AMLR, CDD-RTS, DIdG, GwBG: Geldwäscheprävention ab 2027

WAS SICH BEI DER KUNDENPRÜFUNG IM RAHMEN DER GELDWÄSCHEPRÄVENTION ÄNDERT, WELCHE ROLLE DIE EUDI-WALLET DABEI SPIELEN KANN UND WANN KLASSISCHES VIDEO-IDENT ZULÄSSIG BLEIBT



Executive Summary

Ab dem 10. Juli 2027 gilt die EU-Geldwäscheverordnung (AMLR) unmittelbar; zeitgleich soll in Deutschland ein neues Geldwäschebekämpfungsgesetz (GwBG) das bisherige Geldwäschegesetz (GwG) ablösen. Wie Verpflichtete die Identität ihrer Kunden im Rahmen der AMLR künftig prüfen und Bestandsdaten aktuell halten müssen, konkretisiert der finale Entwurf der entsprechenden technischen Standards der EU-Geldwäschebehörde AMLA (CDD-RTS). In Deutschland passt das Digitale Identitätengesetz (DIdG) das GwG bereits für die Übergangszeit an. Das Update zeigt, wie sich Verpflichtete auf die neuen Vorgaben vorbereiten können, wann klassisches Video-Ident künftig noch infrage kommt und warum gerade Banken und Finanzdienstleister ihre AMLR-Umsetzung strategisch mit der EUDI-Wallet-Integration nach eIDAS 2.0 bündeln sollten.

1. Einleitung und Rechtsrahmen: Von der Richtlinie zur Verordnung

Für Verpflichtete im Sinne der EU-Geldwäscheverordnung[1] (AMLR) rückt der 10. Juli 2027 näher. Bislang setzten die Mitgliedstaaten die Vorgaben zur Kundensorgfalt und zu Know-Your-Customer-Prüfungen (KYC) auf Grundlage der EU-Geldwäscherichtlinien in nationales Recht – in Deutschland das Geldwäschegesetz (GwG) – um. Mit

[1] Verordnung (EU) 2024/1624 des Europäischen Parlaments und des Rates vom 31. Mai 2024 zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung.

der AMLR wechselt der europäische Gesetzgeber das Instrument: Die Anforderungen ergeben sich künftig unmittelbar aus einer EU-Verordnung. Die durch die AMLR erforderlichen Anpassungen des nationalen Rechts werden durch das neue Geldwäschebekämpfungsgesetz (GwBG), zu dem ein Gesetzentwurf[2] bereits vorliegt, vorgenommen. Das GwG wird zum 10. Juli 2027 aufgehoben.

Während die AMLR somit in Zukunft die Grundpfeiler der Kundensorgfalt unmittelbar festlegt – den Anlass für Sorgfaltsmaßnahmen, deren Umfang sowie die Feststellung und Überprüfung der Identität von Kunden und wirtschaftlichen Eigentümern –, bedarf es für die operative Umsetzung konkretisierender technischer Standards. Mit dem Abschlussbericht der Behörde zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung[3] (AMLA) zum Entwurf technischer Regulierungsstandards nach Artikel 28 Absatz 1 AMLR liegt nun das Regelwerk vor, das die Sorgfaltspflichten gegenüber Kunden (Customer Due Diligence, CDD) im Detail ausgestaltet (nachfolgend „CDD-RTS"). Die CDD-RTS präzisieren nicht nur die allgemeinen Anforderungen an Datenerhebung, Datenprüfung und laufende Überwachung, sondern stärkt auch die Rolle digitaler Identitäten in CDD- und KYC-Prozessen erheblich.

