Contribution ID: ef981f85-23d6-454d-a009-15c06f986f6a
Date: 08/05/2026 15:09:20

Public Consultation on the draft Regulatory Technical Standards on Customer Due Diligence under Article 28(1) of Regulation (EU) 2024/1624

Fields marked with * are mandatory.

Public Consultation on the draft RTS on Customer Due Diligence under Article 28(1) AMLR

Objective of the consultation

AMLA would like to receive feedback on provisions of the draft RTS under Article 28(1) of Regulation (EU) 2024/1624 ('AMLR') and in particular on the specific questions set out below.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices AMLA should consider.

Such comments should be sent by **8 May 2026, 23:59 (CET).**

Personal data protection:

The protection of individuals with regard to the processing of personal data by the AMLA is based on Regulation (EU) 2018/1725. Further information on the processing of the personal data is available in the Data Protection Notice.

All legal details can be found in our Specific Privacy Statement (SPS).

How to provide feedback

All the fields marked with an asterisk (*) are mandatory. If a question is not relevant for you, please answer with "NA".

We are using a survey format to help us analyse feedback effectively and efficiently. For this reason, document uploads are not enabled for this exercise, and we kindly invite you to share your comments directly within the survey.

Please note that by submitting your contribution, you acknowledge that it will be published on AMLA's website. Contributions will always be published. The name of organisations submitting their contribution will also always be published. The name of the natural person providing a contribution will be published unless they object to said publication. Please refrain from inserting further personal information beyond what we ask from you. In particular, please refrain from providing confidential information or special categories of personal data (that is "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"). Your email address will never be published.

Before publication, AMLA staff will perform a limited screening of all contributions provided for the sole purpose of filtering any inappropriate submissions. After this, the replies are made available to the public directly on AMLA's public consultations page.

Please note that your contribution may be subject to a request for access to documents under Regulation 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

Language disclaimer

AMLA welcomes submissions in all official EU languages. You can change the displayed language of this public consultation using the language selector in the top right corner of the EU Survey platform. Please note that all language versions other than English have been produced using machine translation and may contain inaccuracies. When in doubt, please refer to the English version.

Should you encounter issues with submitting your responses, please contact us by email at public.consultations@amla.europa.eu no later than 48 hours before the deadline of the consultation period.

Section 1 - Respondent profile

* This contribution is made by:

An organisation

* Name of the organisation

200 character(s) maximum

Institut National de Bitcoin (INBi)

* First name of individual (individual respondent or representative of organisation)

100 character(s) maximum

Bastien

* Surname of individual (individual respondent or representative of organisation)

100 character(s) maximum

Desteuque

* Email (note that your email address will not be published)

100 character(s) maximum

bastien@inbi.fr

* Publication of your name and surname

- ○ I agree to the publication of my name and surname (note that your email address will never be published).
- ◉ Contribution to be published without my name and surname (note that your email address will never be published).

* Which of the following best describes your activity or organisation? Obliged entities are those listed in Article 3 of Regulation (EU) 2024/1624.

Maximum 1 selection(s)

- ☐ Obliged entity in the non-financial sector
- ☐ Obliged entity in the financial sector
- ☐ Self-regulatory body in the sense of Regulation (EU) 2024/1624 Article 2(1) point (47)
- ☐ Industry association representing non-financial sector obliged entities
- ☐ Industry association representing financial sector obliged entities
- ☑ Civil society organisation/non-governmental organisation
- ☐ Other

* Please select the country from which you or your organisation carry out your main activities:

FR - France

Section 2 - Substantive comments on the draft Regulatory Technical Standards

* 1. 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 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.

Provisions that are clearly marked as applying only to a specific sector or service should not be taken into consideration if they do not impact your sector.

5000 character(s) maximum

Les propositions peuvent s'appliquer à de nombreux produits et services, mais elles nécessitent une clarification pour les services sur le registre Bitcoin impliquant des retraits pour de la conservation en propre.

L'article 18 du projet de RTS précise les informations que les entités assujetties peuvent être conduites à collecter pour documenter l'objet et la nature envisagée de la relation d'affaires ou de la transaction occasionnelle. Certaines de ces catégories, en particulier celles relatives à la destination des fonds, peuvent être mal adaptées ou donner lieu à une interprétation extensive lorsqu'elles sont appliquées aux retraits vers des portefeuilles auto-hébergés.

Dans ce cas, certaines informations relatives à la destination des fonds peuvent ne pas être pertinentes : identité d'un bénéficiaire tiers, existence d'un intermédiaire, ou "juridiction de réception" assimilable à celle d'un compte bancaire. Une adresse bitcoin n'est pas un compte tenu par un prestataire situé dans une juridiction déterminée.

