Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

BC4EU response to the '*Draft updated Guidance for a risk-based approach to virtual assets and VASPs*'

20 April 2021

Executive summary

Blockchain for Europe ("***BC4EU***") welcomes the FATF's objective of updating its pre-existing Guidance to ensure a common understanding and smooth application of FATF standards in the context of VA/VASPs, in line with existing standards applicable to financial institutions and other AML/CFT-obliged entities. Whilst the current rights and obligation remain unchanged, this draft interpretive guidance should level the playing field for VASPs' provision of financial services, by minimising the opportunity for regulatory arbitrage between sectors and countries.

However, if it remains unchanged and unclarified, the draft Guidance risks creating a **novel regulatory framework** which could potentially reach far beyond the FATF's traditional AML/CFT remit. Among others, the draft Guidance's **expansive definition of what constitutes a VASP**, which would now include Decentralised Finance ("***DeFi***") projects too, is highly problematic. Indeed, in contrast to the 2019 guidance, and despite the stated intention to exclude it, the proposed expansion of AML/CTF regulations to the virtual-assets industry, **would effectively regulate many areas of ordinary commerce including the creation and distribution of software that supports such activities**. This ultimately creates disincentives for responsible innovation and proves ineffective or even counterproductive to fighting illicit financial activity. Instead of overregulation pushing activities underground, the draft guidance should leverage the inherent transparency that blockchain technology enables.

In other words, imposing the **contemplated rules on the teams behind DeFi projects would likely jeopardise the projects and the whole ecosystems** around them, which thrives on openness and accessibility. Accordingly, FATF should **take a step back to properly understand this fast-growing space and carry out a thorough impact assessment beforehand.** Considering the novelty of DeFi projects, FATF's position on this phenomenon should best be formulated in a **separate guidance and/or at a subsequent date**.

In addition, the draft guidance raises **serious privacy concerns**, notably with regards to the **envisaged application of the so-called "*Travel Rule*" ("*TR*")**, which is **ill-adapted to the VASP market and VA activities**. It would effectively result in a **disproportionate amount of personal identifiable information ("*PII*") being collected** (or potentially falling into the wrong hands), far beyond what is actually done in the traditional banking and financial markets (e.g., real-time balances and whole transaction and counterparty histories available with VA wallet addresses in the former case, versus only single transaction information in the latter case).

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

BC4EU therefore invites FATF to (a) **consult with privacy regulators** on the envisaged application of the TR, (b) clarify that the TR, if implemented, **must be consistent with the application of international and national privacy laws**, and (c) explore **alternatives** to address its AML/CTF concerns, such as through the **adoption of fast-growing blockchain technology analytical tools**, which can increasingly effectively and transparently track and trace criminal activity through the use of various methods.

Similarly, the draft guidance categorically **designates unhosted wallets as high-risk without a factual basis** for doing so -- an approach which runs counter to the FATF's general guidance on adopting a risk-based approach. There too, FATF should explore realistic **alternatives** to address its AML/CTF concerns, such as **blockchain technology analytical tools** (e.g., wallet scan services) and r**equests to users on Source of Funds ("*SoF*") ** whenever they send crypto funds back to their VASP account and/or convert back to fiat.

Finally, BC4EU would like to underline the key importance of: (i) **training supervisors and law enforcement** with regards to crypto matters for them to properly understand and constructively regulate this space, (ii) **ensuring that fit & proper requirements for VASPs are subject to strict and objective criteria** - binding both on regulators and potential applicants - so as to avoid arbitrary and unsubstantiated assessments, and (iii) highlighting that the formulation of the **draft Guidance constantly uses the term "*should*",** which could wrongly be perceived as denoting obligations instead of clarifications.

