DIGITALSIGN - CERTIFICADORA DIGITAL, SA.

AMLR & EIDAS 2.0

A NOVA INFRAESTRUTURA DE VERIFICAÇÃO DE IDENTIDADE PARA INSTITUIÇÕES FINANCEIRAS EUROPEIAS

O QUE MUDA EM 2027, O QUE ESTÁ EM JOGO E COMO PREPARAR A SUA ORGANIZAÇÃO

CONTENTS

SUMÁRIO EXECUTIVO

Em 10 de julho de 2027, torna-se diretamente aplicável em toda a União Europeia o Regulamento (UE) 2024/1624, o novo Regulamento relativo à Prevenção do Branqueamento de Capitais (AMLR). Importa desde já sublinhar a distinção: o regulamento entrou em vigor em 2024, mas só passa a ser aplicável a partir daquela data. Pela primeira vez, as regras de combate ao branqueamento de capitais deixam de depender de transposição fragmentada por cada Estado-Membro, passando a vigorar de modo uniforme.

O artigo 22.º, n.º 6, alínea b), do AMLR codifica os métodos aceites para a verificação de identidade à distância: os meios de identificação eletrónica conformes com o Regulamento (UE) n.º 910/2014 nos níveis de garantia «substancial» ou «elevado» e os serviços de confiança qualificados pertinentes, designadamente as Assinaturas Eletrónicas Qualificadas (QES) e os Certificados Eletrónicos Qualificados de Atributos (QEAA). Em paralelo, o artigo 5.º-F do eIDAS 2.0 impõe às instituições financeiras a aceitação da EUDI Wallet, a pedido do utilizador, no prazo de 36 meses a contar da entrada em vigor dos respetivos atos de execução, ou seja, até 24 de dezembro de 2027.

No presente *white paper*, analisamos o impacto destas alterações, explicamos o que representam para a diligência devida relativa à clientela (CDD) e apresentamos um roteiro prático de preparação, dirigido aos responsáveis de *compliance*, operações e tecnologia.

1. O PROBLEMA COM O REGIME ATUAL

Consideremos o caso de uma *fintech* portuguesa com ambições de expansão europeia. Hoje, os seus procedimentos de KYC foram desenhados em torno das especificidades da Lei n.º 83/2017, de 18 de agosto. Amanhã, ao abrir operações em Espanha, na Alemanha ou na Polónia, constatará que cada jurisdição transpôs as 4.ª e 5.ª Diretivas em matéria de branqueamento de capitais de forma ligeiramente distinta.

Qual o resultado prático? Regras fragmentadas, custos de *compliance* multiplicados por cada mercado e uma concorrência regulatória que favorece os operadores já estabelecidos, isto é, aqueles com mais recursos para gerir a complexidade jurisdicional.

O CUSTO DA FRAGMENTAÇÃO

Segundo a Europol, a atividade financeira suspeita representa entre 0,7% e 1,2% do PIB anual da União Europeia, ou seja, cerca de 1% (mais de 160 mil milhões de euros por ano) que transita pelo sistema financeiro europeu. Parte substancial deste problema está diretamente ligada à inconsistência na aplicação das regras de CDD entre Estados-Membros. *(Fonte: Europol, From Suspicion to Action: Converting Financial Intelligence into Greater Operational Impact, Financial Intelligence Group, 2017. O valor em euros é uma aproximação derivada da percentagem do PIB.)*

Ora, o AMLR foi concebido precisamente para resolver este problema. Ao substituir uma diretiva por um regulamento de aplicação direta, o legislador europeu elimina a margem de transposição nacional e cria, pela primeira vez, um verdadeiro conjunto único de regras (*single rulebook*) europeu em matéria de prevenção do branqueamento de capitais.

Para as instituições financeiras, tal representa, simultaneamente, um desafio e uma oportunidade: o desafio de adaptar processos já consolidados a uma nova realidade regulatória; e a oportunidade de simplificar as operações transfronteiriças com base num conjunto de regras unificado.