Angesichts der regulären Fristen für die Annahme durch die Kommission mittels delegierter Verordnung sowie für etwaige Einwände von Europäischem Parlament und Rat – und da die delegierte Verordnung erst sechs Monate nach ihrem Inkrafttreten gelten soll – werden die CDD-RTS voraussichtlich erst nach dem Geltungsbeginn der AMLR am 10. Juli 2027 förmlich zur Anwendung kommen. Eine vorzeitige Umsetzung durch die Verpflichteten geht mit einem gewissen datenschutzrechtlichen Risiko einher, da es in der Zwischenphase an einer eindeutigen regulatorischen Pflicht fehlt. Dieses Risiko hätte der Gesetzgeber durch einen besser abgestimmten Zeitplan vermeiden können. Angesichts der festen Grundlage im AMLR, die durch die CDD-RTS lediglich konkretisiert wird, erscheint es aber gut vertretbar und mangels alternativer Standards und in Anbetracht der wenigen Zeit, die verbleibt, sogar empfehlenswert, dass Verpflichtete schon jetzt beginnen, ihre Prozesse entsprechend der CDD-RTS anzupassen, um am 10. Juli 2027 startklar zu sein.

Flankiert werden diese Entwicklungen auf nationaler Ebene durch das Digitale Identitätengesetz[4] (DIdG) zur Umsetzung der eIDAS-Verordnung[5], das neben dem neuen Gesetz über die Europäische Brieftasche für die Digitale Identität (EBDIG) bereits vorab gezielte Anpassungen im deutschen Geldwäschegesetz (GwG) und perspektivisch dessen Nachfolgergesetz, dem GwBG, vornimmt, um den Übergang in das neue EU-Regelwerk vorzubereiten.

2. Zwei gleichwertige Regelwege für Identitätsprüfungen: Ausweisdokument oder eIDAS-Lösung

Für die Informationsbeschaffung zur Überprüfung der Identität des Kunden sowie jeder Person, die vorgibt, für den Kunden zu handeln, sieht bereits Artikel 22 Absatz 6 AMLR zwei gleichrangige Regelwege vor:

- **Dokumentenbasiert (lit. a):** anhand eines Personalausweises, Reisepasses oder gleichwertigen Dokuments, oder
- **Elektronisch (lit. b):** mittels elektronischer Identifizierungsmittel mit dem Sicherheitsniveau „substanziell" oder „hoch" nach der eIDAS-Verordnung sowie einschlägiger qualifizierter Vertrauensdienste gemäß dieser Verordnung.

Welche Mittel kommen für den elektronischen Weg nach Artikel 22 Absatz 6 lit. b AMLR konkret in Betracht? Die CDD-RTS erfassen elektronische Identifizierungsmittel im Sinne von Artikel 3 Nr. 2 eIDAS-VO unabhängig davon, ob sie notifiziert sind, solange sie das Sicherheitsniveau

[2] Erreichbar unter https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Downloads/Gesetz/2026/20260715-gesetzentwurf-12-gwb-novelle.pdf.

[3] Erreichbar unter https://www.amla.europa.EU/document/download/e15ab2e5-4074-4de8-bb9d-613dd8b7fdd1_en.

[4] Erreichbar unter https://dip.bundestag.de/vorgang/gesetz-zur-durchf%C3%BChrung-der-unionsrechtlichen-vorschriften-%C3%BCber-die-europ%C3%A4ische-brieftasche/335473.

[5] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

„substanziell“ oder „hoch“ erreichen, sowie einschlägige qualifizierte Vertrauensdienste. Im Einzelnen sind dies insbesondere:

- **Bisherige nationale elektronische Identifizierungsmittel:** etwa die eID, die es zwar bereits seit Ende 2010 gibt (z.B. in der Online-Ausweisfunktion des deutschen Personalausweises), deren Nutzung in den Mitgliedstaaten bislang aber sehr unterschiedlich verbreitet ist;

- **EUDI-Wallet:** Die künftige Europäische Brieftasche für die Digitale Identität erreicht kraft Gesetzes das Sicherheitsniveau „hoch“ und wird von der AMLA in den Erwägungsgründen der CDD-RTS ausdrücklich als Identifizierungsmittel hervorgehoben. In Deutschland nimmt das DIdG diese Öffnung bereits für die Übergangszeit bis zum 10. Juli 2027 vorweg: Durch Artikel 6 DIdG wird die EUDI-Wallet als neues Identifizierungsmittel in § 12 Absatz 1 Satz 1 Nr. 4a GwG n.F. aufgenommen und geregelt, dass zu Dokumentationszwecken die bei der Authentifizierung und Validierung der Personenidentifizierungsdaten anfallenden elektronischen Daten gemäß Artikel 5b Absatz 9 eIDAS-VO aufzuzeichnen sind (§ 8 Absatz 2 Satz 9 GwG n. F.);

