April 17, 2026

SUBMITTED VIA WEB PORTAL:
https://ec.europa.eu/eusurvey/runner/ConsultationDraftRTSonCDD

To whom it may concern,

Re: AMLA Consultation Paper on Draft Regulatory Technical Standards under Article 28(1) of Regulation (EU) 2024/1624

About Global Digital Finance (GDF)

GDF is the leading global members association advocating and accelerating the adoption of best practices for crypto and digital assets. GDF's mission is to promote and facilitate greater adoption of market standards for digital assets through the development of best practices and governance standards by convening industry, policymakers, and regulators.

The input to this response has been curated through a series of member discussions, industry engagement, and previous engagement with the EU authorities over the years and GDF is grateful to its members who have taken part.

As always, GDF remains at your disposal for any further questions or clarifications you may have, and we would welcome a meeting with you to further discuss these matters in more detail with our members.

Yours faithfully,
Elise Soucie Watts – Executive Director – GDF

Response to the Public Consultations: Executive Summary

GDF welcomes the opportunity to respond to this consultation and commends AMLA for the quality of the draft Regulatory Technical Standards on Customer Due Diligence (the draft RTS). We are supportive of the overarching objective of harmonising CDD requirements across Member States and sectors and consider that AMLA's decision to build on the EBA's foundational work while extending its applicability to the non-financial sector is both pragmatic and appropriate. GDF represents a broad membership of digital asset firms, including CASPs, stablecoin issuers, payment service providers, and infrastructure firms operating across the EU and internationally. Our response reflects positions developed through our EU Working Group and broader member engagement.

We are broadly supportive of the proposals. We welcome in particular AMLA's commitment to proportionality, the risk-based approach, and simplification as guiding principles, which are essential to ensuring CDD obligations remain effective and workable across the wide range of obliged entities now subject to the AMLR. We also welcome the technology-neutral framing of the draft RTS, including in the provisions on non-face-to-face verification and electronic identification, though we note that the realisation of technology neutrality in practice depends on how specific provisions are drafted, and we set out our views on particular articles in our responses to the consultation questions.

Our key points of feedback are:

1. Article 5: should be amended, or accompanied by guidance, to confirm that where a customer declares multiple nationalities, obliged entities may apply a risk-based approach and verify a single nationality where there are reasonable grounds to consider this sufficient, consistent with the good faith verification standard in Recital 3. AMLA should also provide operational indicators of what constitutes "good faith" for these purposes to support consistent supervisory expectations across Member States.

2. Article 7: should be amended to recognise explicitly that privacy-preserving verification technologies, including zero-knowledge proof mechanisms and other cryptographic methods, may constitute valid and compliant verification solutions where they meet the underlying objectives of the provision, consistent with AMLA's stated commitment to technology neutrality. AMLA should also clarify that the justification obligation in Article 7(4) may be discharged categorically, at the level of a customer cohort or onboarding channel, rather than on an individual customer-by-customer basis.

3. Article 31: should be amended to ensure that factors (h) and (i), which relate to distribution channels, do not inadvertently disadvantage non-custodial and decentralised business models, and that factor (k), which identifies geo-fencing and IP address tracking as relevant risk

mitigants, is applied consistently with GDPR data minimisation principles and does not create an expectation to collect or retain technical data beyond what is necessary for legitimate AML/CFT purposes.

4. Article 11(4)(b): should be accompanied by guidance on what constitutes sufficient evidence of rationale for complex ownership and control structures, including a safe harbour for listed and regulated group structures, to avoid the provision operating as an open-ended documentary requirement for legitimate multinational groups.

5. Article 12(1): should be amended to require opacity, obfuscation, or nominee involvement as a necessary condition for a structure to be treated as complex, rather than treating structural characteristics such as non-EU incorporation at multiple layers as standalone qualifying conditions.

6. Article 30(a)(iii): should be accompanied by guidance clarifying that wallet address screening requires format validation and normalisation prior to matching, that evidentiary expectations for match disposition should reflect the technical characteristics of address matching in a digital asset context, and that supervisors should assess screening adequacy by reference to the reasonableness of methodology rather than solely by reference to outcomes.

7. The draft RTS should include a specific provision or accompanying guidance clarifying the application of CDD requirements to transactions involving self-hosted wallets: confirming that obliged entities are not required to obtain standard CDD information in relation to self-hosted wallet counterparties who are not customers of the obliged entity, and that a risk-based assessment using blockchain analytics and other available tools provides a proportionate and effective framework in such circumstances.

