DIGITALSIGN - CERTIFICADORA DIGITAL, SA.

AMLR & eIDAS 2.0

THE NEW IDENTITY VERIFICATION INFRASTRUCTURE FOR EUROPEAN FINANCIAL INSTITUTIONS

WHAT CHANGES IN 2027, WHAT IS AT STAKE, AND HOW TO PREPARE YOUR ORGANISATION

CONTENTS

Executive Summary

On 10 July 2027, Regulation (EU) 2024/1624, the new Anti-Money Laundering Regulation (AMLR), becomes directly applicable throughout the European Union. It is worth stressing the distinction at the outset: the Regulation entered into force in 2024, but only becomes applicable from that date. For the first time, the rules on combating money laundering will no longer depend on fragmented transposition by each Member State, but will apply uniformly.
Article 22(6)(b) of the AMLR codifies the methods accepted for remote identity verification: electronic identification means compliant with Regulation (EU) No 910/2014 with regard to the assurance levels 'substantial' or 'high', and relevant qualified trust services, namely qualified electronic signatures (QES) and qualified electronic attestations of attributes (QEAA). In parallel, Article 5f of eIDAS 2.0 requires financial institutions to accept the EUDI Wallet, upon the user's request, within 36 months of the entry into force of the relevant implementing acts, that is, by 24 December 2027.
In this white paper, we analyse the impact of these changes, explain what they mean for customer due diligence (CDD), and set out a practical preparation roadmap addressed to those responsible for compliance, operations and technology.

1. The Problem with the Current Regime

Consider the case of a Portuguese fintech with European expansion ambitions. Today, its KYC procedures have been designed around the specific features of Law No 83/2017 of 18 August. Tomorrow, when it opens operations in Spain, Germany or Poland, it will find that each jurisdiction has transposed the Fourth and Fifth Anti-Money Laundering Directives in a slightly different way. What is the practical result? Fragmented rules, compliance costs multiplied across each market, and regulatory competition that favours incumbents, that is, those with greater resources to manage jurisdictional complexity.

The Cost of Fragmentation

According to Europol, suspicious financial activity accounts for between 0.7% and 1.2% of the European Union's annual GDP, that is, around 1% (more than EUR 160 billion per year) flowing through the European financial system. A substantial part of this problem is directly linked to inconsistency in the application of CDD rules across Member States. *(Source: Europol, From Suspicion to Action: Converting Financial Intelligence into Greater Operational Impact, Financial Intelligence Group, 2017. The euro figure is an approximation derived from the percentage of GDP.)*

The AMLR was designed precisely to address this problem. By replacing a directive with a directly applicable regulation, the European legislator removes the margin for national transposition and creates, for the first time, a genuine European single rulebook for the prevention of money laundering.
For financial institutions, this represents both a challenge and an opportunity: the challenge of adapting well-established processes to a new regulatory reality; and the opportunity to simplify cross-border operations on the basis of a unified set of rules.

2. Article 22 of the AMLR: Required Reading

2.1. The Remote Identity Verification Regime

Article 22 of the AMLR, headed 'Identification and verification of the identity of the customer and the beneficial owner', sets out the customer due diligence (CDD) requirements and, in particular, the methods accepted for identity verification where the customer is not physically present. Point (b) of paragraph 6 lies at the heart of this change:

> *(b) the use of electronic identification means that meet the requirements laid down in Regulation (EU) No 910/2014 with regard to the assurance levels 'substantial' or 'high', and of relevant qualified trust services within the meaning of that Regulation.*
>
> **Article 22(6)(b), Regulation (EU) 2024/1624 (AMLR)**

In practical terms, this provision recognises the following identity verification methods as compliant:

- **(i) national eIDs notified under eIDAS, at a substantial or high assurance level, such as the Portuguese Cartão de Cidadão and Chave Móvel Digital, the Spanish DNIe or the Dutch DigiD;**
- **(ii) EUDI Wallets, the European Digital Identity Wallets that each Member State must provide by 24 December 2026;**
- **(iii) qualified trust services (QTS), namely qualified electronic signatures (QES) and qualified electronic attestations of attributes (QEAA).**

