bitkom

Position Paper

2026 May

Draft RTS on Customer Due Diligence under Article 28(1) of Regulation (EU) 2024/1624

Answers to Consultation Questions

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.

Verification of Nationality

i. **Provision concerned**: Article 5 in conjunction with Recital 3 (Nationality)

ii. **Rationale for the position**: The current draft lacks internal coherence between the operative provisions and the recitals.

Article 5:»...obliged entities shall obtain information on all nationalities...«

Recital 3: »Where a person holds multiple nationalities and declares them in good faith, verifying one nationality will be sufficient.«

iii. **Drafting proposal**: Verification of one single nationality shall be considered sufficient.

iv. **Explanation**: The discrepancy creates legal uncertainty for obliged entities regarding the extent of their verification duties. Streamlining the criteria to a single nationality reduces the administrative burden on obliged entities.

Given that other geographical risk-based criteria provide more meaningful insights into a customer's risk profile (e.g. country of residence, centre of economic activity, or country of registration), focusing on multiple nationalities is disproportionate to the actual risk-mitigation value it provides. Obliged entities should, however, retain the discretion to investigate further nationalities on an individual case-by-case basis when necessary to adjust a risk rating (e.g., in the case of risk associated with »Citizenship by Investment«) or to accurately distinguish between individuals during list-screening activities.

Use of Data Already Held by Obliged Entities

i. **Provision concerned**: Article 3(1)(c) and (d) of the RTS under Article 19(9), as well as Article 21(1)(b) of the RTS under Article 28(1), in conjunction with the corresponding recitals

ii. **Rationale for the position**: The draft RTS under Article 19(9) and Article 28(1) both require obliged entities to take into account data or information »available to the obliged entity« or »any information provided by the customer, including information that obliged entities may already hold« in different provisions.

This includes Article 3(1)(c) and (d) of the RTS under Article 19(9) as well as Article 21(1)(b) of the RTS under Article 28(1). The recitals provide further details on the kind of information covered by these provisions. For example, Recital (12) of the RTS under Article 19(9) refers to »information available that customers are connected via family ties«, while Recital (13) refers to IP addresses, device identifiers and geolocation.

In most cases, these kinds of information will constitute personal data within the meaning of Article 4 or even Article 9 of the GDPR (e.g. sexual orientation may be indicated by family ties). However, the draft RTS do not provide a sufficient legal basis for the processing of such data in accordance with Article 6(c) GDPR, but only require obliged entities to »take into account« such data.

Personal data that is already »available to an obliged entity« has been collected for a different purpose and in accordance with a distinct legal basis. As a result, the obliged entity is not free to use it for any other purpose as it deems appropriate, in particular without informing the data subject accordingly.

iii. **Drafting proposal**: We therefore suggest deleting the requirement to »take into account« or »consult« such data in the respective RTS. The alternative, a general requirement to obtain such data for AML purposes, would lead to an excessive burden of the obliged entities as well as their customers.

Timeliness of information provision

i. **Provision concerned**: Article 22 (a)

ii. **Rationale for the position**: "Immediately" is not defined in the RTS or the AMLR. In a digital environment, a supervisor might interpret this as "real-time API access," whereas an operational reality might involve a longer retrieval window for older archived files. In this context, "immediately" is highly subjective and creates

significant legal uncertainty for obliged entities. It creates a risk of technical non-compliance if an obliged entity cannot prove "instant" access to its supervisor.

iii. **Drafting proposal**: Article 22 (a): «(a) the credit institution is satisfied that the account holder will provide the information and documents required pursuant to Article 20(1)(h) of Regulation (EU) 2024/1624 in relation to clients for whom it administers their funds, without undue delay after such request has been made by the credit institution;"

Effective Supervision Requirement

i. **Provision concerned**: Article 22 (c)

ii. **Rationale for the position**: This provision establishes as a condition that the account holder must be «effectively supervised for compliance with obligations as provided for in point (b)". The issue is that there is no clarity as to what «effectively supervised" means. Like the term "satisfied," this is a subjective standard that is not defined in the AMLR or the RTS.

