) specifically stipulated the admissibility of crypto-asset payments for goods and services, provided they are conducted by merchants through service providers regulated under MiCA. It also noted the absence of a restriction on private transactions using self-hosted wallets and no limitation on the use of self-hosted wallets in commercial transactions, as long as the merchants use regulated crypto-asset service providers. **Its removal in the post-Trialogue version has created ambiguity regarding the**

[16] https://en.odfoundation.eu/a/723329,submission-to-fatf-tools-to-prevent-abuse-of-aml-cft-laws/

admissibility of crypto-assets payments for the provision of goods and services either in store or online.

Some users of self-hosted wallets might initially perceive the deletion as positive, suggesting less regulatory oversight on their transactions. However, BTC Coalition believes this will lead to a more restrictive environment for crypto-asset transactions, including those from self-hosted wallets, resulting in more control and less freedom for legitimate users of self-hosted wallets.

Furthermore, this deletion could potentially lay the groundwork for a future effective ban on self-hosted wallets. This deletion of Recital (94a) removes a structured approach to integrating crypto-assets transactions into the EU economy. Maintaining such Recital (94a) will provide a more balanced and clearer regulatory environment that supports digital innovation in the EU while preventing AML/CFT misuse.

As **a co-founder of the New Belarus platform and the Bysol Foundation (EU), and director of the AI company Deepdee from Belarus, Jaroslav Likhachevsky**,[17] who currently resides in the Netherlands, testifies: "Shipping of funds to Belarus is a small part of our current tasks. At the moment we are launching the Digital Belarus platform. Which is aimed to be a prototype for the future Belarusian Democratic state. At a certain point, the most important civil institutes (such as healthcare, education, and judiciary) started to fall apart under the Lukashenko regime. The only way for us to keep going was to build our own institute and services in parallel. The same, we have no other choice, but to build a parallel economy.

For example, in 2021 (COVID-19 pandemic year), the regime fired hundreds of medical doctors because of their civil position, with no chance to get a new job in healthcare in Belarus. We have built the telemedicine platform to enable online consultations for patients in Belarus, hiring the same doctors, who have been recently fired. The service is registered as an EU entity. We need to process cross-border payments: (1) Salaries to doctors from the EU to Belarus, (2) Payments from the patients to the platform. None of them are safe from being revealed by the regime if we use the traditional banking system.

The team uses Bitcoin and stablecoins to deliver humanitarian aid to Belarus and support pro-democratic and anti-Russian activists on the ground.

The team's future plans include building Digital Belarus, as a prototype for the future Belarusian Democratic state, with democratic institutions, including taxation and representation, using crypto assets like Bitcoin and stablecoins **to maintain privacy and security, and to ensure they are not de-platformed or de-banked due to the upcoming Anti-Money Laundering regulation in the EU**. So, the people of Belarus could elect and finance their leaders and representatives (as Office of Svietlata Tsikhanouskaya).

At the same time, Lukashenko's regime is considering the financing of civil and democratic initiatives as financing extremists or even terrorist organisations. That's why privacy and security are our top priorities. In parallel, the Ministry of Interior of Belarus announced the development of a regulation to ban cryptocurrency peer-to-peer transactions between individuals, allegedly to combat criminal transactions."[18]

5. **BTC Coalition is also concerned that AMLR bluntly prohibits credit institutions, financial institutions and crypto-asset service providers to use all anonymity-enhancing instruments used for crypto-asset transactions,** (Article (58), and Article (1)(1)(c) in the post-Trilogue AMLR and Recital (93), Article (1)(1)(c) in the EP AMLR draft). Privacy payment instruments, such as mixers, are essential for protecting individual financial privacy and freedom in the digital age. Financial privacy should be viewed as an extension of personal privacy.

[17] https://en.odfoundation.eu/a/723329,submission-to-fatf-tools-to-prevent-abuse-of-aml-cft-laws/
[18] https://t.me/police_minsk/12242

Tools like mixers enable individuals to exercise control over their personal financial information, safeguarding them against unwarranted surveillance and abuse. For activists living under oppressive regimes, dissidents, whistleblowers, or anyone vulnerable to financial targeting, these tools can be a lifeline, providing security and privacy that could protect their lives and freedoms. Prohibiting credit institutions, financial institutions, and crypto-asset service providers from using all anonymity-enhancing instruments used for crypto-asset transactions, effectively means that individuals and organisations, as clients of those obliged entities, will lose crucial privacy protections.

