



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

Important: This factsheet reflects the content of the draft RTS on Customer Due Diligence under Article 28(1) of Regulation 2024/1624 at the date of AMLA's final draft. Please note that the RTS remain subject to review and potential amendments by the European Commission and their provisions will only become definitive upon publication in the Official Journal of the European Union.

This factsheet accompanies the RTS on customer due diligence and should be considered when the RTS are endorsed by the European Commission in a delegated Regulation at its date of application.

1. Objective

The purpose of this factsheet is to present, in a concise and accessible manner, selected key aspects of the Regulatory Technical Standards (RTS) developed under the mandate set out in Article 28(1) of Regulation (EU) 2024/1624 (AMLR). The AMLR establishes the legal framework for customer due diligence across the Union, while the RTS specify specific elements of that framework to promote its consistent and effective implementation. **This factsheet is intended as an overview of selected RTS provisions and does not cover the full range of articles contained in the RTS.** This means that the RTS in all instances, takes precedence. The factsheet serves merely as a concise overview, highlighting the principal elements of that RTS.

The mandate under Article 28(1) of the AMLR requires AMLA to specify the requirements that apply to obliged entities pursuant to Article 20 of the AMLR on CDD, and the information to be collected for that purpose. The RTS must also specify:

- the types of simplified due diligence (SDD) measures which obliged entities may apply in low-risk situations, and the reliable and independent sources of information that may be used to verify identification data;



- the risk factors associated with features of electronic money instruments that supervisors should consider when determining the extent of CDD exemptions on certain electronic money products; and
- the attributes which electronic identification means must meet to comply with the AMLR.

This factsheet should be read in conjunction with the AMLR and the RTS. It is intended solely as a summary document and does not replace, amend, or supplement the requirements set out in the AMLR or the RTS.

2. Key aspects

Identification and verification of the customer and the beneficial owners

The AMLR requires obliged entities to identify and verify the identity of their customers, any person purporting to act on behalf of the customer, the natural persons on whose behalf or for the benefit of whom a transaction or activity is being conducted, and the beneficial owners before establishing a business relationship and when carrying out an occasional transaction. The RTS specify the information to be collected, thereby ensuring a consistent approach to data collection.

In particular, the RTS set out the information that should be collected in relation **to names, addresses and place of birth**:

- For natural persons, obliged entities should obtain all names, including first names (given names), and surnames (family names), appearing on an identity document, passport or equivalent or through an electronic identification mean and relevant qualified trust services. The information to be collected on place of birth should include at least the country, the state, the city, municipality, town, or the village.
- For legal entities, obliged entities should obtain the legal name and, where different, the trade name.

Address information should include the country and the city, municipality, town or village as mandatory data points, together with any other address elements such as the state, postal code, street name and building number, where such information exists. Where no beneficial owner can be identified and obliged entities are therefore required to identify the senior managing officials, the legal or official office address of the legal entity may be obtained instead of the senior managing official's residential address and country of residence, in order to minimise the processing of personal data.



The RTS also further specify the information to be collected on **nationalities**. Obligated entities should take reasonable measures to establish whether a natural person holds more than one nationality; however, where multiple nationalities are declared, **verifying one nationality is sufficient**.

Article 22(1) AMLR, on identification, in conjunction with Article 22(6) AMLR, on verification, is clear that all the data points in Article 22(1) AMLR used for the identification purposes, need to be verified. However, in **low-risk situations**, obliged entities are required to collect and verify a reduced set of identification data. For customers who are **natural persons**, the information to be collected and verified consists of the core identity data typically contained in a passport or national identity document, namely all customer's names and surnames, date and place of birth and nationality, or their statelessness, refugee or subsidiary protection status. In these circumstances, obliged entities are **not required to obtain and verify the customer's address**. This ensures that obliged entities have sufficient and verifiable information to establish the identity of their customers, while keeping the requirements proportionate to the low level of ML/TF risk.

Where an identity document, passport or equivalent **does not contain all the information required for customer identification and verification**, obliged entities should acquire the missing information from **reliable and independent sources**, as set out in the AMLR.

When acquiring such missing information from reliable and independent sources, the RTS clarifies the **factors that should be considered to ensure the reliability and independence of those sources**.