Therefore, there is no legal certainty as to how an obliged entity (or the account holder itself) shall prove effective supervision. This leaves it to the discretion of the obliged entity and its local auditor to judge whether the supervisor provides "effective" oversight. A supervisor in one Member State might consider the supervisory practices of another Member State to be insufficient, leading to the rejection of the simplified due diligence (SDD) measures entirely.

If "effective supervision" cannot be objectively verified, obliged entities will likely default to full CDD to avoid regulatory risk, rendering the simplification in Article 22 useless in practice.

iii. **Drafting proposal**: Article 22 (c): »(c) the account holder is subject to supervision by a supervisory authority as defined in Article 2(1), point (46), of Regulation (EU) 2024/1624, or, in the case of a third country, is subject to equivalent supervision by a competent authority.«

Risk Threshold for Simplified Due Diligence

i. **Provision concerned**: Article 22 (d)

ii. **Rationale for the position**: The requirement that the ML/TF risk must be »low« is inconsistent with the threshold established in Article 17(1)(c) for Collective Investment Undertakings, which allows for simplified measures in »low or standard« risk scenarios. Both provisions address fundamentally similar structures where an intermediary manages third-party funds.

Restricting Article 22 to »low« risk relationships creates an uneven playing field and imposes a disproportionate burden on obliged entities. It forces them to justify a »low« risk categorisation for entities that are already subject to robust EU supervision and CDD requirements.

This subjectivity will lead to a fragmented application of the standards, as different supervisors will have varying expectations for what constitutes »low« risk in a cross-border context.

iii. **Drafting proposal**: Remove such a requirement; or »(d) the ML/TF risk associated with the business relationship is low or standard;«

Assessment of Due Diligence Standards

i. **Provision concerned**: Article 22 (e)

ii. **Rationale for the position**: Another condition for the application of Article 22 is that the obliged entity must be satisfied that the account holder applied robust and risk-sensitive due diligence measures.

However, the terms »satisfied« and »robust« are highly subjective and do not provide the legal certainty required for a harmonised AML/CFT framework. This provision risks creating an unsustainable administrative burden for both credit institutions and the account holders (in such a scenario). Without clear, Union-wide standards for what constitutes »satisfaction,« there is a significant risk that credit institutions will default to full, redundant CDD to mitigate potential supervisory criticism, thereby rendering the simplified measures for pooled accounts ineffective.

To achieve the AMLA's objective of operational efficiency and harmonisation, the RTS should specify objective evidence that an obliged entity can use to meet this requirement. This should leverage existing institutional safeguards, such as independent audits or the status of being a regulated obliged entity within the Union.

iii. **Drafting proposal**: Article 22 (e): »(e) the credit institution obtains evidence that the account holder applies customer due diligence measures in compliance with Regulation (EU) 2024/1624. Such evidence may include independent AML audit reports or certifications.«

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.

i. **Rationale for the position**: Article 7, 3(a) requires an examination of the customer's identity document. However, accepting a copy of the original document would introduce more flexibility while at the same time ensuring high security standards during the verification process.

ii. **Drafting proposal**: To reduce unnecessary administrative burden in the verification process on a non-face-to-face basis, we suggest complementing Article 7, 3(a) as follows:

»*controls to ensure that the natural person presenting the customer's identity document, passport or equivalent, <u>including a copy thereof</u>, is the person in the picture on the document.*«

iii. **Additional safeguard**: Where a copy of the identity document is accepted, the verification process must include additional controls to detect presentation attacks (deepfakes, synthetic images, injection of manipulated media) in accordance with ISO/IEC 30107-3 and CEN/TS 18099, as well as document template validation against known genuine templates. Accepting copies without such safeguards significantly increases the risk of fraud through AI-generated synthetic documents.