The definition of VASP

1. BC4EU currently has **strong reservations on the proposed scope and definition of what constitutes a VASP**: it is not bound to financial instruments but covers anything that can be used for payments or investments. By doing so, FATF essentially **leaves VASPs to guess whether and when the conditions are fulfilled**. This lack of clarity around the very core of the VA definition is particularly problematic as the entire draft Guidance derives from it, resulting in numerous adverse effects.
2. In practice, it **encompasses nearly all commercial exchanges depending on the subjective intent of the buyer.** Despite the stated intention to exclude it, this broadened scope will effectively **regulate many areas of ordinary commerce**, including the **creation and distribution of software** that supports such activities. This unprecedented far-reaching approach goes far beyond FATF's traditional AML/CFT-related remit for the financial sector. Ultimately, the implicit inclusion of commerce is detrimental towards innovation, impractical to enforce, and counterproductive to fight illicit financial activity.
3. Although BC4EU recognises that FATF attempts to curtail an **overly-broad definition of VAs** by excluding merchants from the VASP definition, this exclusion is revoked if the merchant programs or operates a platform that permits the exchange of VAs. This is again extremely vague as it **could potentially turn any company combining the blockchain technology** (e.g., to present its sales items) **and an exchange activity** (to facilitate trades between customers)

into VASPs. The NBA Top Shots is a good example of an entity risking to become regulated as a VA just because its basketball trading cards can be traded on a platform using blockchain. Again, this effectively breaks the divide between financial intermediation and commerce by attempting to impose regulation designed for the financial sector on completely different types of activities.

4. The inclusion of DeFi projects in the **draft Guidance** (e.g., see paras, 56-57 and 68) presents another example of the risk to overstep the scope of the definition. Imposing the contemplated rules on the teams behind DeFi projects is highly problematic and may lead to unintended consequences. In effect, the draft Guidance considers that most financial transactions are done through financial intermediaries, despite the built-in disintermediation blockchain technology brings. Yet, the notion of "*financial intermediaries*" itself is not even defined in the FATF glossary. Although acting "*on behalf*" of someone is still a defining criterion for VASPs, it is later stretched to shoehorn operators of DApps and other stakeholders.

   The resulting administrative and financial burdens will likely severely dampen the development of such projects. **It would likely jeopardise the whole surrounding ecosystems** which thrives on openness and accessibility. Considering the novelty of DeFi projects, FATF's position on this phenomenon should best be formulated in a **separate guidance and/or at a subsequent date**. **Taking a step back would allow FATF to properly understand this fast-growing space while carrying out a thorough impact assessment beforehand.**
5. Although **BC4EU**, like the larger blockchain community, is **strongly committed to working with public authorities to find effective ways to fight ML/TF activities and other criminal uses of blockchain and VAs**, BC4EU is **critical of an approach that,** in effect, **requires merchants and software companies to become registered financial services companies** simply because they deploy some sort of trading platform involving digital items that fall into the VA's broadened definition. This **implicit expansion of the financial regulations scope for digital assets, goes far beyond the established norms for physical assets: strict rules apply to VAs while commodities, like gold, remain largely unregulated** despite their ability to be used for payments or investments. While we recognise the opportunity to minimise regulatory arbitrage between sectors (e.g., VASPs and other AML/CFT-obliged entities) and countries, we believe that the FATF's updated draft Guidance risks stifling innovation as it is not technology-neutral in its current state.
6. **Computer programmers**, as ground-breaking innovators, **are not meant to become financial intermediaries**. By attempting to force computer software companies to be regulated under VASP, the Guidance will be detrimental for the software industry, particularly open-source projects because they do not even know by whom and how their code is being deployed. For example, performing costly customer due diligence processes is simply not workable for most software companies. The FATF's assumption that DApps and DeFi projects can somehow be transformed into traditional intermediaries without destroying their business model is a grave misjudgement. To avoid inadvertently falling into VASP, we are more likely to see developers publishing anonymous and unaudited code. Resulting vulnerabilities would provide a far

secretariat@blockchain4europe.eu | @BlockchainforEU | Transparency register number: 910251734425-24

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

greater attack surface, risks of scams, and other fraudulent behaviour than the current situation.