Privacy instruments such as mixers are at the forefront of cryptographic research, offering advancements that can enhance the security and efficiency of digital transactions. Banning privacy instruments contradicts the principle of technology neutrality by discriminating against certain types of blockchain technology. A balanced approach that targets AML/CFT misuse while promoting innovation and privacy is more aligned with the EU's regulatory approach.

Attempts to restrict the use of private payment instruments as mixers are reminiscent of past attempts to ban Voice over Internet Protocol (VoIP) services in the United States. These concerns were largely focused on the potential misuse of VoIP technology by terrorists and other malicious actors. Law enforcement agencies complained that VoIP communications would be more difficult to intercept compared to traditional telephony, due to their digital nature and the use of varying protocols and encryption. VoIP was considered dangerous for national security, specifically surveillance and intelligence efforts aimed at preventing terrorist activities. However, eventually, VoIP was not banned but embraced, and anyone can benefit from apps like WhatsApp, Zoom, Skype, or Signal, offering free or low-cost calls and messaging over the internet, even on devices without a cellular service plan.

The prohibition against the use of privacy instruments by credit institutions, financial institutions, and crypto-asset service providers can set a dangerous precedent in the EU for governmental overreach into personal freedoms. History and examples from other countries show that tools and laws intended to combat crime are often misused or expanded beyond their original scope, potentially endangering the privacy and freedom of all citizens. For instance, Russia's repressive Law on Foreign Agents[19] originated from FATF's Recommendation 8, which states that non-profit organizations are vulnerable to terrorist financing abuse.[20] FATF's Recommendation 8 has been widely applied around the world to impose disproportionate compliance burdens on NPOs, irrespective of their size or risk level, affecting their operational efficiency and having a chilling effect on fundraising activities.[21] In some instances, it has led to the suppression of dissenting voices and civil society organizations, effectively destroying civic space under the guise of preventing terrorism financing.[22]

Experience with the internet and digital technologies suggests that outright bans are often ineffective at stopping malfeasance. Instead, they drive activities underground, making it harder for law enforcement to track and address actual illegal behavior. A more nuanced approach, focusing on illegal activities rather than the tools themselves, would be more effective and less invasive.

While the concerns driving the AMLR's stance on anonymity-enhancing instruments are valid, an outright ban would be a disproportionate response that undermines fundamental rights, innovation, and the EU's stance on privacy and technological neutrality. A more balanced approach that targets illicit use while preserving the benefits of these technologies is essential for the EU to navigate the complexities of modern finance and preserve the rights and securities of its

[19] https://www.hrw.org/news/2022/12/01/russia-new-restrictions-foreign-agents
[20] https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Fatf-recommendations.html ; https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Fatf-recommendations.html
[21] https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Unintended-consequences-project.html
[22] https://www.rusi.org/explore-our-research/publications/commentary/fatfs-recommendation-8-cure-worse-disease

citizens, without putting the EU at a competitive disadvantage in the global finance and technology markets.

6. One of the EU's guiding principles is **technology neutrality**, specifically "**the freedom of individuals and organizations to choose the most appropriate and suitable technology for their needs. Products, services, or regulatory frameworks that adhere to the principle of technology neutrality neither impose nor discriminate in favor of the use of a particular type of technology**."[23] This principle is relevant for digital technologies such as self-hosted wallets that securely store crypto-assets like Bitcoin and allow users to avoid relying on third-party services to hold their crypto-assets, thus giving them full control over their cryptographic keys and, consequently, their funds. This principle should also be considered in the treatment of privacy instruments, such as mixers.

   Applying the principle of technology neutrality to self-hosted wallets and privacy instruments would mean that regulatory frameworks should neither impose restrictions specifically targeting self-hosted wallets nor discriminate against them in favor of other types of financial technologies, such as bank- or crypto-asset service provider- managed digital wallets. Individuals and organisations should be free to choose self-hosted wallets if they believe these tools better meet their security, privacy, or operational needs without facing undue regulatory burdens that are not equally applied to other similar technologies. Similarly, the principle of technology neutrality should extend to privacy instruments like mixers, ensuring that regulations do not unfairly target these tools or favorless private alternatives, thereby preserving the right of individuals and organisations to select the security measures that best align with their privacy expectations and requirements.