8. The draft RTS should recognise on-chain transparency and blockchain analytics as risk mitigants: capable of supporting simplified due diligence measures in lower-risk digital asset contexts, including reduced frequency of periodic CDD reviews and reliance on on-chain transaction data as a primary source of ongoing monitoring information.

Response to the Consultation Paper Questions

Question 1: Do you agree with the proposals set out in these draft RTS? If you do not agree, please specify: (i) the provision(s) concerned; and (ii) the rationale for your position. Please provide concrete drafting proposals to resolving the issue and explain why the measure you propose would be more appropriate.

GDF is broadly supportive of the proposals set out in the draft RTS. We welcome AMLA's commitment to proportionality, the risk-based approach, and simplification as guiding principles, and consider that the horizontal, flexible framework applying across both the financial and non-financial sectors is the appropriate approach. We also welcome the decision to build on the EBA's foundational work, which provides continuity for obliged entities and supports a smooth transition.

We wish to flag four areas where targeted amendments would strengthen the draft RTS. First, Article 7 would benefit from explicit recognition that privacy-preserving verification technologies, including zero-knowledge proof mechanisms and other cryptographic methods, may constitute valid and compliant verification solutions, to avoid the hierarchy of methods being read prescriptively in a manner inconsistent with technology neutrality. Second, Article 31 requires further consideration in relation to factors (h), (i), and (k), which may inadvertently disadvantage non-custodial and decentralised business models and, in the case of factor (k), create tension with GDPR data minimisation principles. Third, the draft RTS should provide greater clarity on the application of CDD requirements where obliged entities interact with self-hosted wallets, where required information may be structurally unavailable; a risk-based approach anchored in what can reasonably be obtained, complemented by blockchain analytics, provides a proportionate framework. Fourth, Article 5 should be read consistently with Recital 3 to permit risk-based verification of a single nationality where the obliged entity has reasonable grounds to consider this sufficient, and AMLA should provide operational indicators of what constitutes good faith for these purposes.

We also consider that Articles 8, 10(a), and 12 would benefit from targeted clarification: Article 8 on the reliability and independence of digital sources and specialist tools; Article 10(a) on the accessibility of registers and the availability of alternative sources where registers are not practically accessible; and Article 12 on anchoring the definition of structural complexity to ML/TF-relevant risk factors rather than structural characteristics alone.

In all areas, our proposed amendments are directed at ensuring the draft RTS delivers on its stated objectives of proportionality, risk-based application, and technology neutrality. We do not

consider that any proposal would reduce the effectiveness of AML/CFT controls, and we remain committed to supporting AMLA in delivering a high-quality, workable CDD framework.

Question 2: Do you agree that the proposals set out in these draft RTS can be applied across the range of products and services provided by your obliged entity? If you do not agree, please: (i) explain your rationale for why the current proposals do not provide sufficient flexibility; and (ii) provide concrete drafting proposals and explain why the specific measures you propose would be more appropriate.

GDF's membership includes CASPs providing exchange, custody, transfer, and payment services, stablecoin issuers, and infrastructure firms. We consider the draft RTS broadly capable of application across these business models and welcome the flexibility embedded in the horizontal, principles-based approach. We wish to highlight the following articles where targeted amendments would ensure more effective and proportionate application.

Article 5: Nationality identification and the good faith verification standard

Article 5 requires obliged entities to obtain information on all nationalities held by a natural person, while Recital 3 provides that verifying one nationality is sufficient where the obliged entity acts in good faith. The relationship between the two is not sufficiently clear, and obliged entities cannot safely rely on a recital to depart from the plain terms of an operative provision. We invite AMLA to resolve this ambiguity by amending Article 5 explicitly or by providing guidance confirming that risk-based verification of a single nationality is permissible where the obliged entity has reasonable grounds to consider this sufficient. AMLA should also provide operational indicators of what constitutes good faith, for example the absence of information suggesting a second nationality is risk-relevant, or the verified nationality being issued by an EEA Member State. Without such anchoring, supervisory expectations risk varying significantly across Member States.

Article 7: Non-face-to-face verification and digital asset business models

The hierarchy in Articles 7(1) and (2) risks being read as a closed list of compliant methods, inconsistent with technology neutrality. Privacy-preserving verification technologies, including zero-knowledge proof mechanisms and other cryptographic methods, can deliver verification outcomes equivalent to or stronger than traditional document-based methods while materially reducing data minimisation and cyber risk concerns. We propose that AMLA add an explicit paragraph after Article 7(2) recognising that such technologies may satisfy the requirements of Article 7 where they achieve an equivalent assurance level and the obliged entity can demonstrate compliance to its competent authority.