Obligated entities should also ensure that they can understand and properly assess the information obtained, irrespective of the language used.

Alternative verification measures in non-face-to-face circumstances

In situations where an identity document, passport or equivalent **cannot be submitted in a face-to-face context** and the natural person does not have access to the electronic identification means and relevant qualified trust services as set out in the AMLR, obliged entities can verify the identity through **alternative verification solutions**, as long as these solutions use reliable and independent information sources and include the safeguards listed in Article 7 of the RTS. Such a situation may occur, for example, where the customer cannot reasonably submit the identity document, passport or equivalent in person and where the customer cannot use the electronic identification means and relevant qualified trust services referred to above. To ensure financial inclusion for such persons and to ensure that financial and commercial services can continue to be provided, the RTS permit the use of alternative verification methods.



What information electronic identification means and relevant qualified trust services should be able to provide

Annex I of the RTS set out the minimum attributes that electronic identification means and qualified trust services **should be capable of providing** for customer due diligence purposes. However, this does **not imply that obliged entities are required to identify or verify all attributed listed in Annex I in each and every case**. Certain data points are only applicable to specific customer types for example, data points concerning legal entities are not relevant when the customer is a natural person, while certain data points may only be required when available, such as specific address elements. Nevertheless, electronic identification means and qualified trust services should be capable of capturing the minimum attributes set out in Annex I.

Reasonable measures for verification of the beneficial owner and the persons on whose behalf or for the benefit of whom a transaction or activity is being carried out

The RTS also set out the sources of information that obliged entities may use when taking reasonable measures to verify the identity of beneficial owners and the persons on whose behalf or for the benefit of whom a transaction or activity is being carried out. These sources may include public registers and other reliable national systems, such as business registers, residence registers, tax registers, passport databases and land registers, as well as information from reputable data service providers, including credit agencies, credit or financial institutions, other obliged entities within the same group, and documents of legal entities or legal arrangements where the beneficial owner is named, and where the identity of the named person is certified by persons that are authorised for document certification purposes. In situations of low risk, information from the central beneficial ownership register may be used to identify the beneficial owner. However, as set out in the AMLR, information from the register alone is not sufficient to fulfil the verification requirements, obliged entities should verify that information using information obtained from the customer or other reliable sources.

Purpose and intended nature of the business relationship or the occasional transaction

Identification of the purpose and intended nature of a business relationship or occasional transaction is a central element of the customer due diligence measures. The RTS set out **non-exhaustive examples of information** that may be used to understand the purpose and intended nature of a business relationship or occasional transaction. This information should **not be treated as a prescriptive checklist** to be followed systematically. Instead, it should be applied in a proportionate and risk-based manner, taking into account the specific characteristics of the obliged entity and the relevant ML/TF risks. To that end, obliged entities shall also consider relevant **information already available to them or from other obliged entities within the same group**.



In situations assessed as presenting a **low risk of ML/TF**, obliged entities may determine the purpose and intended nature of the business relationship or occasional transaction on the basis of **information that can reasonably be inferred from the customer's profile, activities, products, services or transactions already available**, provided that such information is sufficient for that purpose.

Screening of targeted financial sanctions and politically exposed persons (PEPs)

As part of the customer due diligence measures, obliged entities must verify whether the customer and the beneficial owners are subject to targeted financial sanctions and determine whether the customer, the beneficial owner and, where relevant, the person on whose behalf or for whose benefit a transaction or activity is being carried out, is a politically exposed person (PEP), a family member or a person known to be a close associate.

The screening of targeted financial sanctions and PEPs must be performed through **automated screening tools or solutions, manual checks, or a combination of both**. Where applicable and available, **aliases, trade names and digital wallet addresses are also relevant** for targeted financial sanctions screening purposes.

Transitional period for existing and ongoing business relationships

For customers whose business relationship with an obliged entity was established **before the** date of entry into force **of the RTS and is existing on that date**, the customer documentation, information and data are brought into compliance with the RTS and AMLR on a **risk-sensitive basis**, and no later than **one year for higher risk customers and five years for all other customers**, as set out in the AMLR.