Sans clarification, les CASP peuvent être incités à créer des questionnaires intrusifs ou à collecter des informations artificielles pour documenter des catégories qui ne correspondent pas à l'opération réalisée. Cela nuirait à la proportionnalité du dispositif sans bénéfice démontré pour la lutte contre le blanchiment de capitaux et le financement du terrorisme.

INBi recommends that Article 18 be clarified as follows:

"For the avoidance of doubt, where a crypto-asset service provider assesses the purpose and intended nature of a transaction involving a withdrawal of bitcoin to a self-hosted address indicated by an identified customer for self-custody purposes, information on a third-party recipient, intermediary or receiving jurisdiction should be collected only where it is relevant, available and necessary to mitigate an identified ML/TF risk. In low-risk situations, self-custody may constitute the relevant information on the intended use or destination of funds."

* 2. 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.

5000 character(s) maximum

Le projet affirme une approche fondée sur les risques, mais il ne contient pas de garde-fou suffisant contre la surcollecte défensive. En l'état, il risque de consolider une interprétation extensive des obligations de vigilance client, particulièrement problématique lorsqu'elle conduit à associer identité civile, adresses sur le registre Bitcoin et historique transactionnel.

En pratique, une entité assujettie encourt un risque juridique et réputationnel important lorsqu'elle collecte trop peu d'informations, mais elle est rarement sanctionnée pour avoir collecté trop d'informations. Cette asymétrie pousse les acteurs privés à collecter "plus au cas où", même lorsque l'utilité LBC/FT marginale des données n' est pas démontrée.

Dans le cas du registre Bitcoin, l'association entre identité civile, adresse et historique transactionnel peut révéler durablement des éléments patrimoniaux. Une fuite de telles données ne crée pas seulement un risque de fraude numérique ; elle peut exposer les personnes concernées à des risques d'extorsion et de violences physiques graves, pouvant aller jusqu'à l'enlèvement, la séquestration, la torture ou les actes de barbarie.

L'approche fondée sur les risques ne doit donc pas être comprise comme une collecte maximale, mais comme une collecte nécessaire, documentée et proportionnée. elle que l'impose le RGPD. Devraient en outre être imposés aux acteurs (1) une obligation de dissocier identité et adresse physique d'une part et éléments patrimoniaux et transactionnels d'autre part, et (2) une obligation de chiffrement de ces informations, afin que les informations soient illisibles en cas de fuite de données.

INBi recommends adding the following interpretative clause:

"For the purposes of this Regulation, risk-based customer due diligence shall not be interpreted as requiring maximum information collection. Where an obliged entity documents that a less intrusive measure sufficiently mitigates the identified ML/TF risk, the absence of additional data collection should not, in itself, be considered a deficiency in the application of customer due diligence measures."

INBi also recommends that supervisory expectations explicitly take into account the risks created by overcollection and excessive retention of sensitive crypto-financial data.

* 3. 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.

5000 character(s) maximum

Oui.

Dans le cas de retraits de bitcoins pour de la conservation en propre, plusieurs informations prévues ou suggérées par le projet de RTS peuvent être structurellement indisponibles, artificielles ou non pertinentes.

Premièrement, l'information relative à un bénéficiaire tiers ou à un intermédiaire peut être non pertinente lorsque le client retire des bitcoins vers une adresse qu'il contrôle. L'opération ne devrait pas être traitée par défaut comme impliquant un bénéficiaire tiers.

Deuxièmement, la notion de "juridiction de réception" n'est pas toujours pertinente pour une adresse sur le registre Bitcoin. Contrairement à un compte bancaire, une adresse bitcoin n'est pas tenue par un établissement situé dans une juridiction déterminée.

Troisièmement, exiger une destination économique détaillée peut conduire à produire une information artificielle. La conservation en propre peut constituer en elle-même la finalité légitime de l'opération.

Quatrièmement, l'information relative à l'origine patrimoniale historique peut être indisponible ou disproportionnée lorsqu'un particulier a acquis des bitcoins sur plusieurs années, par achats successifs, dons, activité de minage ou opérations antérieures à la relation avec le CASP. Cette difficulté ne devrait pas conduire automatiquement à exiger des informations relevant d'une vigilance renforcée lorsque le risque identifié ne le justifie pas.