Article 7: Proportionality of the fallback verification requirements

The safeguards in Articles 7(3) and (4) should make clear that the degree of assurance required should be calibrated to the ML/TF risk of the customer and business relationship. We also invite AMLA to clarify Article 7(3)(e), where ambiguity around "valid and up to date" and "copies" could create inconsistent supervisory expectations in digital-first onboarding flows.

Article 7(4): Categorical justification for non-eIDAS verification

Article 7(4) as drafted appears to require case-by-case justification for each individual customer, which is disproportionately burdensome where reasons are structural and consistent across entire cohorts. We invite AMLA to clarify that the obligation may be discharged categorically, at the level of a customer cohort, product line, or onboarding channel, documented in policies and procedures and reviewed periodically.

Articles 11(4)(b) and 12(1): Ownership structures and the definition of complexity

Article 11(4)(b) risks becoming an open-ended documentary requirement without guidance on sufficient evidence of rationale. A group structure chart with a short explanation and publicly available filings should ordinarily suffice for a legitimate multinational group, with more intensive requirements reserved for situations where specific risk indicators are present. A safe harbour should also apply for structures involving entities regulated in an EEA Member State or equivalent jurisdiction or listed on a recognised exchange.

Article 12(1) compounds this by treating non-EU registration at multiple layers as a standalone qualifying condition without requiring any indicator of opacity or obfuscation. We propose that opacity, obfuscation, or nominee involvement be a necessary condition for structural complexity. This concern is particularly acute in institutional onboarding, where multi-layered structures are routine among asset managers, funds, and financial groups, and structural complexity is a poor proxy for ML/TF risk.

Article 31: Application to digital asset business models

Factors (h) and (i) may inadvertently disadvantage non-custodial and decentralised models, and factor (k), identifying geo-fencing and IP tracking as risk mitigants, raises proportionality and GDPR concerns. We address these in Question 3. We also encourage AMLA to clarify how the reliability and independence criteria in Article 8 apply to digital sources and third-party tools, and how responsibility allocation operates under Article 9 in intermediated structures where different parties hold different elements of the relevant information.

Question 3: Do you agree that the proposals set out in these draft RTS allow for the effective application of a risk-based approach towards compliance with AML/CFT requirements? If you do not agree, please: (i) specify the provisions concerned; and (ii) provide concrete drafting proposals and explain why the specific measures you propose would be more appropriate.

GDF is broadly supportive of the risk-based approach embedded in the draft RTS and welcomes AMLA's commitment to proportionality. We wish to flag three areas where targeted amendments would strengthen the framework.

Article 31: Risk factors for electronic money instrument exemptions

GDF welcomes the non-exhaustive framing of Article 31 and the inclusion of factors reflecting digital payment ecosystems. However, we have concerns regarding three specific factors.

Factor (h) enumerates electronic signatures and anti-impersonation measures as the relevant safeguards for online distribution. Cryptographic authentication mechanisms, including multi-signature authorisation, public key cryptography, and on-chain identity attestations, provide equivalent or stronger controls and should be explicitly recognised alongside electronic signatures. We propose amending factor (h) to refer to adequate safeguards "including but not limited to" electronic signatures and cryptographic authentication mechanisms.

Factor (i) treats distribution through regulated intermediaries as a risk mitigant. This risks structurally disadvantaging non-custodial and decentralised models where controls are applied at issuance, redemption, and regulated on-ramp and off-ramp touchpoints rather than at each individual transfer. The absence of intermediaries does not indicate elevated risk where equivalent controls exist elsewhere in the distribution architecture. We propose amending factor (i) to recognise that equivalent risk controls applied at regulated touchpoints within the distribution architecture should satisfy this factor.

Factor (k) identifies geo-fencing and IP tracking as relevant technological tools. IP addresses can be masked through widely available tools and do not reliably evidence geographical location. Their systematic collection also engages GDPR data minimisation obligations. We propose reframing factor (k) to focus on the outcome, restriction of access from higher-risk jurisdictions, rather than prescribing specific technological methods, with an explicit proportionality and data protection qualifier.