7. In the post-Trialogue version of the AMLR, there was a deletion of Recital (27b), which was added in the European Parliament version. Recital (27b) could have had significant implications for the economy and society, particularly in terms of the regulatory burden on small businesses and **the principle of proportionality**. Without Recital (27b), there is a risk that small businesses, like sole traders and micro enterprises, will face the same stringent AML/CFT requirements as larger institutions. This regulatory one-size-fits-all approach can disproportionately burden smaller entities, potentially stifling their operations and growth. Deletion also undermines the principle of proportionality, which should be one of the guiding principles for the new EU Anti-Money Laundering Authority (AMLA) and all obliged entities to ensure that smaller entities are not subjected to the same level of regulatory complexity and cost as larger organisations.

   Stringent, non-proportional AML/CFT requirements could act as a barrier to market entry for new and small businesses, driving small businesses out of business, which, in turn, leads to a less competitive environment, dominated by fewer large obliged entities. Less competition among fewer large obliged entities will lead to increased financial exclusion, especially for NGOs and vulnerable communities, including all classes of immigrants (dual citizens, refugees, and asylum seekers, among others), especially after the change of Recital (32a) during the Trilogue, as discussed above.

8. The principle of proportionality, suggesting that the regulatory standards should be balanced and consider the varied nature and size of entities within a group, is also deleted in a revised version of Recital (28). The post-Trilogue version of Recital (28) omits this principle, which could suggest a one-size-fits-all approach to regulatory standards that may not be suitable for all entities, especially smaller ones or those with different risk profiles.

9. Many safeguards aimed at protecting individual rights have been either limited or completely removed in the post-Trilogue version of the AMLR. These changes are highlighted in the Exhibit attached to the Statement of BTC Coalition. Among the deleted provisions are protections for

[23] https://eur-lex.europa.eu/EN/legal-content/summary/supporting-telecommunications-networks-and-digital-service-infrastructures-across-europe.html

citizens confronting non-democratic regimes, whether in exile or within their own countries. Additionally, measures aimed at safeguarding against the phenomenon of so-called "false positives" in AML/CFT compliance have been substantially weakened or removed. This is particularly true in the realm of information processing and the reliance on credible, unbiased sources of information.

10. Furthermore, **the post-Trilogue draft neglects the significant role of regular consultations by the European Commission and/or the AMLA with civil society, as introduced in the EP AMRL.** This oversight affects a broad range of stakeholders, including industry experts, citizens and organisations experiencing financial exclusion, human rights lawyers, academia, and foreign policy experts. The lack of engagement with these groups undermines the comprehensive understanding and addressing of the AMLR's impact.

11. BTC Coalition welcomes the introduction of AMRL, which intends to harmonise the AML/CFT requirements in all Member States. However, BTC Coalition is concerned that in its current form, with its global impact even on the countries outside of the EU, as unintended consequence of increased regulatory requirements, AMLR will enable hybrid and authoritarian regimes to weaponise the EU AML/CFT regulatory framework to financially exclude and harass their opponents both within the EU and worldwide.

    For instance, as **president of the Organisation for Economic Inclusion, a global coalition comprising youth leaders, industry experts, and policymakers, and an economist at IESE Business School, Jorge Jraissati**,[24] who resides in Spain, testifies: "Authoritarian regimes and illiberal governments have been weaponising the international banking system as a tool for domestic and transnational repression. In response to this development, our network of activists has turned Bitcoin into their "bank of last resort" to support activists in over fifty countries. In autocratic countries, my network of leaders has reported that their bank accounts were either closed or their banking data was illegally used. We have also documented cases of activists in exile who have been deprived of the right to have financial services, as they are targeted with disinformation campaigns and fabricated criminal allegations, which trigger de-risking mechanisms in bank compliance."

    The BTC Coalition expresses grave concerns that the EU's AMLR could inadvertently lead to a ban on self-hosted wallets and privacy instruments, severely affecting the cryptocurrency sector and those vulnerable to oppression. We call on the European Parliament and European Commission to restore critical protective measures in the AMLR's final draft.

    With the European Parliament set to vote on this matter during the April II plenary session, BTC Coalition emphasises the need for immediate action to ensure these issues are addressed before the legislative process concludes.