Cinquièmement, les informations collectées ou conservées pour documenter l'analyse transactionnelle devraient rester strictement limitées à ce qui est nécessaire au risque identifié. Une interprétation extensive conduisant à conserver des historiques transactionnels ou données d'adresses au-delà de ce besoin accroîtrait le risque pour les personnes sans bénéfice LBC/FT démontré.

Les solutions alternatives devraient donc pouvoir inclure une déclaration limitée du client, un filtrage des sanctions financières ciblées, un contrôle de cohérence avec le profil client et une analyse transactionnelle limitée à ce qui est strictement nécessaire au risque identifié.

INBi recommends the following clarification:

"Where information requested under these RTS is not relevant or not routinely available for a specific crypto-asset service, obliged entities should be allowed to rely on less intrusive measures that are adequate to mitigate the identified ML/TF risk. Such measures should not require the systematic retention of address graphs, extended transaction histories or speculative information on future use."

* 4. 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.

5000 character(s) maximum

Oui.

L'INBi recommande de prévoir des mesures de vigilance simplifiée pour les situations de faible risque dans lesquelles un client déjà identifié et vérifié retire des bitcoins depuis un CASP vers une adresse auto-hébergée qu'il indique utiliser pour sa conservation en propre.

Cette mesure ne doit pas être conçue comme une exemption, ni comme une nouvelle obligation autonome de preuve de contrôle des adresses auto-hébergées. Elle devrait simplement permettre de limiter les informations collectées à ce qui est strictement nécessaire lorsque l'usage de conservation en propre ne présente pas, en lui-même, d'indicateur spécifique de risque élevé.

En particulier, l'usage d'une adresse auto-hébergée ne devrait pas conduire par défaut à exiger l'identité d'un bénéficiaire tiers, l'existence d'un intermédiaire ou des informations de destination qui ne sont ni pertinentes ni disponibles. Les RTS devraient éviter toute interprétation conduisant à étendre la collecte au-delà de ce qui est nécessaire au risque LBC/FT identifié.

INBi recommends adding the following simplified due diligence measure:

"Where the ML/TF risk is low and an identified and verified customer carries out a withdrawal of bitcoin to a self-hosted address for self-custody purposes, simplified due diligence may consist in treating self-custody as the relevant information on the intended use or destination of funds, provided that no specific higher-risk indicator is identified. The use of a self-hosted address should not, in itself, require the collection of additional destination information beyond what is relevant, available and necessary to assess the identified ML/TF risk."

* 5. Additional observations: Do you have any additional comments relevant to the draft RTS that have not been covered above? Please ensure that comments refer to a specific article, are precise, and, where possible, supported by evidence. Where necessary, comments should also include a proposed solution.

5000 character(s) maximum

L'Institut National de Bitcoin (INBi) est un think tank français indépendant, constitué sous forme d'association loi 1901. Cette contribution s'appuie sur sa note de recherche d'avril 2026 "Collecter plus, protéger moins ?", consacrée aux fuites de données, à l'irréversibilité du préjudice et à la proportionnalité des obligations de collecte dans le cadre européen LBC/FT https://inbi.fr/collecter-plus-proteger-moins-amlr-tfr/.

Cette note a bénéficié d'une contribution et relecture externes d'Estelle De Marco, docteure en droit, sur la discussion juridique. Les développements méthodologiques relatifs aux analyses d'impact, à la nécessité, à la proportionnalité et à la distinction DPIA/PIA s'appuient notamment sur ses travaux publiés, en particulier "A DPIA is a PIA" : https://inthemis.fr/ressources/A-DPIA-is-a-PIA.html

La présente contribution ne doit pas être comprise comme un soutien général à l'extension du cadre européen de collecte de données financières. L'INBi prend acte du mandat confié à AMLA, mais considère que l' accumulation de normes techniques de vigilance peut, si elle n'est pas strictement encadrée, rendre arbitrairement la conservation en propre progressivement plus complexe, plus risquée et moins accessible pour les utilisateurs légitimes.

Sans clarification, le projet de RTS laisse subsister une incitation pratique à la surcollecte défensive. Cette incitation est particulièrement dangereuse dans le cas de registre public, car l'association entre identité civile, adresse et historique transactionnel peut révéler durablement des éléments patrimoniaux et exposer physiquement les personnes concernées. Une telle mise en danger des personnes paraît disproportionnée, particulièrement lorsqu'il n'existe pas de raison valable de penser que ces personnes sont en train de commettre une infraction.