2.2. The Weight of Recital 66

Recitals have no direct normative force, but they are decisive for the interpretation of the provisions. Recital 66 of the AMLR is particularly revealing as to the intention of the European legislator:

> *The electronic identification provided for in that Regulation should be taken into account and accepted by obliged entities for the customer identification process. The use of such identification means may, where appropriate risk-mitigation measures are in place, reduce the level of risk to normal or even low. Where a customer does not have such electronic identification, for example due to the nature of their residence status in a given Member State or their residence in a third country, verification should be carried out through relevant qualified trust services.*
>
> **Recital 66, Regulation (EU) 2024/1624 (AMLR)**

This passage has substantive implications for risk management. The use of eIDAS-compliant identification means is not a mere technical option: it is a risk-reduction factor recognised by the regulator itself. To that extent, and provided that adequate mitigation measures are in place, it constitutes a relevant element of the risk assessment, capable of justifying the classification of the customer at a lower level, normal or even low, without prejudice to the assessment remaining risk-based.

Moreover, the same recital indicates the course to be followed where the customer does not have eIDAS-compliant electronic identification, for example due to the nature of their residence status or because they reside in a third country: in such cases, verification 'should be carried out through relevant qualified trust services'. Accordingly, without prejudice to electronic identification means constituting the primary route, the legislator highlights qualified trust services as the preferred verification mechanism where the customer does not have suitable electronic identification means, which is of particular relevance to the onboarding of third-country customers. It must be borne in mind, however, that a recital does not, in itself, create an autonomous obligation, and that point (a) of Article 22(6) continues to permit other methods: this is, therefore, a preference resulting from a systematic interpretation and not a literal requirement of the enacting terms.

3. The AMLR-eIDAS 2.0 Convergence: A Twofold Obligation

The AMLR does not operate in a vacuum. Its application is deeply intertwined with eIDAS 2.0, that is, Regulation (EU) 2024/1183, which revised the European digital identity framework originally established in 2014. This convergence gives rise to a twofold regulatory obligation that financial institutions must understand in full.

This convergence is not merely doctrinal: it is expressly echoed in the text of eIDAS 2.0 itself. Indeed, Recital 62 of Regulation (EU) 2024/1183 acknowledges that '*secure electronic identification and the provision of attestation of attributes should offer additional flexibility and solutions to the financial services sector to allow the identification of customers and the exchange of specific attributes necessary to comply, for example, with customer due diligence requirements*' under the Regulation that went on to establish the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA). It was thus the European digital identity legislator itself that pointed to electronic identification and trust services as an instrument for complying with customer due diligence obligations.

3.1. Article 5f of eIDAS 2.0 and the EUDI Wallet

Whereas the AMLR governs what obliged entities must accept for anti-money laundering purposes, Article 5f of eIDAS 2.0, headed 'Cross-border reliance on European Digital Identity Wallets', goes further. Under paragraph 2 thereof, private relying parties that are required, by virtue of Union or national law (or by contractual obligation), to use strong user authentication for online identification, a category that includes, in particular, banking and financial services, must accept the EUDI Wallet upon the voluntary request of the user. Microenterprises and small enterprises are exempt. The time limit is 36 months from the entry into force of the relevant implementing acts, which occurred on 24 December 2024, meaning, in practice, by 24 December 2027.

Acceptance Obligation

Article 5f of eIDAS 2.0 is not a recommendation, but a legal obligation: financial institutions subject to strong user authentication will have to accept the EUDI Wallet as a means of identification, upon the user's request, by 24 December 2027 (36 months after the entry into force of the implementing acts). Non-compliance may give rise to penalties, both under eIDAS and under the AMLR.

The EUDI Wallet is a mobile application that allows the holder to store and present verified identity attributes, from the national identity document to professional attributes or academic qualifications. For CDD purposes, two aspects must be distinguished. As an electronic identification means, the wallet is provided under a scheme with a high assurance level (Article 5a(11) of eIDAS 2.0). Qualified electronic attestations of attributes (QEAA), by contrast, as qualified trust services, attest specific attributes, corresponding to the qualified level (the most demanding form of attestation), and do not in themselves constitute a means of identification, but rather complement it.