[24] https://en.odfoundation.eu/a/723329,submission-to-fatf-tools-to-prevent-abuse-of-aml-cft-laws/

- [RECITAL 13] One of the 'targets' of the upcoming regulation remain all types of crowdfunding platforms, including those based on crypto-assets and serving humanitarian purposes, deemed a high-risk, ever-evolving ML/TF channel:

EP Mandate	**Trilogue procedure Draft Agreement**
[DELETED]	(13) Crowdfunding ▌ ***intermediaries, which operate a digital platform in order to match or facilitate the matching of funders with projects owners such as associations or individuals that seek funding, are exposed to money laundering and terrorist financing risks. Undertakings*** that are not licensed under Regulation (EU) 2020/1503 are currently left either unregulated or to diverging regulatory approaches, including in relation to rules and procedures to tackle anti-money laundering and terrorist financing risks. ▌ ***Those intermediaries should therefore be subject to the obligations of this Regulation, in particular to avoid the diversion of funds as defined in Article 4, point (25) of Directive (EU) 2015/2366 or crypto-assets raised for illicit purposes by criminals. In order to meet the challenges, these obligations apply to a wide range of projects, including, inter alia, educational or cultural projects and the collection of those funds or crypto-assets to support more general causes, for example in the humanitarian field, or to organize or celebrate a family or social event***.

- Analogously, under [Article 4a (new)], the low-risk exemption for certain classes of crowdfunding platforms has been removed:

EP Mandate	**Trilogue procedure Draft Agreement**
Article 4 a (new) *Exemptions for certain providers of crowdfunding services* 1. *With the exception of crowdfunding service providers covered by Regulation (EU) 2020/1503, Member States may decide to exempt certain providers of crowdfunding services from the requirements set out in this Regulation on the basis of an individual risk assessment resulting in a proven low risk posed by the nature and, where*	***[DELETED]***

appropriate, the scale of operation of such services, provided that all the following conditions are met: *a) the crowdfunding service provider exclusively promotes projects with a public benefit purpose, it does not have as a primary aim the generation of profits and, where a profit is generated, it is invested by the provider for the pursuit of the objectives of the service and not distributed among members, founders or any other private parties;* b) *the crowdfunding service provider implements minimum due diligence requirements in respect of project owners that propose their projects to be funded through the crowdfunding platform in a manner consistent with Article 5 of Regulation (EU) 2020/1503 and all the natural persons involved in the senior management fulfill the criteria set out in Article 6 of Directive (EU) 2023/... [AMLD VI Proposal]; **[…]***	

- [RECITAL 20] Internal compliance control systems are to be specifically focused on transactions with self-hosted wallets:

EP Mandate	**Trilogue procedure Draft Agreement**
(20) […] In line with the risk-based approach of this Regulation, those policies, controls and procedures should be proportionate to the nature, activity and size of the obliged entity and respond to the risks of money laundering and terrorist financing that the entity faces.	(20) […] In line with the risk-based approach of this Regulation, those policies, procedures and controls should be proportionate to the nature of the business, including its risks and complexity, and the size of the obliged entity and respond to the risks of money laundering and terrorist financing that the entity faces, ***including, for crypto-asset service providers, transactions with self-hosted wallets. [ADDED]***

- [RECITAL 21] Analogously, the risk determination rule is specifically designed to include transactions involving self-hosted wallets as a key factor:

EP Mandate	**Trilogue procedure Draft Agreement**
(21) An appropriate risk-based approach requires obliged entities to identify the inherent risks of money laundering and terrorist financing that they face by virtue of	(21) An appropriate risk-based approach requires obliged entities to identify the inherent risks of money laundering and terrorist financing as well as risks of non-

their business in order to mitigate them effectively and to ensure that their policies, procedures and internal controls are appropriate to address those inherent risks. In doing so, obliged entities should take into account the characteristics of their customers, the products, services or transactions offered, the countries or geographical areas concerned and the distribution channels used. In light of the evolving nature of risks, such risk assessment should be regularly updated.	implementation or evasion of targeted financial sanctions that they face by virtue of their business in order to mitigate them effectively and to ensure that their policies, procedures and internal controls are appropriate to address those inherent risks. In doing so, obliged entities should take into account the characteristics of their customers, the products, services or transactions offered, ***including, for crypto-asset service providers, transactions with self-hosted addresses [ADDED]***, as well as the countries or geographical areas concerned and the distribution channels used.