L'INBi recommande donc qu'AMLA intègre explicitement, dans les RTS ou dans les considérants, un principe de nécessité, de proportionnalité et de minimisation des données. L'harmonisation ne doit pas devenir une standardisation de la collecte maximale, laquelle serait contraire à la Charte des droits fondamentaux de l'Union européenne et à la Convention européenne des droits de l'Homme.

Proposed horizontal recital:

"Customer due diligence measures should be applied in accordance with the principles of necessity, proportionality and data minimisation. In particular, where information relates to bitcoin addresses, transaction histories or other data that may reveal a person's holdings or patterns of behaviour, obliged entities should not collect, process or retain more information than is strictly necessary to mitigate a specific and documented ML /TF risk."

This is especially important because AMLA's own IA/CBA acknowledges that quantitative figures for this mandate are currently unavailable and that the assessment is primarily qualitative. Where the privacy and physical-security costs of overcollection are potentially irreversible, the RTS should avoid creating incentives for maximum collection in the absence of demonstrated marginal AML/CFT benefit.

Section 3 - Additional substantive input

Use this section to provide feedback on specific articles of the draft RTS, in case these were not already covered in your responses to the previous questions.

For each reply, please describe the issue identified, indicating, where relevant, whether it relates to legal certainty, proportionality, technical implementation or other factors. You are kindly asked to provide alternative drafting proposals and to explain why your proposal would be more appropriate.

Do you have any comments on a specific article in the draft RTS? There is no need to repeat comments made in the previous sections of this survey.

- (●) Yes
- ( ) No

* Please state the article number in simple figures, without referring to the subparagraphs or points (e.g. '3' or '21')

Only values between 1 and 33 are allowed

30

* Please share your comments below, specifying the subparagraph and point, if applicable (e.g. paragraph 1 point (a)).

5000 character(s) maximum

Article 30 — Screening requirements
INBi does not object to targeted financial sanctions screening as such. However, Article 30 should be clarified to ensure that screening of digital wallet addresses remains limited to what is necessary to determine whether a customer, beneficial owner or relevant person is the intended target of targeted financial sanctions. The reference to digital wallet addresses should not be interpreted as requiring or encouraging the systematic retention of address graphs, extended transaction histories, probabilistic clustering data or commercial risk-scoring data unrelated to a specific targeted financial sanctions match. Where a digital wallet address generates a match, obliged entities should apply proportionate human review and avoid automated exclusion or excessive retention beyond what is necessary to resolve the match.

Do you have any other comments on a specific article in the draft RTS?

- (●) Yes
- ( ) No

* Please state the article number in simple figures, without referring to the subparagraphs or points (e.g. '3' or '21')

Only values between 1 and 33 are allowed

7

* Please share your comments below, specifying the subparagraph and point, if applicable (e.g. paragraph 1 point (a)).

5000 character(s) maximum

Article 7 — Non-face-to-face verification
Where remote verification involves images, videos, sound or other identity data, the RTS should explicitly

require strict retention limitation, purpose limitation and protection against secondary use, including biometric processing or reuse for unrelated risk-scoring purposes, unless such processing is strictly necessary, lawful and proportionate.

Do you have any other comments on a specific article in the draft RTS?

- ○ Yes
- ◉ No

Do you have any comments on the recitals? The recitals are the statements at the start of the draft RTS and are numbered from (1) to (25).

- ◉ Yes
- ○ No

Please specify which recital you refer to, and share your comments below.

New recital after recital (21):

"Customer due diligence measures should be applied in accordance with the principles of necessity, proportionality and data minimisation. In particular, where information relates to bitcoin addresses, transaction histories or other data that may reveal a person's holdings or patterns of behaviour, obliged entities should not collect, process or retain more information than is strictly necessary to mitigate a specific and documented ML /TF risk. Risk-based customer due diligence should not be understood as maximum information collection."

Do you have any comments on the Annex in the draft RTS?

- ◉ Yes
- ○ No

Please share your comments below.

Annex I — Electronic identification attributes
The list of attributes in Annex I should not be interpreted as requiring obliged entities to retrieve, process or retain all available attributes in every CDD scenario. In line with necessity, proportionality and data minimisation, obliged entities should retrieve and retain only the subset of attributes that is necessary for the specific CDD measure and ML/TF risk identified. This is particularly important where identity attributes are combined with bitcoin addresses or transaction-related data, as such combination may reveal long-term financial behaviour and holdings.

Section 4 - Overall assessment

* How would you rate the proposals set out in the draft RTS overall?

- ☐ Inadequate
- ☑ Somewhat inadequate
- ☐ Neutral
- ☐ Good
- ☐

Excellent

Thank you very much for your feedback.

Contact

Contact Form