2. O Artigo 22.º do AMLR: Uma Leitura Obrigatória

2.1. O Regime de Verificação de Identidade Remota

O artigo 22.º do AMLR, epigrafado «Identificação e verificação da identidade dos clientes e dos beneficiários efetivos», estabelece os requisitos de diligência devida (CDD) e, em particular, os métodos aceites para a verificação de identidade quando o cliente não se encontra fisicamente presente. A alínea b) do n.º 6 constitui o cerne desta mudança:

> *b) A utilização de meios de identificação eletrónica que cumpram os requisitos estabelecidos no Regulamento (UE) n.º 910/2014 no que respeita aos níveis de garantia "substancial" ou "elevado" e de serviços de confiança qualificados pertinentes, na aceção do mesmo regulamento.*
>
> Artigo 22.º, n.º 6, alínea b), Regulamento (UE) 2024/1624 (AMLR)

Em termos práticos, esta disposição reconhece como conformes os seguintes métodos de verificação de identidade:

- i) os eIDs nacionais notificados ao abrigo do eIDAS, com nível de garantia substancial ou elevado, como sucede com o Cartão de Cidadão e a Chave Móvel Digital portugueses, o DNIe espanhol ou o DigiD neerlandês;
- ii) as EUDI Wallets, as carteiras europeias de identidade digital que cada Estado-Membro deve disponibilizar até 24 de dezembro de 2026;
- iii) os serviços de confiança qualificados (QTS), designadamente as Assinaturas Eletrónicas Qualificadas (QES) e os Certificados Eletrónicos Qualificados de Atributos (QEAA).

2.2. O Peso do Considerando 66

Os considerandos não têm força normativa direta, mas são determinantes na interpretação das disposições. O considerando 66 do AMLR é particularmente revelador sobre a intenção do legislador europeu:

> *A identificação eletrónica prevista no referido regulamento deverá ser tida em conta e aceite pelas entidades obrigadas para o processo de identificação do cliente. A utilização desses meios de identificação pode reduzir, caso existam medidas adequadas de redução dos riscos, o nível de risco para normal ou mesmo baixo. Se um cliente não dispuser dessa identificação eletrónica, por exemplo devido à natureza do seu estatuto de residência num determinado Estado-Membro ou à sua residência num país terceiro, a verificação deverá ser efetuada através de serviços de confiança qualificados pertinentes.*
>
> Considerando 66, Regulamento (UE) 2024/1624 (AMLR)

Esta passagem tem implicações substantivas para a gestão do risco. A utilização de meios de identificação conformes com o eIDAS não é uma mera opção técnica: é um fator de redução de risco reconhecido pelo próprio regulador. Nessa medida, e desde que existam medidas adequadas de mitigação, constitui um elemento relevante da avaliação de risco, suscetível de justificar a classificação do cliente num nível inferior, normal ou mesmo baixo, sem prejuízo de a apreciação continuar a assentar no risco.

Ademais, o mesmo considerando indica a via a seguir quando o cliente não dispõe de identificação eletrónica conforme com o eIDAS, por exemplo devido à natureza do seu estatuto de residência ou por residir num país terceiro: nesses casos, a verificação «deverá ser efetuada através de serviços de confiança qualificados pertinentes». Deste modo, sem prejuízo de os meios de identificação eletrónica constituírem a via primária, o legislador evidencia os serviços de confiança qualificados como mecanismo preferencial de verificação quando o cliente não disponha de um meio de identificação eletrónica adequado, o que assume particular relevância no *onboarding* de clientes de países terceiros. Importa, contudo, ter presente que um considerando não cria, por si, obrigação autónoma e que a alínea a) do n.º 6 do artigo 22.º continua a admitir outros métodos: trata-se, pois, de uma preferência que resulta da interpretação sistemática e não de uma imposição literal do articulado.

3. A Convergência AMLR-eIDAS 2.0: Uma Dupla Obrigação

O AMLR não opera no vácuo. A sua aplicação encontra-se profundamente entrelaçada com o eIDAS 2.0, ou seja, o Regulamento (UE) 2024/1183, que reviu o quadro europeu de identidade digital originalmente estabelecido em 2014. Esta convergência gera uma dupla obrigação regulatória que as instituições financeiras devem compreender na sua totalidade.

Esta convergência não é meramente doutrinária: tem eco expresso no próprio texto do eIDAS 2.0. Com efeito, o considerando 62 do Regulamento (UE) 2024/1183 reconhece que *«a identificação eletrónica segura e o fornecimento de certificados de atributos deverão oferecer flexibilidade e soluções adicionais ao setor dos serviços financeiros, a fim de permitir a identificação de clientes e o intercâmbio de atributos específicos necessários para cumprir, por exemplo, os requisitos do dever de diligência relativo à clientela»* ao abrigo do regulamento que veio a criar a Autoridade para o Combate ao Branqueamento de Capitais (AMLA). Foi, pois, o próprio legislador da identidade digital europeia a apontar a identificação eletrónica e os serviços de confiança como instrumento de cumprimento das obrigações de diligência quanto à clientela.