7. **Blockchain is a database technology**, much like any other database, which can be **used to maintain records and information to denote digital representations of assets**. This process of so-called "*tokenisation*" simply recognises the usefulness of blockchain databases as a means to record and transfer value on the internet. It does not, however, make every tokenised asset into a financial instrument. Yet, the FATF seeks different treatment for DeFi/DApps based on the use of different technology, as if disintermediation was meant to circumvent regulation when it actually increases the security and dependability of financial services. Instead of this overregulation pushing innovative activities underground, FATF should leverage the inherent transparency that blockchain technology enables.
8. **Developers will find it challenging to "*centralise*" a technology that is inherently decentralised:** the code of open-source distributed ledger protocols is voluntarily run by validators and node operators, which can always choose not to be part of a centralised system. Furthermore, new clones of protocols can be spun up almost instantaneously and would almost certainly result in decentralised "*hard forks*". On the contrary, projects can evolve from being centralised to being fully distributed (e.g., the entirety of the bloc production of the Cardano protocol was recently transferred to the community of stake pool operators), thereby illustrating that decentralisation is actually a spectrum. Both regulators and the industry thus need legal certainty with regards to the level of decentralisation of an entity. To that end, the FATF should clarify in its draft Guidance specific thresholds for when a project is deemed fully decentralised and therefore, excluded in the scope of financial services legislation.
9. The DeFi innovation leads to the creation of new commercial opportunities, the economic inclusion of anyone having access to the internet, and the establishment of global computing platforms bringing people closer together through communication, recreation, and trade. Keeping this flexibility to innovate would likely unleash further positive outcomes Moreover, the incentive to formally oversee DeFi is limited since the unavoidable collaborations between centralised VASPs and DeFi projects will already spontaneously spread a culture of compliance: to the extent that DeFi users bring back large amounts back to their centralised VASP accounts, they will in any case be subject to ongoing monitoring of their transactions and enhanced due diligence requests. Accordingly, the draft Guidance should focus on centralised VASPs rather than seek to regulate decentralised software.

In light of the foregoing, **BC4EU therefore invites FATF to** make the **proposed revised wording** for the most relevant provisions (see additions <u>underlined</u>):

- *"56. Exchange or transfer services may also occur through so-called decentralized exchanges or platforms. "Decentralized or distributed application (DApp)," for example, is a term that refers to a software program that operates on a P2P network of computers running a blockchain protocol—a type of distributed public ledger that allows the development of other applications. These applications or platforms are*

often run on a distributed ledger and may in some cases, but not always, have a central party with some measure of involvement, such as creating and launching an asset, setting parameters, holding an administrative "key" or collecting fees. Often, a DApp user must pay a fee to the DApp, which is commonly paid in VAs, for the ultimate benefit of the owner/operator/developer/community in order to develop/run/maintain the software. DApps can facilitate or conduct the exchange or transfer of VAs.".

- "*57. A DApp itself (i.e., the software program) is not a VASP under the FATF standards, as the Standards do not apply to underlying software or technology (see below). However, entities involved with the DApp may be VASPs under the FATF definition. For example, the owner/operator(s) of the DApp likely fall under the definition of a VASP, as they are conducting the exchange or transfer of VAs as a business on behalf of a customer. The owner/operator is likely to be a VASP, even if other parties play a role in the service or portions of the process are automated. Likewise, a person that conducts business development for a DApp may be a VASP when they engage as a business in facilitating or conducting the activities previously described on behalf of another natural or legal person. The decentralization of any individual element of operations does not eliminate VASP coverage if the elements of any part of the VASP definition remain in place. However, the level of decentralisation can vary from one project to another, or even change over time. Projects that are fully decentralised, based on predefined criteria and thresholds, should not be part of the VASP definition and FATF standards.*"

Serious privacy concerns behind "*Travel Rule*"