- RECITAL 27b; RECITAL 28: The provisions concerning the so-called alleviation of excessive administrative and financial burden and proportionality principle (which were to be applied to some of the obliged entities) have been arbitrarily (no justification provided) removed e.g.:

EP Mandate	**Trilogue procedure Draft Agreement**
(27b) Given that AML/CFT requirements are applicable to a wide range of obliged entities in both nature and size, AMLA should have the task of developing draft regulatory technical standards concerning minimum requirements and standards by obliged entities which are sole traders, single operators or micro enterprises taking due account of the principle of proportionality and alleviation of administrative burden AMLA should have the task of drawing up draft regulatory standards specifying the minimum requirements of group- wide procedures and policies, including minimum standards for information sharing within the group and the role and responsibilities of parent undertakings that are not themselves obliged entities***, and taking into account the principle of proportionality.***	***[DELETED]***
28 […] AMLA should have the task of drawing up draft regulatory standards specifying the minimum requirements of group-wide procedures and policies, including minimum standards for information sharing within the group and the role and responsibilities of parent undertakings that are not themselves obliged entities***, and taking into account the principle of proportionality***.	*28 […]* AMLA should have the task of drawing up draft regulatory standards specifying the minimum requirements of group-wide procedures and policies, including minimum standards for information sharing within the group and the ▌***criteria for identifying the*** parent ▌***undertaking for groups whose head office is outside of the Union [DELETED and ADDED]***.

- [RECITAL 32A] Significantly reduced to the scope of the Recital to "the civil society organisations that conduct charitable or humanitarian work in third countries", including by providing a recommendation more than obligation. At the same time, protection of legitimate customers such as asylum-seekers and refugees (the latter being excluded whatsoever), civil society organisations and representatives as well as their associates in terms of ensuring financial inclusion (including basic banking services) - in comparison to the EP AMLR draft:

EP Mandate	**Trilogue procedure Draft Agreement**
32 a (new) Credit and financial institutions should ensure that the application of due diligence measures is carried out on the basis of an individual risk assessment and does not result in unduly denying legitimate customers access to financial services, in particular with regard to specific categories of individual customers associated with higher risk, such as refugees and asylum seekers as well as human rights defenders, and non-governmental organisations and their representatives and associates. To that end, credit and financial institutions should ensure that their internal policies, controls and procedures are commensurate to the risks identified and do not unduly undermine financial inclusion. Access to basic financial products and services allows refugees and people seeking temporary or international protection to participate in the economic and social life of the Union, in line with the right to protection enshrined in Article 18 of the Charter of Fundamental Rights. At the same time, financial inclusion avoids transactions being driven underground through informal channels, thereby making the detection and reporting of suspicious transactions more difficult. Therefore, financial inclusion contributes significantly to the fight against money laundering and terrorist financing. This Regulation provides sufficient flexibility to financial institutions to perform the identification and verification of prospective clients who are refugees or seek protection and to adopt, in line with the risk-based approach, proportionate and effective measures to manage and mitigate risks linked to these clients. To ensure such flexibility is exploited to the fullest, credit and financial institutions should accept documents issued by Member States stating legal residence as a valid means for the purposes of customer identity verification. In order to ensure the	***(32a) Civil society organisations that conduct charitable or humanitarian work in third countries contribute to the Union's goals of achieving peace, stability democracy and prosperity. Credit and financial institutions play an important role in ensuring that such organisations can continue to conduct their work, by providing access to the financial system and important financial services that allow development and humanitarian funding to be channelled to developing or conflict areas. While obliged entities should be aware that activities conducted in certain jurisdictions expose them to a higher risk of money laundering or terrorist financing, operations of civil society organisations in these jurisdictions should not, alone, result in the refusal to provide financial services or termination of such services, as the risk-based approach requires a holistic assessment of risks posed by individual business relationships, and the application of adequate measures to mitigate the specific risks. While credit and financial institutions remain free to decide with whom they engage in contractual relationships, they should also be mindful of their central role in the functioning of the international financial system and in enabling the movement of funds as defined in Article 4, point (25) of Directive (EU) 2015/2366 or crypto-assets for the important development and humanitarian goals that civil society organisations pursue. They should therefore make use of the flexibility allowed by the risk-based approach to mitigate the risks associated with business relationships in a proportionate manner. Under no circumstances AML/CFT reasons should be invoked to justify commercial decisions as regards prospective or existing clients. [Commission Drafting proposal]***