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.

i. **Provision concerned**: Article 7, 1 refers to electronic identification means for verification measures, but does not sufficiently take into account already established and highly trusted verification methods. A clarification that existing verification measures such as video identification comply with non-face-to-face verification would enhance legal certainty.

ii. **Drafting proposal**: To clarify verified means of non-face-to-face identification, we suggest complementing Article 7, 1:

»*To comply with the verification requirements pursuant to Article 22(6) of Regulation (EU) 2024/1624 in a non-face-to-face situation, obliged entities use electronic*

identification means that meet the requirements of Regulation (EU) No 910/2014 with regard to the assurance levels 'substantial' or 'high', or relevant qualified trust services such as video identification and qualified electronic attestations of attributes (QEAA) pursuant to Articles 45d to 45g of Regulation (EU) 2024/1183.«

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.

No.

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.

We welcome AMLA's initiative to specify the criteria for Simplified Due Diligence (SDD) and thereby strengthen the risk-based approach. Currently, however, SDD often fails to provide actual time and effort savings compared to standard KYC processes, which undermines its regulatory intent. The resource-intensive »pre-check« required to qualify for SDD often drives obliged entities to default to standard due diligence to avoid legal uncertainty.

The primary obstacle in the process is the complexity of the UBO drill-down, particularly regarding legal entities. This exhaustive identification process for corporate structures is the leading cause of SDD underutilisation. To ensure that SDD becomes an operationally viable tool, we propose the following:

AMLA should provide a list of low-risk factors for SDD (e.g. specific entity types in specific geographies) that are determinable at the very beginning of a business relationship. If a client meets these predefined criteria, obliged entities should be able to apply SDD measures immediately. Without such clarity, SDD offers no practical added value, as the most resource-intensive KYC work would have already been performed.

6. 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.

We would also like to provide additional observations regarding the risk factors associated with electronic money instruments under Article 31 and Section 8 of the draft RTS under Article 28(1).

In this context, we support the changes introduced by the EBA to the risk factors that NCAs should consider when determining the extent of the CDD exemption for e-money products, compared to the first draft presented by the EBA (Draft RTS under Article 28(1) – Section 8: Risk Factors Associated with Features of Electronic Money Instruments; Article 31: Risk Factors). The EBA has clarified that the risk factors set out in the RTS constitute a non-exhaustive list of examples, which do not need to be met cumulatively or in their entirety. NCAs are instead expected to consider the extent to which one or more of these risk factors are present. These clarifications are important, as they enhance legal certainty for both market participants and NCAs.

However, we would encourage AMLA to reassess the risk factors in terms of their practical relevance and usability. For example, »the extent to which the payment instrument is issued at a nominal or no charge« is, in our view, not a factor that determines the risk of an e-money product being misused for money laundering or terrorist financing purposes. Furthermore, Article 31, points (d) and (e) set out risk factors that closely resemble the criteria applied to products falling under the so-called »limited network/limited range exemption« provided for in the Second Payment Services Directive. Such products fall outside the definition of e-money. In our view, the extent to which an exemption for e money products can be applied should not depend on criteria that largely replicate those determining whether a product qualifies as e-money in the first place.

In addition, we encourage AMLA to remove the risk factor relating to whether the entity distributing an e-money product is itself an obliged entity (point (i)). By definition, the CDD exemption provides for the possibility of not applying certain CDD measures. Whether the entity refraining from carrying out specific CDD measures is itself an obliged entity is, in this context, irrelevant. This risk factor is also inconsistent with the EBA's statement that risk factors should focus solely on the e-money product, not on the issuer or its organisational set-up. Whether a distributing entity is itself an obliged entity does not relate to the characteristics of the e-money product.

Bitkom represents more than 2,200 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 700 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by

Bitkom e.V.

Albrechtstr. 10 | 10117 Berlin

Contact person

Alina Stephanie Bone-Winkel | Head of Digital Banking & Financial Services

P +49 30 27576-273 | a.bone-winkel@bitkom.org

Responsible Bitkom committee

WG Fintech & Digital Banking

WG Digital Payments

Copyright

Bitkom 2026

This publication is intended to provide general, non-binding information. The contents reflect the view within Bitkom at the time of publication. Although the information has been prepared with the utmost care, no claims can be made as to its factual accuracy, completeness and/or currency; in particular, this publication cannot take the specific circumstances of individual cases into account. Utilising this information is therefore sole responsibility of the reader. Any liability is excluded. All rights, including the reproduction of extracts, are held by Bitkom.