3.1. O Artigo 5.º-F do eIDAS 2.0 e a EUDI Wallet

Enquanto o AMLR regula o que as entidades obrigadas devem aceitar para efeitos de prevenção do branqueamento, o artigo 5.º-F do eIDAS 2.0, epigrafado «Recurso transfronteiriço às carteiras europeias de identidade digital», vai mais longe. Nos termos do seu n.º 2, os utilizadores privados que estejam obrigados, por força do direito da União ou nacional (ou por obrigação contratual), a utilizar a autenticação forte do utilizador para a identificação em linha, categoria em que se incluem, designadamente, os serviços bancários e financeiros, devem passar a aceitar a EUDI Wallet, a pedido voluntário do utilizador. Excetuam-se as micro e pequenas empresas. O prazo é de 36 meses a contar da entrada em vigor dos atos de execução pertinentes, ocorrida em 24 de dezembro de 2024, o que significa, na prática, até 24 de dezembro de 2027.

OBRIGAÇÃO DE ACEITAÇÃO
O artigo 5.º-F do eIDAS 2.0 não é uma recomendação, mas uma obrigação legal: as instituições financeiras sujeitas a autenticação forte do utilizador terão de aceitar a EUDI Wallet como meio de identificação, a pedido do utilizador, até 24 de dezembro de 2027 (36 meses após a entrada em vigor dos atos de execução). O incumprimento pode originar sanções, tanto ao abrigo do eIDAS como do AMLR.

A EUDI Wallet é uma aplicação móvel que permite ao titular armazenar e apresentar atributos de identidade verificados, desde o documento de identidade nacional até atributos profissionais ou habilitações académicas. Para efeitos de CDD, importa distinguir dois planos. Enquanto meio de identificação eletrónica, a carteira é disponibilizada ao abrigo de um sistema com nível de garantia elevado (artigo 5.º-A, n.º 11, do eIDAS 2.0). Já os Certificados Eletrónicos Qualificados de Atributos (QEAA), enquanto serviços de confiança qualificados, atestam atributos específicos, correspondendo ao nível qualificado (o mais exigente de atestação), e não constituem, em si, um meio de identificação, antes o complementando.

3.2. A ARQUITETURA DOS NÍVEIS DE GARANTIA

Um elemento central deste regime é o conceito de nível de garantia (LoA, do inglês *Level of Assurance*). O eIDAS define três níveis, que determinam a força probatória de uma identificação eletrónica. Importa ter presente que a escala de níveis de garantia respeita, nos termos do artigo 8.º, aos meios de identificação eletrónica; os serviços de confiança qualificados (QES, QEAA), por seu turno, não se inserem nessa escala, produzindo antes os efeitos jurídicos qualificados que o Regulamento lhes confere.

Nível	Características	Relevância AMLR
Baixo	Autodeclaração; autenticação simples por palavra-passe	Não reconhecido para CDD
Substancial	Verificação de identidade com documento físico e autenticação de dois fatores	Aceite para CDD [art. 22.º, n.º 6, al. b)]
Elevado	Requisitos reforçados de verificação e de gestão dos meios de identificação; nível a que é disponibilizada a EUDI Wallet, através da qual se apresentam QES e QEAA	Aceite para CDD; permite redução do risco [art. 22.º, n.º 6, al. b), e cons. 66]

4. CRONOLOGIA: O QUE MUDA E QUANDO

Data	Marco / Obrigação
24 dez. 2026	Disponibilização da EUDI Wallet Cada Estado-Membro deve disponibilizar pelo menos uma EUDI Wallet aos seus cidadãos (art. 5.º-A eIDAS 2.0).
10 jul. 2027	AMLR torna-se aplicável O Regulamento (UE) 2024/1624 passa a ser diretamente aplicável. As entidades obrigadas devem ter procedimentos de CDD conformes, incluindo a aceitação de eIDs notificados e serviços de confiança qualificados.

24 dez. 2027	Aceitação obrigatória da EUDI Wallet Prazo (36 meses após os atos de execução) para as instituições financeiras aceitarem a EUDI Wallet, a pedido do utilizador (art. 5.º-F eIDAS 2.0).