- **Qualifizierte Vertrauensdienste:** insbesondere Verfahren auf Grundlage qualifizierter elektronischer Signaturen (QES), qualifizierter Zertifikate oder qualifizierter elektronischer Attributsbescheinigungen (QEAA). Auch hier sorgt das deutsche DIdG für eine praxisrelevante Vorab-Harmonisierung: Es streicht die bisher in § 12 Absatz 1 Satz 3 GwG verankerte Pflicht, beim Einsatz einer QES zusätzlich eine Referenzüberweisung von einem Zahlungskonto des Kunden zu verlangen. Damit antizipiert der deutsche Gesetzgeber die Rechtslage unter der AMLR und den CDD-RTS, die bei einer QES keine Referenzüberweisung mehr fordern.

Artikel 6 Absatz 4 CDD-RTS stellt zudem ausdrücklich klar, dass elektronische Identifizierungsmittel und qualifizierte Vertrauensdienste auch dann zur Identitätsprüfung natürlicher Personen genutzt werden können, wenn der Kunde persönlich anwesend ist. Damit steht fest, dass eIDAS-konforme Lösungen unter der AMLR nicht nachrangig, sondern dem **physischen Ausweisdokument mindestens ebenbürtig** sind. In der Praxis lassen sich solche elektronischen Mittel damit als einheitliches Identifizierungsmedium für alle Vertriebskanäle – digital wie stationär – einsetzen.

3. Video-Ident & Co.: Zwischen Vertrauensdienst und eng begrenzter Ausnahme (Artikel 7 CDD-RTS)

Was bedeutet diese Vorrangstellung eIDAS-konformer Mittel bei der Fernidentifizierung für bestehende Video-Ident-Verfahren? Hier ist künftig nach der regulatorischen Einbettung zu differenzieren: Nach eIDAS zertifizierte Video-Ident-Verfahren können zur Identitätsprüfung nach Artikel 24 Absatz 1a lit. c eIDAS-VO für die Ausstellung qualifizierter Zertifikate oder elektronischer Attributsbescheinigungen (QEAA) dienen und damit mittelbar Teil eines regulären Identifizierungswegs nach Artikel 22 Absatz 6 lit. b AMLR sein.
Isolierte Video-Ident-Verfahren ohne Einbettung in einen qualifizierten Vertrauensdienst – wie viele der heute nach dem GwG und dem BaFin-Rundschreiben 3/2017 (GW) gebräuchlichen Verfahren – werden gemäß Artikel 7 Absatz 1 CDD-RTS dagegen zu einer subsidiären Ausnahme. Im Vergleich zum Konsultationsentwurf hat die AMLA Artikel 7 CDD-RTS deutlich strenger formuliert: Die Wege nach Artikel 22 Absatz 6 AMLR bleiben der strikte Regelfall; alternative Fernidentifizierungslösungen dürfen nur eingesetzt werden, wenn keiner dieser Regelwege genutzt werden kann.
Der Rückgriff auf solche alternativen Lösungen setzt konkret zweierlei voraus:

1. Der natürlichen Person ist es vernünftigerweise nicht zumutbar, ihr Identitätsdokument persönlich vorzulegen, und

2. ihr stehen weder eIDAS-konforme elektronische Identifizierungsmittel noch qualifizierte Vertrauensdienste zur Verfügung.