10. The draft Guidance raises **serious privacy concerns,** notably with regards to the envisaged application of the so-called **"*Travel Rule*"** ("***TR***" - see in particular paragraphs 152-157), which the authors submit is ill-adapted to the VASP market and VA activities.
11. Indeed, if implemented, the TR would effectively result in a **hugely disproportionate amount of personal identifiable information ("*PII*") being processed** by VASPs, and potentially available to supervisors and law enforcement far beyond what they actually need, to address any legitimate AML/CTF concerns, or what is actually done in the traditional financial markets today.
12. Whereas in the **banking world**, the application of the TR means that **only limited information is collected** in relation to a single given transaction (e.g., originator and recipient names and account numbers, transaction amount etc), in the **VA world**, however, wallet addresses, and the activities associated with them are inherently public. This means that it is possible to obtain **vastly more information** from those VA wallet addresses than just the information related to the single given transaction, i.e., real-time balances and whole transaction and counterparty histories available.

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

13. In other words, the moment such extremely sensitive information "*on chain*" is tied to an individual VASP user identity "*off chain*", **financial privacy** has essentially been **eviscerated**. This would create a vicious cycle where the VASPs, supervisors or law enforcement routinely and arbitrarily overstep their boundaries by exploiting "*all the other information*" at their disposal. Worse, as **single points of failure**, in the event of a **data breach** (e.g., hacking of VASPs IT systems), such user PII tied to specific wallet addresses would fall into the wrong hands, and cause irreparable damage to the affected individual users.
14. BC4EU therefore submit that VASP users' financial information is a form of financial asset. By forcing the record-keeping, disclosure and reporting of wallet addresses and identity information for both clients and their counterparties, **regulated entities and governments** will be able to compile and **map entire blockchains**, thereby giving them the **ability to see all past, present and future transactions** in each known account and attribute all such transactions to the owner, without regard to the size or counterparty identity or consent. This **massive breach of financial privacy** is **not justified by any risk assessment** and there is **nothing close to comparable in the traditional financial services** world or the ordinary commercial world.
15. Similarly, the **TR should not apply to unhosted wallets either**. The FATF acknowledges that it is not feasible/wise to actually transmit the transactional data from VASPs to unhosted wallets. VASPs cannot entrust individual unhosted wallet holders to collect and store transactional data for security and privacy concerns. Individuals are not logistically equipped to send this data. So, the FATF TR proposal is really just a mechanism for requiring VASPs to collect counterparty information from their customers. Customers would provide unverified information on counterparties. Users could simply send/receive VAs from an unhosted wallet they set up as an intermediary from the true senders/receiver. The TR affirmative counterparty collection obligation creates real challenges.
16. Among others, it is crucial to remember that many jurisdictions, such as the EU, have specific rules regarding how long exchanges can store personal information on users. Yet how is an exchange to reliably identify which laws govern the retention and other obligations relating to a non-customer's information? We know where a customer is located because a customer discloses this in order to establish a customer relationship with a VASP. With non-customer information, however, we do not have any relationship to reliably establish location. And VASP customers may not know where the counterparty non-customer is located or may incorrectly identify it, which raises important questions about how to responsibly store this information. When the transfer is between exchanges, the most reliable information about the counterparty to a transaction is held by the recipient exchange where the counterparty is a customer. In these exchange-exchange transactions, counterparty collection seems particularly unnecessary and worry will be counterproductive. Counterparties may be unwilling -- for legitimate reasons -- to turn over their PII to customers or exchanges that reach out to them and who they do not know, leading to high failure rates.
17. From a **legal standpoint**, therefore, such a **sweeping and unlimited application of the TR to VASPs is in direct conflict with core privacy law principles such as purpose limitation, data minimisation, and storage limitation** (e.g., see Article 5 of the EU General Data Protection Regulation (GDPR)).