3.2. The Architecture of Assurance Levels

A central element of this regime is the concept of the level of assurance (LoA). eIDAS defines three levels, which determine the evidential weight of an electronic identification. It must be borne in mind that the scale of assurance levels relates, under Article 8, to electronic identification means; qualified trust services (QES, QEAA), in turn, do not fall within that scale, but rather produce the qualified legal effects that the Regulation confers upon them.

Level	Characteristics	AMLR Relevance
Low	Self-declaration; simple password authentication	Not recognised for CDD
Substantial	Identity verification with a physical document and two-factor authentication	Accepted for CDD [Art. 22(6)(b)]
High	Enhanced requirements for verification and for the management of identification means; the level at which the EUDI Wallet is provided, through which QES and QEAA are presented	**Accepted for CDD; enables risk reduction [Art. 22(6)(b) and Recital 66]**

4. Timeline: What Changes and When

Date	Milestone / Obligation
24 Dec. 2026	**Provision of the EUDI Wallet** Each Member State must provide at least one EUDI Wallet to its citizens (Art. 5a eIDAS 2.0).
10 Jul. 2027	**AMLR becomes applicable** Regulation (EU) 2024/1624 becomes directly applicable. Obliged entities must have compliant CDD procedures in place, including the acceptance of notified eIDs and qualified trust services.
24 Dec. 2027	**Mandatory acceptance of the EUDI Wallet** Deadline (36 months after the implementing acts) for financial institutions to accept the EUDI Wallet, upon the user's request (Art. 5f eIDAS 2.0).

The timetable is demanding, especially for organisations that have not yet begun their impact assessment. Integration with eID or QTSP providers, the adaptation of onboarding systems, the updating of risk policies and the training of compliance teams cannot be accomplished in a matter of weeks.

5. Comparison of Verification Methods

The AMLR does not eliminate existing verification methods, but it significantly alters their relative position in terms of compliance, risk and operational efficiency. The following table sets out a comparison of the main methods available:

Method	Legal Basis	Assurance Level	Residual Risk	Risk Reduction
Notified national eIDs	Art. 22(6)(b)	Substantial / High	Medium/Low	Yes (with adequate measures)
EUDI Wallet (QEAA)	Art. 22(6)(b) + Art. 5f eIDAS 2.0	High	Low	Yes
QES (qualified signature)	Art. 22(6)(b)	Qualified service	Low	Yes
Videoconference (with docs.)	Art. 22(6)(a)	N/A	Medium	Possible
Physical documents and third party	Art. 22(6)(a)	N/A	High	Higher operational risk

Note: the 'Residual Risk' and 'Risk Reduction' columns reflect an operational assessment and not a classification established by the AMLR.

5.1. The Privileged Position of QTSPs

Reading point (b) of Article 22(6) together with Recital 66 places qualified trust service providers (QTSPs) in a position of particular relevance within the new AML compliance ecosystem. Unlike videoconferencing, which requires human resources and does not scale, or physical documents, which involve intermediaries and a greater risk of fraud, QTSPs offer:

- (i) automated and traceable verification, with a cryptographic chain of trust;
- (ii) a high assurance level, recognised by all Member States of the Union;
- (iii) native compatibility with the EUDI Wallet and the eIDAS 2.0 ecosystem;
- (iv) documented risk reduction, recognised by the regulator (Recital 66);
- (v) scalability for high-volume onboarding processes.

For organisations with high onboarding volumes, such as neobanks, investment platforms or payment fintechs, the automation afforded by QTSPs is not merely a compliance advantage: it is also a significant factor of operational efficiency. This centrality does not stem from the AMLR alone: as we have seen, Recital 62 of eIDAS 2.0 itself expressly points to the provision of attestation of attributes as a solution enabling the financial services sector to fulfil customer due diligence obligations.

6. Practical Implications by Type of Entity

6.1. Traditional Banks and Credit Institutions

Traditional banks face a modernisation challenge. Most KYC procedures still rely on hybrid processes that combine videoconferencing with the manual verification of documents. This is a functional model, but a costly and slow one that is difficult to scale.