Liegen beide Voraussetzungen vor, darf die Identität aus der Ferne anhand von Personalausweis, Reisepass oder gleichwertigem Dokument über eine alternative Lösung geprüft werden. Als Auffanglösung muss diese jedoch strenge Mindestanforderungen erfüllen (Artikel 7 Absatz 2 CDD-RTS):

- **Verlässlichkeit:** Einzusetzen sind verlässliche und unabhängige Informationsquellen sowie angemessene Sicherungsmaßnahmen.
- **Inhaberabgleich:** Es muss sichergestellt sein, dass die vorlegende Person tatsächlich Inhaber des Identitätsdokuments ist.
- **Sichere Kommunikation:** Integrität und Vertraulichkeit der Kommunikation sind zu gewährleisten.
- **Datenqualität:** Bild-, Video-, Ton- und sonstige Daten sind lesbar und in einer Qualität zu erfassen, die eine eindeutige Identifizierung zulässt.
- **Abbruch:** Treten technische Mängel oder unerwartete Verbindungsabbrüche auf oder bestehen Zweifel an der Identität oder der Integrität des Verfahrens, ist der Identifizierungsvorgang abzubrechen.
- **Dokumentation:** Die geprüften Informationen und Dokumente müssen gültig und aktuell sein; Kopien sind mit Zeitstempel sicher aufzubewahren und müssen eine nachträgliche Überprüfung ermöglichen.

Vor allem die Anforderung an die Datenqualität und Manipulationssicherheit wird für Verpflichtete zunehmend zur Herausforderung: Generative KI, Deepfakes und Angriffe, bei denen manipulierte Inhalte in den Prüfprozess eingespeist werden, erleichtern Täuschungsversuche erheblich. Die derzeit in Deutschland auf Grundlage des BaFin-Rundschreibens 3/2017 (GW) genutzten Videoidentifizierungsverfahren könnten diesen Maßstäben zwar in weiten Teilen genügen, sollten jedoch insbesondere mit Blick auf aktuelle Anforderungen zur Abwehr dieser Angriffsvektoren im Einzelfall überprüft werden.
Zudem tritt eine **Begründungspflicht** hinzu: Verpflichtete müssen im Einzelfall darlegen und dokumentieren können, weshalb der Kunde nicht über die Regelwege nach Artikel 22 Absatz 6 AMLR überprüft werden konnte, und gegenüber der Aufsicht nachweisen können, dass die eingesetzte Alternativlösung den Anforderungen des Artikels 7 entspricht (Artikel 7 Absatz 3 CDD-RTS). Für die Praxis entsteht dadurch erhebliche Rechtsunsicherheit. Und mit zunehmender Verfügbarkeit und Verbreitung eIDAS-konformer Identifizierungsmittel und qualifizierter Vertrauensdienste dürfte es immer schwieriger werden, den Rückgriff auf ein Alternativverfahren überzeugend zu begründen.

4. Detailvorgaben der CDD-RTS: Datensatz, gleichwertige Dokumente und elektronische Attribute

Ein reibungsloses Onboarding ist für Institute ein Wettbewerbsfaktor. Umso größere Bedeutung kommt den CDD-RTS zu, soweit sie den über natürliche Personen gemäß Artikel 22 Absatz 1 lit. a AMLR zu beschaffenden Datensatz über die AMLR hinaus präzisieren (Artikel 2 bis 5 CDD-RTS):

- **Namen:** Erfasst werden müssen alle Vor- und Nachnamen, wie sie im verwendeten Ausweisdokument oder elektronischen Identifizierungsmittel ausgewiesen sind.
- **Anschrift:** Anzugeben sind das Land – ausgeschrieben oder als Länderkürzel nach ISO 3166 – , Stadt, Gemeinde oder Ortschaft samt Postleitzahl (soweit vergeben) und gegebenenfalls Bundesstaat sowie Straße, Hausnummer, Wohnungs- und Postfachnummer, soweit diese Angaben existieren.
- **Geburtsort:** Mindestens erforderlich ist die Angabe von Land, Bundesstaat oder Stadt, Gemeinde bzw. Ortschaft, so wie sie im

Identitätsdokument oder über das elektronische Identifizierungsmittel ausgewiesen ist.

- **Staatsangehörigkeit:** Verpflichtete haben angemessene Maßnahmen zu ergreifen, um Mehrstaatigkeit zu erkennen.