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

In light of the foregoing, **BC4EU therefore invites FATF to**:

a. **Consult with privacy regulators** on the envisaged application of the TR,
b. At the very least, **clarify that the TR**, if implemented, **must be consistent with the application of international and national privacy laws** (in particular in paragraphs 152-157). For instance, by adding a sentence to paragraph 157 of the draft Guidance below (see addition underlined):
   - "*157. Countries should ensure that ordering institutions (whether a VASP or other obliged entity such as a FI) involved in a VA transfer, obtain and hold required and accurate originator information and required beneficiary information and submit the information to beneficiary institutions (whether a VASP or other obliged entity, such as a FI), if any. Further, countries should ensure that beneficiary institutions (whether a VASP or other obliged entity, such as a FI) obtain and hold required (but not necessarily accurate) originator information and required and accurate beneficiary information, as set forth in INR. 16 (see Box 4 below). Notwithstanding the above, jurisdictions shall ensure that application of the travel rule is carried out in a manner consistent with their own privacy laws."*
c. **Focus on more balanced alternatives** to address its AML/CTF concerns, such as the obligation to resort to fast-growing **blockchain technology analytical tool**s, which can increasingly effectively and transparently track and trace criminal activity through the use of Artificial Intelligence.

High-risk qualification of unhosted wallets

18. The **draft Guidance also categorically designates unhosted wallets as high-risk** (see paras 91(a) and (b), 93, 179-180) without a factual basis for doing so -- an approach which contradicts the FATF guidance.
19. More specifically, the draft Guidance **should not classify all unhosted wallets as high-risk** as evidence demonstrates that these pose **less risk than commonly believed**.
20. Indeed, transactions with unhosted wallets are often first-party payments: i.e., customers sending money from an exchange to their own unhosted wallet or merchants receiving payment from their customers. The current **risk-based approach**, which is a cornerstone principle of international AML//CTF law, is therefore **well suited and efficient to deal with situations where VASPs transact with unhosted wallets**.
21. To put things into perspective, users of unhosted wallets anyway need to use regulated VASPs (or other regulated financial intermediaries) if and when they want to "*cash out*" or exchange the proceeds of their VAs for fiat currency. VASPs already effectively apply a risk-based approach by monitoring interactions with unhosted wallets. SAR-focused reporting already allows VASPs to spend resources on high-value data that is useful to law enforcement. FinCEN recently provided updated guidance on what is of value to law enforcement when filing a SAR.

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

22. Furthermore, the **flow of transactions between custodial and unhosted wallets allows blockchain analytics to understand ownership and use of unhosted wallets**. There are also positive uses of unhosted wallets in terms of consumer protection: hedge against potential hacks of exchanges or account takeovers/scams. It is also useful for new technology, such as Decentralised Applications ("*DApps*") that often have nothing or little to do with movement of funds. There is therefore no compelling reason to make people who use unhosted wallets and decentralised blockchains feel suspicious through a default high-risk classification (see in particular para 91 (b)). Nor is there a need to take radical and ill-considered steps such as denying licenses to VASPs that interact with unhosted wallets (see para 91(c)) or require enhanced due diligence on absolutely all transactions with unhosted wallet.
23. Finally, although we utilise the terminology "*unhosted wallet*" from the draft Guidance, we would prefer the term "*self-hosted wallet*" because it indicates that the activity is subject to monitoring by some person or entity.
24. "*Digital cash*" is now a reality, which presents formidable opportunities for global commerce, economic inclusion and humanity. If FATF forces regulators to impose ever-expanding requirements on both already-regulated entities and newly regulated entities, it will just further drive these technologies underground.

In light of the foregoing, **FATF should explore realistic alternatives to address its AML/CTF concerns**, such as fast-growing **blockchain technology analytical tools** (e.g., wallet scan services) and **requests to users on Source of Funds** whenever they send crypto funds back to their VASP account and/or convert back to fiat, and above certain threshold amounts. Below is BC4EU's proposed revised wording for the most relevant provisions (see additions, deletions and edits underlined):

- "*91. Countries should also seek to understand the ML/TF risks related to P2P transactions and how P2P transactions are being used in their jurisdiction. Countries may consider the following non-exhaustive list of options to mitigate risks posed by P2P transactions at a national level if the ML/TF risks are unacceptably high. This includes measures that seek to bring greater visibility to P2P transactions, as well as to limit jurisdiction's exposure to P2P transactions. These measures may include:"* (...)