General observations on the risk-based approach

The transparency and traceability of on-chain transactions, the availability of blockchain analytics, and the architecture of compliance controls at regulated touchpoints collectively provide a robust risk management framework for the digital asset sector. A genuinely risk-based approach should recognise these as relevant mitigants rather than applying CDD requirements designed for traditional financial models without adjustment. We would also encourage AMLA to clarify that Article 8 reliability and independence criteria apply to commonly used digital sources and third-party tools, and that sanctions-screening expectations under Articles 29 and 30 should remain proportionate in high-volume digital contexts, including through appropriate automation and robust false-positive management.

We also note, as addressed in detail in our response to Question 2, that Articles 11(4)(b) and 12(1) require targeted clarification to avoid disproportionate documentary obligations for legitimate multinational and institutional groups.

Article 30(a)(iii): Wallet address screening

GDF welcomes the recognition of wallet addresses as identifiers for sanctions screening but wishes to flag two concerns about the operational implications of Article 30(a)(iii).

Unlike name-based screening, which involves probabilistic matching against multiple variants with false positives well understood and managed, wallet address screening appears deterministic. This creates a risk that supervisory expectations drift toward a zero-tolerance standard that does not account for the practical complexities of address matching, including format discrepancies, truncation, and chain-specific parsing requirements.

We invite AMLA to clarify: first, that a match should be understood as a match after appropriate format validation and normalisation rather than a raw string match; second, that evidentiary expectations for match disposition should reflect the technical characteristics of wallet address screening and should not default to zero-tolerance; and third, that supervisors should assess screening adequacy by reference to the reasonableness of methodology and robustness of disposition processes rather than solely by reference to outcomes. These clarifications would support consistent and proportionate supervisory expectations and provide obliged entities with the regulatory certainty needed to invest in robust screening processes.

Question 4: Considering the nature of your business, including its size, risks, and complexity, are there any situations where the information to be collected for the purposes of customer due diligence as proposed in these draft RTS is routinely unavailable and the proposals in these draft RTS do not provide an alternative solution? If so, please provide concrete examples of such situations and your proposals for alternative solutions.

GDF wishes to engage with this question in the context of a specific and increasingly common operational challenge: the application of standard CDD requirements to transactions involving self-hosted wallets. This is an area where required information may be genuinely and structurally unavailable, not as a consequence of any compliance failing, but as a direct result of the technical architecture of the technology involved.

The structural challenge: CDD and self-hosted wallets

When a CASP processes a transaction involving a self-hosted wallet, full CDD applies to the CASP's own customer. However, the counterparty, namely the holder of the self-hosted wallet, is not a customer of the CASP and has no account relationship with it. The CASP has no direct means of collecting the information required under Articles 2 to 18 in relation to that counterparty, and this cannot be resolved by applying greater compliance effort. As GDF and co-signatories including ADAN and CryptoUK set out in our joint Travel Rule report submitted to European authorities in 2025, 90% of surveyed CASPs reported significant difficulties in this context. The consequence has been that CASPs ban these transactions entirely, undermining transparency and driving legitimate activity towards less regulated channels.

The draft RTS does not address this situation. We would also encourage AMLA to clarify in relation to Article 10(a) that reliance on registers is expected only where they are practically accessible, that alternative reliable independent sources remain acceptable where they are not, and that supervisors should not treat the absence of checks against inaccessible sources as a compliance failing.

The existing compliance architecture provides effective controls

Transactions involving self-hosted wallets are not uncontrolled. Full CDD applies to the CASP's own customer. Blockchain analytics tools enable real-time assessment of wallet address risk profiles, identifying exposure to sanctioned addresses, darknet-linked services, and other indicators of illicit activity. Where analytics indicate elevated risk, the CASP should apply enhanced due diligence to its own customer and file a suspicious transaction report where appropriate. Other jurisdictions, including the UK following HM Treasury's 2022 consultation, have concluded that unhosted wallet transactions should not automatically be treated as higher risk.

Proposed solution

We propose that AMLA include a provision clarifying that: standard CDD applies in full to the obliged entity's own customer; where a self-hosted wallet counterparty is not a customer of the obliged entity, the obliged entity is not required to obtain Articles 2 to 18 information in relation to that third party where it is not reasonably available; and in such circumstances the obliged entity should apply a risk-based assessment having regard to blockchain analytics, transaction value and pattern, and the risk profile of its own customer, applying enhanced due diligence where the assessment warrants it. This would provide legal certainty for CASPs operating in good faith and avoid the outcome of blanket transaction bans that reduce rather than strengthen supervisory oversight.

We would also note that, in relation to Article 27, AMLA could usefully clarify that obliged entities may corroborate source of funds using alternative evidence proportionate to the level of risk, reserving more intensive corroboration for elevated-risk scenarios.