Die erhobenen Daten sind anschließend zu überprüfen. Erfolgt dies **dokumentenbasiert**, hat dies gemäß Artikel 22 Absatz 6 lit. a AMLR anhand eines Personalausweises, eines Reisepasses oder eines **gleichwertigen Ausweisdokumentes** zu erfolgen. Die CDD-RTS konkretisieren die Bedingungen für eine solche Gleichwertigkeit (Artikel 6 Absatz 1 CDD-RTS). Erforderlich sind:

- **Ausstellung:** durch eine nach geltendem Recht hierfür bestimmte Behörde;
- **Angaben:** Vor- und Nachnamen, Geburtsort und Geburtsdatum des Inhabers sowie Dokumentennummer und Ablaufdatum;
- **Lichtbild und Unterschrift:** ein Gesichtsbild und die Unterschrift des Inhabers;
- **Fälschungssicherheit:** Sicherheitsmerkmale, die die Echtheit des Dokuments gewährleisten.

Für Personen, die aus legitimen Gründen – etwa wegen Staatenlosigkeit oder eines Flüchtlings- oder subsidiären Schutzstatus – kein solches Dokument vorlegen können, genügen Dokumente mit Namen, Geburtsdatum und Gesichtsbild; fehlende Angaben sind dann über andere verlässliche und unabhängige Quellen zu beschaffen (Artikel 6 Absatz 2 CDD-RTS).
Erfolgt die Überprüfung **elektronisch** nach Artikel 22 Absatz 6 lit. b AMLR, legt Anhang I der CDD-RTS fest, welche Attribute elektronische Identifizierungsmittel oder qualifizierte Vertrauensdienste hierfür bereitstellen müssen; die Attribute orientieren sich dabei an den Personenidentifizierungsdaten der EUDI-Wallet nach der eIDAS-Durchführungsverordnung (EU) 2024/2977 (Artikel 27 Absatz 1 CDD-RTS). Übermittelt die eingesetzte eIDAS-Lösung die erforderlichen Attribute vollständig, gelten diese Attribute bereits als verifiziert und müssen nach Klarstellung der AMLA nicht nochmals anhand anderer Quellen überprüft werden. Da der eIDAS-Datensatz bestimmte Angaben je nach Mitgliedstaat oder eingesetztem Mittel jedoch nur als optionale Attribute vorsieht, gilt: Soweit einzelne nach der AMLR und den CDD-RTS erforderliche Attribute in der konkret genutzten eIDAS-Lösung nicht enthalten sind, müssen diese fehlenden Angaben ergänzend auf anderem Weg erhoben und verifiziert werden (Artikel 27 Absatz 2 CDD-RTS).

5. Kundensorgfalt als Daueraufgabe: Laufende Überwachung und Bestandskunden

Mit dem Onboarding ist die Kundensorgfalt keineswegs abgeschlossen. Operativ besonders ins Gewicht fallen dürften die Pflichten zur laufenden Überwachung der Geschäftsbeziehung (Artikel 26 AMLR):

- **Turnusmäßige Aktualisierung:** Kundeninformationen sind bei allen Kunden spätestens alle fünf Jahre zu aktualisieren, bei Kunden mit höherem Risiko spätestens jährlich.
- **Anlassbezogene Überprüfung:** Auch zwischen diesen Terminen können bestimmte Anlässe eine Überprüfung erforderlich machen.
- **Screening:** Ob Kunden oder wirtschaftliche Eigentümer politisch exponierte Personen (PEP) sind oder geworden sind, ist risikoorientiert und unverzüglich bei neuen Informationen oder Aktualisierungen der Liste wichtiger öffentlicher Ämter zu prüfen. Der Abgleich mit Finanzsanktionslisten ist bei Begründung der Geschäftsbeziehung, bei Änderungen der Listen oder der Kundendaten sowie regelmäßig zu wiederholen. Zulässig sind automatisierte Tools, manuelle Prüfungen oder eine Kombination.