effective implementation of AML/CFT rules, financial institutions should address the situation of refugees and persons seeking temporary or international protection within their internal policies and procedures of refugees and persons seeking temporary or international protection within their internal policies and procedures AMLA and EBA should issue joint guidelines to specify how to maintain a balance between the financial inclusion of the categories of customers particularly affected by de-risking and AML/CFT requirements and clarify how risk can be mitigated in relation to these customers and ensure transparent and fair processes for customers.	

- [RECITAL 49] The need to monitor, consult and take into account information from multiple and various sources, including civil society, academia and industry experts by the EC has been removed - limited only to the reliance on international organisations and standard setters such as FATF:

EP Mandate	**Trilogue procedure Draft Agreement**
(49) […] The Commission should take into account information from ***other Union institutions, bodies and agencies, competent authorities, civil society organisations, academia, and by*** international organisations and standard setters in the field of AML/CFT, such as FATF public statements, mutual evaluation or detailed assessment reports or published follow-up reports, and adapt its assessments to the changes therein, where appropriate.	*(49) […]* The Commission should take into account, as a baseline for its ***assessment,*** information from international organisations and. standard setters in the field of AML/CFT, such as FATF public statements, mutual evaluation or. detailed assessment reports or. published follow-up reports, and adapt its assessments to the changes therein, where appropriate. ***[DELETED]***

- [RECITAL 52] Also with regard to the process of identifying third countries which may constitute a threat to the to the integrity of the Union's financial system (what can be applied to, e.g. identifying EU sanction regimes' violators), the need to cooperate with civil society and academic experts has been removed from the regulation:

EP Mandate	**Trilogue procedure Draft Agreement**
*(52) […]To mitigate those risks, it should be possible for **AMLA** to take action by identifying, based on a clear set of criteria and with the support of **other Union institutions, bodies and agencies, and competent authorities, analysis by civil society organisations and academia, as well as assessments or reports drawn up by** international organisations and standard*	***[DELETED]***

setters with competence in the field of preventing money laundering and combating terrorist financing, third countries or territories posing a specific and serious threat to the Union's financial system, which may be due to either compliance weaknesses or significant strategic deficiencies of a persistent nature in their AML/CFT regime, and the relevant mitigating measures.	

- [RECITAL 86, 86a] The new draft proposes a very abstract and broad definition of the processing of certain categories of sensitive data. This will lead to more problematic implementation by financial compliance. The EP AMLR draft proposed a clear definition, stating that the processing of special categories of personal data and of personal data relating to criminal convictions and offenses should be subject to appropriate safeguards laid down in this Regulation:

EP Mandate	**Trilogue procedure Draft Agreement**
(86) […] The collection and subsequent processing of personal data by obliged entities should be limited to what is necessary for the purpose of complying with AML/CFT requirements and personal data should not be further processed in a way that is incompatible with that purpose. In particular, ***the processing of special categories of personal data and of personal data relating to criminal convictions and offences should be subject to appropriate safeguards laid down in this Regulation.*** Further processing of personal data for commercial purposes should be strictly prohibited.	(86) […] The collection and subsequent processing of personal data by obliged entities should be limited to what is necessary for the purpose of complying with AML/CFT requirements and personal data should not be further processed in a way that is incompatible with that purpose. In particular, ▌. ***[DELETED]*** further processing of personal data for commercial purposes should be strictly prohibited.
	(86a) The processing of certain categories of sensitive data as defined under Article 9 of Regulation 2016/679 may give rise to risks to the fundamental rights and freedoms of the subjects of those data. To minimise the risks that the processing of such data by obliged entities results in discriminatory or biased outcomes that adversely impact the customer, such as the termination or refusal to enter into a business relationship, obliged entities should not take decisions solely on the basis of information in their possession concerning special categories of personal data within the meaning of Regulation 2016/679 where that information bears no relevance to the money laundering or terrorist financing risk posed by a transaction or relationship. Similarly, in

	order to ensure that the intensity of customer due diligence is based on a holistic understanding of the risks associated with the customer, obliged entities should not base the application of a higher or lower level of customer due diligence measures solely on the basis of sensitive data that they possess on the customer. [Commission Drafting proposal]

- [RECITAL 94a] The caveat regarding the admissibility of crypto-asset payments for goods and services (assuming they are carried out by regulated service providers) and the lack of such a restriction on private transfers (involving the use of self-hosted wallets) has been removed. This change creates ambiguity regarding the admissibility of transactions of this nature and potentially lays the groundwork for a possible future effective ban on self-hosted wallets.