The AMLR generates regulatory pressure towards digitalisation that can, however, be harnessed as an opportunity for transformation: replacing manual processes with automated flows based on eID and QTSPs, reducing operational costs while, at the same time, improving the quality and auditability of the process.

6.2. Fintechs

For fintechs, the AMLR is at once a validator and an accelerator. The good practices that many already adopt, namely fully digital onboarding and integration with eIDs, now become the European regulatory standard.

The specific risk for this segment is complacency, that is, assuming that current processes are already compliant without a careful analysis against the exact requirements of the AMLR. The question is not only 'whether' we verify digitally, but 'how' we do so and whether the method used attains the required 'substantial' or 'high' assurance level.

6.3. Asset Managers and Investment Funds

Asset managers frequently have a smaller but more complex client base, as is the case with institutional investors, trusts or SPVs. The AMLR applies, albeit with nuances: the enhanced due diligence requirements for high-risk customers are not eliminated, but rather complemented by the new digital verification infrastructure.

The integration of QEAA through the EUDI Wallet for the verification of attributes, such as investor qualification or professional status, can significantly reduce the cost of enhanced due diligence while maintaining higher compliance standards.

6.4. Cross-Border Operators

For organisations operating in multiple Member States, the AMLR potentially represents the most significant change ever in AML compliance. Replacing a patchwork of national CDD regimes with a single, directly applicable rulebook, equipped with a harmonised verification infrastructure through the eIDAS ecosystem, transforms the cost of European expansion.

The Single Market Opportunity

A fintech that today must maintain specialised compliance teams for each country in which it operates can, with the AMLR and the EUDI Wallet, standardise its onboarding process across the entire Union. A single flow, a single technical standard, compliance in 27 markets.

7. Frequently Asked Compliance Questions

Do our current videoconferencing processes remain valid after the AMLR?
Yes. Point (a) of Article 22(6) retains videoconferencing among the acceptable methods. Nevertheless, point (b), concerning eIDAS-compliant means, is presented as an alternative route and, in the light of Recital 66, is the one to which the legislator expressly attaches the risk-reduction effect. Videoconferencing may continue to be used, but does not, *per se*, benefit from that effect recognised for eIDAS means.

Does the AMLR apply to third-country customers?
The AMLR applies to European obliged entities, regardless of the customer's nationality. As regards third-country customers without a notified eID, Recital 66 clarifies that verification 'should be carried out through relevant qualified trust services', that is, through European QTSPs. This gives QTSPs an even more central position in international onboarding.

How does the AMLR interact with the GDPR?
Identity verification under the AMLR entails the processing of personal data. The lawful basis is, as a rule, compliance with a legal obligation (Article 6(1)(c) GDPR). The use of eIDAS-compliant means may, moreover, simplify the management of processing and minimise data retention, since verification can be carried out by reference to attested attributes, without the transfer of the original documents.

What happens if we are not compliant by July 2027?
The AMLR confers supervisory and sanctioning powers on the competent national authorities, with the coordination of cross-border supervision falling to the new Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA), established by Regulation (EU) 2024/1620. Sanctions may include fines, operational restrictions and, in the most serious cases, the withdrawal of licences. AMLA will also assume direct supervisory powers over the entities posing the greatest systemic risk.

8. Conclusion: An Infrastructure, Not Merely an Obligation

The AMLR and eIDAS 2.0 do not represent merely regulatory changes to be managed. They embody the construction of a European digital identity infrastructure, with the potential to transform the way financial institutions interact with their customers.

The obligation to accept the EUDI Wallet, the legislator's recognition of QTSPs as a preferred verification route, and the risk-reduction effect attached to eIDAS means by Recital 66 create an ecosystem in which digital trust acquires measurable economic and regulatory value.

Organisations that approach this transition as an opportunity for modernisation, and not merely as a compliance cost, will be better positioned to compete in the post-2027 European financial market, with more efficient onboarding processes, lower compliance costs and a technological foundation compatible with the next generation of European digital identity.

The time to act is now. Organisations that begin the adaptation process while still in 2026 will have time to do so strategically; those that delay it risk doing so against the clock, as 10 July 2027 approaches.