Auch in diesem Zusammenhang können digitale Identitäten unterstützen, über die Kunden aktualisierte und verifizierte Daten im Rahmen des **KYC-Refreshs** ohne Medienbruch übermitteln können.

Spielraum bei den Fristen besteht nicht: Die AMLA hat Forderungen nach längeren Aktualisierungszyklen ausdrücklich zurückgewiesen. Die Höchstfristen von einem bzw. fünf Jahren folgen unmittelbar aus Artikel 26 Absatz 2 AMLR und lassen sich durch die RTS weder verändern noch verlängern. Überwachungs- und Aktualisierungsprozesse müssen daher vollständig an diesen Fristen ausgerichtet sein.
Zudem ist der **Altkundenbestand** nachzuziehen: Für Geschäftsbeziehungen, die vor dem Inkrafttreten der delegierten Verordnung, welche die CDD-RTS übernimmt, begründet wurden, sind Dokumente, Daten und Informationen risikoorientiert und innerhalb der genannten Höchstfristen an die Anforderungen von AMLR und CDD-RTS anzupassen (Artikel 28 CDD-RTS). Für den diesen Kundenbestand, sollen laut Erwägungsgrund 26 diese Fristen jedoch erst mit dem Inkrafttreten der delegierten Verordnung zu laufen beginnen.

6. Exkurs für eIDAS-Relying Parties: Strategische Bündelung von AMLR-Umsetzung, DIdG und EUDI-Wallet

Während die CDD-RTS technologieneutral alle eIDAS-konformen Identifizierungsmittel und qualifizierten Vertrauensdienste erfassen, lohnt sich insbesondere für Unternehmen des Finanzsektors ein genauerer Blick auf die künftige **EUDI-Wallet** (siehe dazu auch unser GSK Update vom Juli 2026). Denn sie bildet nicht nur das Referenzmodell für den Attributekatalog der CDD-RTS, sondern ihre breite Marktdurchdringung wird – anders als bei bisherigen nationalen eID-Lösungen – durch den Rechtsrahmen der revidierten eIDAS-Verordnung (eIDAS 2.0) und das deutsche Digitale Identitätengesetz (DIdG) regulatorisch flankiert:

- Jeder Mitgliedstaat muss bis zum **24. Dezember 2026** mindestens eine EUDI-Wallet bereitstellen. Mit dem als Artikel 1 des DIdG geschaffenen EBDIG hat der deutsche Gesetzgeber nun die nationalen Grundlagen und Zuständigkeiten – unter Federführung des Bundesministeriums für Digitales und Staatsmodernisierung (BMDS) sowie mit der Bundesnetzagentur als Aufsichtsbehörde – festgelegt; die staatliche deutsche EUDI-Wallet **„d-you“** soll am **2. Januar 2027** starten und schrittweise (u. a. um elektronische Attributsbescheinigungen und QES) ausgebaut werden.
- Öffentliche Stellen, die für den Zugang zu einem Online-Dienst eine elektronische Identifizierung verlangen, müssen EUDI-Wallets hierfür auf Wunsch des Nutzers akzeptieren (Artikel 5f Absatz 1 eIDAS-VO). Anbieter sehr großer Online-Plattformen (VLOPs) im Sinne des Digital Services Act[6] sind **ab Bereitstellung** der ersten EUDI-Wallet ebenfalls verpflichtet, die EUDI-Wallet bei bestimmten Vorgängen als Authentifizierungsmedium für ihre Nutzer zu akzeptieren (Artikel 5f Absatz 3 eIDAS-VO).
- Ab dem **24. Dezember 2027** sind zudem bestimmte private Unternehmen (mit Ausnahme von Kleinst- und Kleinunternehmen) – darunter insbesondere **Banken und Finanzdienstleister** – als sogenannte **Relying Parties** („vertrauende Beteiligte“) verpflichtet, die EUDI-Wallet auf freiwilliges Verlangen des Nutzers zu akzeptieren, soweit sie gesetzlich oder vertraglich zur starken Nutzerauthentifizierung bei der Online-Identifizierung verpflichtet sind (Artikel 5f Absatz 2 eIDAS-VO). Diese Pflichten dürften die Nutzung digitaler Identitäten spürbar beschleunigen und die Erwartung der Kunden prägen, sich auch bei ihrem Institut per Wallet ausweisen zu können.