EP Mandate	Trilogue procedure Draft Agreement
(94a) Technological developments enable merchants to accept payments in crypto-assets for the provision of goods and services either in store or online. Where such payments are not carried out by means of a regulated service providers, the level of traceability to a verified identity might not be sufficient for the purpose of preventing their misuse for money laundering, terrorist financing or predicate offences. The use of such means of payment, in the context of increasing digitalisation, might create a loophole and undermine the effectiveness of the cash limit. While maintaining the possibility to make payments in crypto-assets for goods and services, it is therefore necessary to require merchants to rely on a crypto-asset service provider authorised under MiCA, when accepting payments in crypto-assets. Such limitation should apply to persons trading in goods or providing services and should not be interpreted as a restriction on private transactions by means of self-hosted wallets nor as a restriction to the use of self-hosted wallets in the context of commercial transactions, as long as a crypto-asset service provider is involved.	***[DELETED]***

- [CHAPTER I, Article 1, first paragraph, point (aa)] The objective of the AMLR, which underscored the need to focus on non-implementation and evasion of targeted financial sanctions, has been removed from the regulation's objectives as irrelevant to the updated version of the upcoming regulation:

EP Mandate	Trilogue procedure Draft Agreement

CHAPTER I Article 1, first paragraph, point (aa) […] ***the measures to be applied by obliged entities to mitigate and manage the risks of non-implementation and evasion of targeted financial sanctions;***	***[DELETED]***

- [CHAPTER III, Article 31b] Completely new articles have been added, once again targeting self-hosted wallets: "Measures to mitigate risks in relation to transactions involving self-hosted addresses," which are supposed to subject them to special scrutiny, as they are particularly susceptible (prone to ML/FT and other abuses) by nature:

EP Mandate	**Trilogue procedure Draft Agreement**
	CHAPTER III Article 31b Measures to mitigate risks in relation to transactions with a self-hosted address 1. Crypto-asset service providers shall identify and assess the risk of money laundering and financing of terrorism associated with transfers of crypto-assets directed to or originating from a self-hosted address. To that end, crypto-asset service providers shall have in place internal policies, procedures and controls. Crypto-asset service providers shall apply mitigating measures commensurate with the risks identified. Those mitigating measures shall include one or more of the following: (a) taking risk-based measures to identify, and verify the identity of, the originator or beneficiary of a transfer made from or to a self-hosted address or beneficial owner of such originator or beneficiary, including through reliance on third parties; (b) requiring additional information on the origin and destination of the crypto-assets; (c) conducting enhanced ongoing monitoring of those transactions; (d) any other measure to mitigate and manage the risks of money laundering and financing of terrorism as well as the risk of non-implementation and evasion of targeted financial sanctions. 2. AMLA shall issue guidelines to specify the measures referred to in this Article, including a) the criteria and means for identification and verification of the identity of the originator or beneficiary of a transfer made from or to a self-hosted address, including

	through reliance on third parties, taking into account the latest technological developments; b) criteria and means for the verification of whether or not the self-hosted is owned or controlled by a customer. ***[ADDED, Council Drafting proposal]***

- [CHAPTER III, Article 41a] The entire article regarding 'unwarranted de-risking, non-discrimination, and financial inclusion,' which was introduced by the EP in 2023 as a result of the BTC Coalition's advocacy campaign, has been deleted, putting civil society and marginalized groups at severe risk:

EP Mandate	**Trilogue procedure Draft Agreement**
(Article 41a) Unwarranted de-risking, non-discrimination and financial inclusion ***1. Credit and financial institutions shall have in place controls and procedures to ensure that and in the application of customer due diligence requirements provided under this Chapter does not result in the unwarranted refusal, or termination, of business relationships with entire categories of customers and that obliged entities comply with Article 15 and Article 16(2) of Directive 2014/92/EU. The internal policies, controls and procedures of credit and financial institutions shall include options for mitigating the risks of money laundering and terrorist financing that obliged entities will consider applying before deciding to reject a customer on the grounds of a risk of money laundering or terrorist financing.*** ***The internal policies and procedures of credit and financial institutions shall include options and criteria to adjust the features of products or services offered to a given customer on an individual and risk-sensitive basis and, where applicable, in accordance with the level of services offered under Directive 2014/92/EU.*** ***2. Without prejudice to paragraph 1, credit and financial institutions shall have in place internal policies, controls and procedures to ensure that the application of customer due diligence requirements provided under this Chapter does not result in the undue exclusion of non-profit organisations and their representatives and associates from access to***	***[DELETED]***

financial services exclusively on the basis of geographical risk. ***3. Obliged entities shall not rely exclusively on information provided by public authorities from the third countries covered by Articles 23, 24 and 25, as well as from the third countries covered by a decision adopted in accordance with Chapter 2 of Title V of the Treaty on European Union providing for the interruption or reduction, in part or completely, of economic and financial relations.[…].***	

- [CHAPTER VI, Article 55(1)-55(2), point (bc), 658-661c] The processing of certain categories of personal data: the new draft removes the references that set out limitations in this regard, invoking, among other things, the principle of proportionality, the adequacy of information sources, and the non-reliance solely on automated decision-making. This may lead to biased and discriminatory outcomes, which the draft originally aimed to avoid. These outcomes particularly affect financial institutions' customers, especially those subject to legal assistance and other abuses (including defamation) by states that do not adhere to the rule of law and other actors:

  1. To the extent that it is strictly necessary for the purposes of preventing money laundering and terrorist financing ***and in accordance with the principle of proportionality [DELETED]****, obliged entities may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679 and personal data relating to criminal convictions and offences referred to in Article 10 of that Regulation subject to the safeguards provided for in paragraphs 2 and 3.*

  (…)

  *b) the data originate from reliable sources, are accurate****, adequate [DELETED]*** *and up-to-date;*

  (…)

  (bb) obliged entities ensure the possibility of human intervention on the part of the controller by appropriately trained staff to verify automated individual decision- making; [DELETED]

  (bc) obliged entities ensure verification, where a higher risk is identified solely on the basis of special categories of data; [DELETED]

- [CHAPTER VI, Article 55a] In a similar manner, multiple safeguards introduced by the EP regarding the exchange of personal data (including with other states) have been removed, significantly increasing the risk of the well-known abuse of utilizing banking and other data against certain customers by malicious actors, such as hostile governments and their proxies:

EP Mandate	**Trilogue procedure Draft Agreement**
Article 55a Exchange of data under partnerships for information sharing in AML/CFT field	***[DELETED]***

1. For the purpose of combating money laundering and terrorist financing and related predicate offences, including for the fulfilment of their obligations under Chapter V of this Regulation, obliged entities and public authorities may participate in partnerships for information sharing in AML/CFT field established under national law in one or across several Member States. ***2. Without prejudice to Article 54, each Member State may lay down in its national law that, to the extent that is necessary and proportionate, obliged entities, and where applicable, public authorities that are party to the partnership for information sharing in AML/CFT field, may share personal data collected in the course of performing customer due diligence obligations under Chapter III, and process that data within the partnership for the purposes of the prevention of money laundering and terrorist financing, provided that at a minimum: (a) obliged entities concerned inform their customers or prospective customers that they may share their personal data under this paragraph;*** ***(b) personal data shared originate from reliable sources, are accurate and up-to-date;*** ***(c) the obliged entities concerned adopt measures of a high level of security in accordance with Article 32 of Regulation (EU) 2016/679, in particular in terms of confidentiality, including secure channels for exchange of information;*** ***(d) each instance of sharing of personal data is recorded by obliged entities, and where applicable, public authorities, concerned; the records shall be made available, without prejudice to Article 54(1), to data protection authorities and authorities responsible for protection of customers from undue tipping-off upon request;*** ***(e) obliged entities and, where applicable, public authorities, that are party to the partnership for information sharing in AML/CFT field implement appropriate measures for protection of justified interests of the customer concerned. Further processing of personal data under this paragraph for***	

other purposes, in particular commercial purposes, shall be prohibited.	