  b) ongoing ~~enhanced~~ supervision on a risk-based approach basis of VASPs and entities operating in the VA space with a feature enabling unhosted wallet transactions (e.g., on-site and off-site supervision to confirm whether a VASP has compiled with the regulations in place concerning these transactions);

  ~~*c) denying licensing of VASPs if they allow transactions to/from non-obliged entities(i.e.,private / unhosted wallets)(e.g.,oblige VASPs via the 'travel rule' to accept transactions only from/to other VASPs);*~~"

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

- "*VA transfer to/from unhosted wallets*

  179. The FATF recognises that unlike traditional fiat wire transfers, not every VA transfer may involve (or be bookended by) two obliged entities, whether a VASP or other obliged entity such as a FI. In instances in which a VA transfer involves only one obliged entity on either end of the transfer (e.g., when an ordering VASP or other obliged entity sends VAs on behalf of its customer, the originator, to a beneficiary that is not a customer of a beneficiary institution but rather an individual VA user who receives the VA transfer to an unhosted wallet), countries should still ensure that the obliged entity adopts a risk-based approach on such transfers, and where justified (e.g. above certain amount thresholds) resort to blockchain analytics and requests to clients on source of funds. ~~adheres to the requirements of Recommendation 16 with respect to their customer (the originator or the beneficiary, as the case may be). Countries should also consider requiring VASPs to treat such VA transfers as higher risk transactions that require enhanced scrutiny and limitations.~~"

Other issues

25. **Training of supervisors and law enforcement with regards to crypto matters** is key for them to **properly understand, and constructively regulate this space**. This is already to some extent alluded to in the draft Guidance (see paragraphs 207, 229-231), but should really be reinforced through the **establishment of purpose-built regimes for VASPs** (e.g. specialised regulatory teams which understand the specificities of blockchain technology and tokenomics, when enforcing the law). Given the huge differences between decentralised finance and the traditional one, **financial regulators often lack the required expertise** and the appropriate resources to balance the risks and opportunities arising from VAs. For instance, despite all the anonymity myths, a thorough analysis of virtual-assets (e.g. Bitcoin) reveals that it is actually much too transparent for criminals to launder money, compared to the traditional cash-based system.

We would therefore propose the following changes to the draft Guidance (see additions underlined):

- "*207. Supervisors should also develop a deep understanding of blockchain technology, tokenomics, decentralised finance, the VASP market, its structure, and its role in the financial system and the country's economy to better inform their assessment of risk in the sector. This may require investing in training existing personnel, hiring personnel with prior relevant experience in the VASP market and VA activities (e.g., technical, compliance, legal, tokenomics experts, data analysts / forensics experts etc), or other resources that enable supervisors to gain the*

practical skillsets and expertise needed to regulate and supervise the range of VA providers and activities described in the VA services or business models at the onset of this Guidance.

- *229. Training is important for supervision staff to understand the delicate balance between blockchain technology, tokenomics, the VASP sector and the various business models and blockchain-related use cases that exist alongside the traditional financial markets. In particular, supervisors should ensure that staff are trained to assess the quality of a VASP's ML/TF risk assessment and to consider the adequacy, proportionality, effectiveness, and efficiency of the VASP's AML/CFT policies, procedures, and internal controls in light of its risk assessment. Training in blockchain or other analytics may also be useful.*

- *232.* [New paragraph] *Finally, jurisdictions should strongly consider the establishment of purpose-built regimes for VASPs and VA activities, such as specialised and dedicated supervisors, teams and units, which understand the delicate balance between the specificities of the VASP sector and the wider financial regulations. In particular, supervisors should consider hiring personnel with prior relevant experience in the VASP market and VA activities (e.g., technical, compliance, legal, tokenomics experts, data analysts / forensics experts etc)."*