O calendário é exigente, sobretudo para as organizações que ainda não iniciaram a avaliação de impacto. A integração com fornecedores de eID ou QTSP, a adaptação dos sistemas de *onboarding*, a atualização das políticas de risco e a formação das equipas de *compliance* não se concretizam em semanas.

5. Comparação de Métodos de Verificação

O AMLR não elimina os métodos de verificação existentes, mas altera significativamente a sua posição relativa em termos de conformidade, risco e eficiência operacional. Vejamos, na tabela seguinte, uma comparação dos principais métodos disponíveis:

Método	Base Legal	Nível de Garantia	Risco Residual	Redução de Risco
eIDs nacionais notificados	art. 22.º, n.º 6, al. b)	Substancial / Elevado	Médio/Baixo	Sim (com medidas adequadas)
EUDI Wallet (QEAA)	art. 22.º, n.º 6, al. b) + art. 5.º-F eIDAS 2.0	Elevado	Baixo	Sim
QES (assinatura qualificada)	art. 22.º, n.º 6, al. b)	Serviço qualificado	Baixo	Sim
Videoconferência (com docs.)	art. 22.º, n.º 6, al. a)	N/A	Médio	Possível
Documentos físicos e terceiro	art. 22.º, n.º 6, al. a)	N/A	Alto	Maior risco operacional

Nota: as colunas «Risco Residual» e «Redução de Risco» refletem uma apreciação operacional e não uma classificação estabelecida pelo AMLR.

5.1. A Posição Privilegiada dos QTSPs

A leitura conjugada do artigo 22.º, n.º 6, alínea b), com o considerando 66 coloca os prestadores de serviços de confiança qualificados (QTSP) numa posição de particular relevância no novo ecossistema de *compliance* AML. Ao invés das videoconferências, que exigem recursos humanos e não são escaláveis, ou dos documentos físicos, que envolvem intermediários e maior risco de fraude, os QTSP oferecem:

- i) verificação automática e rastreável, com cadeia de confiança criptográfica;
- ii) nível de garantia elevado, reconhecido por todos os Estados-Membros da União;
- iii) compatibilidade nativa com a EUDI Wallet e o ecossistema eIDAS 2.0;
- iv) redução de risco documentada e reconhecida pelo regulador (considerando 66);

- v) escalabilidade para processos de *onboarding* de elevado volume.

Para as organizações com grandes volumes de *onboarding*, como os neobancos, as plataformas de investimento ou as *fintechs* de pagamentos, a automação proporcionada pelos QTSP não é apenas uma vantagem de conformidade: é também um fator relevante de eficiência operacional. Esta centralidade não decorre apenas do AMLR: como vimos, o próprio considerando 62 do eIDAS 2.0 aponta expressamente o fornecimento de certificados de atributos como solução para o setor dos serviços financeiros cumprir o dever de diligência relativo à clientela.

6. Implicações Práticas por Tipo de Entidade

6.1. Bancos e Instituições de Crédito Tradicionais

Os bancos tradicionais enfrentam um desafio de modernização. A maioria dos procedimentos de KYC assenta ainda em processos híbridos, que combinam a videoconferência com a verificação manual de documentos. Trata-se de um modelo funcional, mas dispendioso, lento e de difícil escalabilidade.

O AMLR gera uma pressão regulatória para a digitalização que pode, todavia, ser aproveitada como oportunidade de transformação: substituir os processos manuais por fluxos automatizados assentes em eID e QTSP, reduzindo custos operacionais e, simultaneamente, melhorando a qualidade e a auditabilidade do processo.

6.2. Fintechs

Para as *fintechs*, o AMLR é, a um tempo, um validador e um acelerador. As boas práticas que muitas já adotam, designadamente o *onboarding* integralmente digital e a integração com eIDs, passam agora a constituir o padrão regulatório europeu.

O risco específico deste segmento é a complacência, isto é, assumir que os processos atuais já se encontram conformes sem uma análise cuidada face aos requisitos exatos do AMLR. A questão não reside apenas em saber «se» verificamos digitalmente, mas «como» o fazemos e se o método utilizado atinge o nível de garantia substancial ou elevado exigido.

6.3. Gestoras de Ativos e Fundos de Investimento

As gestoras de ativos apresentam, frequentemente, uma base de clientes mais reduzida, mas de maior complexidade, como sucede com investidores institucionais, *trusts* ou SPV. O AMLR aplica-se, ainda que com nuances: os requisitos de diligência reforçada para clientes de risco elevado não são eliminados, antes sendo complementados pela nova infraestrutura de verificação digital. A integração de QEAA através da EUDI Wallet para a verificação de atributos, como a qualificação do investidor ou o estatuto profissional, pode reduzir significativamente o custo da diligência reforçada, mantendo simultaneamente padrões de conformidade mais elevados.