Article 33: Phased remediation of existing client files

Implementation of Article 33 may prove challenging if interpreted as requiring simultaneous re-collection of information across the entire existing customer base. For digital-first obliged entities with large legacy populations, and particularly for institutional firms whose client files are detailed, relationship-specific, and resource-intensive to maintain, a simultaneous re-verification exercise would be disproportionately burdensome. We invite AMLA to clarify in Article 33 or accompanying guidance that phased, risk-prioritised remediation focused on material information gaps, trigger events, monitoring alerts, and periodic risk-based review cycles is a compliant approach, and to provide indicative guidance on the triggers and timelines that would be expected to apply.

Question 5: Considering AMLA's legal mandate in Article 28(1) of Regulation (EU) 2024/1624, and taking into account your obliged entities' products offered and service provided, what other simplified due diligence measures should be included in the draft RTS, for example because of the associated lower ML/TF risks of these products and services? Please provide concrete drafting proposals and rationale for the specific measures you would propose.

GDF considers that there is one area in particular where the draft RTS could usefully specify additional SDD measures consistent with AMLA's mandate: contexts where on-chain transparency and blockchain analytics provide a level of transaction visibility materially higher than that available in traditional financial services, and where this elevated transparency

constitutes a genuine and verifiable risk mitigant justifying reduced ongoing monitoring intensity.

On-chain transparency as a risk mitigant

A defining feature of public blockchain infrastructure is the transparency and immutability of transaction records. Every transaction is visible to any observer, permanently retained, and cryptographically verifiable. Where a CASP has completed standard CDD on its own customer and transactions are conducted on a public blockchain, the risk visibility available to the obliged entity and to supervisors is meaningfully higher than for equivalent transactions conducted through traditional payment infrastructure. Blockchain analytics tools amplify this further by enabling real-time, automated assessment of transaction patterns, counterparty risk, and exposure to sanctioned or high-risk addresses. The draft RTS does not explicitly recognise these features as factors that may justify SDD measures in appropriate contexts.

GDF would also encourage AMLA to consider SDD measures for clearly delimited low-risk configurations, for example where the customer is EEA-resident, funding is limited to an account held in the customer's name with an EEA-regulated institution, low transaction and holding limits apply, and withdrawals are restricted to regulated counterparties. In such configurations, AMLA could permit greater use of standardised purpose categories and deferral of more granular source of funds collection unless monitoring triggers justify escalation.

Proposed SDD measure

We propose a specific SDD measure for CASPs in lower-risk situations where: standard CDD has been completed at onboarding; transactions are conducted on a public blockchain subject to full on-chain transparency; blockchain analytics monitoring is applied on an ongoing basis; and the overall risk assessment of the relationship is low. Where these conditions are met, the draft RTS should permit the obliged entity to reduce the frequency of periodic CDD reviews and to rely on on-chain transaction data, including blockchain analytics results, as a primary source of ongoing monitoring information in lieu of additional customer information requests. We propose the following addition as a new article within Section 5:

"Where a crypto-asset service provider has completed standard CDD on its customer and transactions are conducted on a public distributed ledger subject to full on-chain transparency, the provider may, where the ML/TF risk is assessed as low, (a) reduce the frequency of periodic CDD reviews having regard to the continuous availability of on-chain transaction data; and (b) rely on on-chain transaction data, including blockchain analytics results, as a primary source of ongoing monitoring information in lieu of additional customer information requests, where such

data is sufficient to satisfy the obliged entity that transactions are consistent with the customer's risk profile. This shall not affect the obligation to update CDD information or apply enhanced due diligence where a change in risk profile warrants it."
We would also encourage AMLA to clarify that address verification in lower-risk digital onboarding contexts may rely on electronic sources and bank-account verification assessed in accordance with Article 8, rather than requiring documentary proof of address in all cases.
Rationale

This proposed measure is consistent with AMLA's mandate under Article 28(1) and with recital (78) of the AMLR. It does not exempt CASPs from any component of standard CDD but substitutes a more effective and technologically appropriate ongoing monitoring mechanism for periodic information collection. On-chain transparency is a genuine and verifiable risk mitigant specific to the digital asset sector with no direct equivalent in traditional finance, and its recognition in the SDD framework is consistent with FATF's risk-based approach, which explicitly acknowledges that the transparency characteristics of specific products and services are relevant to ML/TF risk assessment. GDF would welcome further engagement with AMLA on the standards that should apply to blockchain analytics tools used for ongoing monitoring under this provision.