26. **Fit & proper requirements for managers and shareholders of regulated VASPs** (see para 118) are welcome by BC4EU and would contribute to aligning the VASP market and VA activities with the requirements of the traditional financial sector, which in turn would contribute to legitimising it for regulators and the broader public. Notwithstanding the foregoing, such **fit & proper requirements for VASPs should be subject to strict and objective criteria, binding both on regulators and potential applicants,** so as to **avoid arbitrary and unsubstantiated assessments** by regulators that VASPs' managers and shareholders are unfit and improper. Indeed, several VASPs, including members of our association have reported being threatened of being deemed unfit and improper during their applications for regulated traditional financial activities, on the only basis that they were from the VASP market and involved in VA activities. The **grounds for deeming someone unfit & improper** should therefore be **clearly delimited to the following:**
    - **Lack of sufficiently relevant professional experience**;
    - **Serious past criminal convictions and administrative sanctions** on matters in relation with the assessment (*N.b. past civil or criminal proceedings, which did not lead to a conviction or sanction, should be declared, but should not in themselves be a sufficient reason for an unfit and improper finding*); and
    - In some particular cases where a legitimate concern is substantiated, **current civil or criminal proceedings** on matters in relation with the assessment.

    To the extent that there might be legitimate concerns around any of the above, **applicants should benefit from a good faith presumption of innocence**, and regulators cannot arbitrarily

deem applicants' board members or shareholders unfit & proper without demonstrating it clearly. Applicants should be **able to respond**, and in the event of a disagreement, the parties should be **able to quickly go before a neutral third-party arbiter** (e.g., an administrative judge or European body) - in parallel to their envisaged or ongoing licensing application procedure and before the final outcome thereof is known - to decide if yes or no the applicants' are objectively unfit & improper to exercise a regulated activity. If no circumstances warrant it (i.e., no criminal records etc), then applicants should be presumed fit and proper.

In light of the above, we would therefore propose the following changes to the draft Guidance (see additions underlined):

- "*118. In the licensing or registration process, Competent authorities should take the necessary legal or regulatory measures to prevent criminals, non-fit and proper person or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a VASP. Such measures should include requiring VASPs to seek authorities' prior approval for substantive changes in shareholders, business operations, and structures. Notwithstanding the above, jurisdictions shall ensure that their supervisors are bound to objective and fair criteria in their fit and proper determinations of VASPs' management and/or shareholders, so as to avoid arbitrary and blanket findings to that effect. The grounds for declaring a VASP's (or applying VASP's) management and/or shareholders unfit & improper should therefore be clearly delimited to the following criteria:*

    - *Lack of sufficiently relevant professional experience;*
    - *Past criminal convictions and administrative sanctions, which should be both relevant and serious towards the assessment;*
    - *Current civil or criminal proceedings, which must be relevant around the fit and proper assessment, neither frivolous nor abusive, and objectively lead to legitimate concerns around it. Past civil or criminal proceedings, which did not lead to a conviction or sanction, should be declared, but should not in themselves be a sufficient reason to deem VASPs' (or applying VASP's) management and/or shareholders unfit and improper.*

  In the event that a supervisor takes the position that there are legitimate concerns around any of the above, this should clearly be demonstrated and substantiated. VASPs (or applying VASPs) should at all times benefit from a presumption of innocence, and a right of response. Jurisdictions shall ensure that in the event of a disagreement, either the supervisor or the VASP (or applying VASP) may seek an expedited resolution before a neutral third party arbiter (e.g. in Europe, an administrative judge or regulatory body), and in parallel to their envisaged or

Blockchain for Europe
Rue Montoyer 47
1000 Brussels
Belgium

ongoing licensing application procedure, and in any case before the final outcome thereof is known, so as determine if a VASP's (or an applying VASP's) management or shareholders are indeed unfit and improper. If no circumstances warrant it (i.e. no criminal records etc), then the VASP's (or applying VASP's) management and/or shareholders will be presumed fit and proper."