6.4. Operadores Transfronteiriços

Para as organizações que operam em múltiplos Estados-Membros, o AMLR representa, potencialmente, a mudança mais significativa de sempre no *compliance* AML. A substituição de um mosaico de regimes nacionais de CDD por um conjunto único de regras diretamente aplicável,

dotado de uma infraestrutura de verificação harmonizada através do ecossistema eIDAS, transforma o custo da expansão europeia.

> A OPORTUNIDADE DO MERCADO ÚNICO
> Uma *fintech* que hoje tem de manter equipas de *compliance* especializadas para cada país em que opera pode, com o AMLR e a EUDI Wallet, padronizar o seu processo de *onboarding* para toda a União. Um único fluxo, um único padrão técnico, conformidade em 27 mercados.

7. QUESTÕES FREQUENTES DE COMPLIANCE

Os nossos processos atuais de videoconferência continuam válidos após o AMLR?

Sim. A alínea a) do n.º 6 do artigo 22.º mantém a videoconferência entre os métodos aceitáveis. Não obstante, a alínea b), relativa aos meios conformes com o eIDAS, é apresentada como via alternativa e, à luz do considerando 66, é aquela a que o legislador associa expressamente o efeito de redução do risco. A videoconferência pode continuar a ser utilizada, mas não beneficia, *per si*, desse efeito reconhecido aos meios eIDAS.

O AMLR aplica-se a clientes de países terceiros?

O AMLR aplica-se às entidades obrigadas europeias, independentemente da nacionalidade do cliente. Quanto aos clientes de países terceiros sem eID notificado, o considerando 66 esclarece que a verificação «deverá ser efetuada através de serviços de confiança qualificados pertinentes», ou seja, através de QTSP europeus. Tal confere aos QTSP uma posição ainda mais central no *onboarding* internacional.

Como se articula o AMLR com o RGPD?

A verificação de identidade ao abrigo do AMLR implica o tratamento de dados pessoais. A base de licitude é, em regra, o cumprimento de uma obrigação jurídica (artigo 6.º, n.º 1, alínea c), do RGPD). A utilização de meios conformes com o eIDAS pode, aliás, simplificar a gestão do tratamento e minimizar a retenção de dados, porquanto a verificação pode ser efetuada por referência a atributos certificados, sem transferência dos documentos originais.

O que sucede se não estivermos em conformidade em julho de 2027?

O AMLR atribui poderes de supervisão e sanção às autoridades nacionais competentes, cabendo à nova Autoridade para o Combate ao Branqueamento de Capitais (AMLA), instituída pelo Regulamento (UE) 2024/1620, a coordenação da supervisão transfronteiriça. As sanções podem incluir coimas, restrições operacionais e, nos casos mais graves, a revogação de licenças. A AMLA assumirá ainda poderes de supervisão direta sobre as entidades de maior risco sistémico.

8. CONCLUSÃO: UMA INFRAESTRUTURA, NÃO APENAS UMA OBRIGAÇÃO

O AMLR e o eIDAS 2.0 não representam apenas mudanças regulatórias a gerir. Consubstanciam a construção de uma infraestrutura europeia de identidade digital, com potencial para transformar o modo como as instituições financeiras interagem com os seus clientes.

A obrigação de aceitação da EUDI Wallet, o reconhecimento dos QTSP como via de verificação privilegiada pelo legislador e o efeito de redução do risco associado aos meios eIDAS pelo considerando 66 criam um ecossistema em que a confiança digital passa a ter valor económico e regulatório mensurável.

As organizações que encararem esta transição como uma oportunidade de modernização, e não apenas como um custo de conformidade, estarão mais bem posicionadas para competir no mercado financeiro europeu pós-2027, com processos de *onboarding* mais eficientes, custos de *compliance* mais baixos e uma base tecnológica compatível com a próxima geração de identidade digital europeia.

O momento de agir é agora. As organizações que iniciem, ainda em 2026, o processo de adaptação disporão de tempo para o fazer de forma estratégica; as que o protelem arriscam-se a fazê-lo contra o relógio, à medida que se aproxima 10 de julho de 2027.