Für Unternehmen, die zugleich AMLR-Verpflichtete und zur Akzeptanz verpflichtete Relying Parties nach Artikel 5f Absatz 2 eIDAS-VO sind, erscheint es ratsam, die enge zeitliche Taktung des Jahres 2027 strategisch zu nutzen: Zwischen dem Start der deutschen EUDI-Wallet samt Öffnung des § 12 Absatz 1 Nr. 4a GwG durch das DIdG (Anfang Januar 2027), dem Geltungsbeginn der AMLR (10. Juli 2027, kurz darauf gefolgt von den CDD-RTS) und dem

[6] Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste).

Greifen der Wallet-Akzeptanzpflicht im Finanzsektor (24. Dezember 2027) liegen jeweils nur wenige Monate. Statt diese Vorgaben getrennt zu betrachten, bietet es sich an, die Integration der EUDI-Wallet gezielt auf den Juli 2027 (oder im Rahmen der neuen GwG-Öffnung sogar noch früher) vorzuziehen und mit der AMLR-Implementierung in einem gemeinsamen Projekt zu bündeln. Dabei sollten Institute beachten, dass sich Relying Parties vor der ersten Wallet-Interaktion gemäß §§ 2 Absatz 2 Satz 1 Nr. 2 lit. b, 10 EBDIG i. V. m. Artikel 5b Absatz 1 bis 3 eIDAS-VO beim **Bundesverwaltungsamt** als zuständiger nationaler Registrierungsstelle registrieren müssen, um die erforderlichen Berechtigungszertifikate zu erhalten. Da bei der Registrierung die anzufragenden Daten konkret zu benennen und zu begründen sind und nur diese registrierten Attribute abgefragt werden dürfen, sollte der Registrierungsumfang beim Bundesverwaltungsamt frühzeitig mit den Vorgaben der AMLR und Anhang I der CDD-RTS abgeglichen werden.
Auch wenn die Nutzung der EUDI-Wallet für die Kunden freiwillig bleibt und nicht zu erwarten ist, dass am 10. Juli 2027 bereits sämtliche Kunden mit einer EUDI-Wallet ausgestattet sein werden, und daher bis auf Weiteres auch alternative Identifizierungsmöglichkeiten unterstützt werden müssen, überwiegen die Vorteile einer solch synchronisierten Umsetzung deutlich: Da die CDD-RTS eIDAS-konforme Verfahren ohnehin als neuen Standardweg für die Fernidentifizierung festschreiben, vermeiden Institute durch die frühzeitige Bündelung nicht nur doppelte IT-Projektaufwände innerhalb von fünf Monaten, sondern schaffen bereits ab dem ersten Tag eine rechtssichere Zielarchitektur nach Artikel 22 Absatz 6 lit. b AMLR, die mit steigender Wallet-Verbreitung den aufwendigen Begründungs- und Dokumentationsaufwand nachrangiger Ausnahmelösungen nach Artikel 7 CDD-RTS sukzessive reduziert.

7. Fazit und Ausblick

Die CDD-RTS konkretisieren die Vorgaben der AMLR für das Onboarding und die laufende Kundensorgfalt und setzen – im Zusammenspiel mit dem deutschen DIdG – bei der Fernidentifizierung einen klaren Akzent: eIDAS-konforme Lösungen wie nationale eIDs, qualifizierte Vertrauensdienste und die künftige EUDI-Wallet werden zum Regelweg der digitalen Kundenidentifizierung, klassisches Video-Ident und vergleichbare Verfahren zur begründungsbedürftigen Ausnahme. Für die Umsetzung bis Juli 2027 empfehlen sich insbesondere folgende Schritte:

- **Gap-Analyse:** Abgleich der bestehenden Onboarding- und KYC-Prozesse mit den präzisierten Daten- und Dokumentenanforderungen der CDD-RTS sowie Prüfung der durch das DIdG geschaffenen Erleichterungen im GwG (insbesondere Wegfall der Referenzüberweisung bei QES und Protokollierung der Validierungsdaten nach § 8 Absatz 2 Satz 9 GwG n. F.);

- **Fernidentifizierung und eIDAS-Strategie:** Überprüfung bestehender Video-Ident- und sonstiger Fernidentifizierungsverfahren und, wo möglich, Überführung in einen qualifizierten Vertrauensdienst, sowie Ausbau weiterer eIDAS-konformer Identifizierungswege, und, soweit erforderlich, Ausnahmelösungen nach Artikel 7 CDD-RTS erfassen und Prozesse zur Einzelfallbegründung aufsetzen;

- **Bündelung mit der EUDI-Wallet (für verpflichtete Relying Parties):** Planung einer vorgezogenen Anbindung der EUDI-Wallet bis spätestens zum 10. Juli 2027 einschließlich der Registrierung als vertrauender Beteiligter beim Bundesverwaltungsamt mit einem auf Anhang I der CDD-RTS abgestimmten Datenumfang;

- **Datenschutz:** Anpassung der Datenschutz-Governance, insbesondere der Datenschutzhinweise, sowie Prüfung, ob eine Datenschutz-Folgenabschätzung erforderlich ist, Überprüfung der Verträge mit sogenannten „eIDAS-Vermittlern“;

- **Laufende Überwachung und Bestandskunden:** Ausrichtung der Überwachungs- und Screening-Prozesse an den gesetzlichen Höchstfristen (ein bzw. fünf Jahre) und Aufsetzen eines

risikoorientierten Plans zur Anpassung des Kundenbestands nach Artikel 28 CDD-RTS.

Wer sich frühzeitig mit den CDD-RTS und den Neuerungen des DIdG befasst, stellt nicht nur die fristgerechte Compliance zum Juli 2027 sicher, sondern kann die neuen regulatorischen Leitplanken gezielt nutzen, um seine Onboarding- und KYC-Prozesse im Neukunden- wie im Bestandsgeschäft medienbruchfrei und effizient neu aufzustellen.

Haben Sie Fragen? Unsere Anwältinnen und Anwälte stehen Ihnen gern zur Verfügung.

Per Meyerdierks
Rechtsanwalt
Standort Hamburg
per.meyerdierks@gsk.de

Dr. Harald Feiler
Rechtsanwalt
Standort Frankfurt am Main
harald.feiler@gsk.de

Haftungsausschluss
Diese Mandanteninformation enthält ausschließlich allgemeine Informationen, die nicht geeignet sind, den besonderen Umständen eines Einzelfalles gerecht zu werden. Sie stellt keine Beratung, Auskunft oder ein rechtsverbindliches Angebot auf Beratung oder Auskunft dar und ist auch nicht geeignet, eine persönliche Beratung zu ersetzen. GSK Stockmann – Alle Rechte vorbehalten.

GSK
STOCKMANN

Urheberrecht

GSK Stockmann – Alle Rechte vorbehalten. Die Wiedergabe, Vervielfältigung, Verbreitung und/oder Bearbeitung sämtlicher Inhalte und Darstellungen des Beitrages sowie jegliche sonstige Nutzung ist nur mit vorheriger schriftlicher Zustimmung von GSK Stockmann gestattet.

Haftungsausschluss

Diese Mandanteninformation enthält ausschließlich allgemeine Informationen, die nicht geeignet sind, den besonderen Umständen eines Einzelfalles gerecht zu werden. Sie hat nicht den Sinn, Grundlage für wirtschaftliche oder sonstige Entscheidungen jedweder Art zu sein. Sie stellt keine Beratung, Auskunft oder ein rechtsverbindliches Angebot auf Beratung oder Auskunft dar und ist auch nicht geeignet, eine persönliche Beratung zu ersetzen. Sollte jemand Entscheidungen jedweder Art auf Inhalte dieser Mandanteninformation oder Teile davon stützen, handelt dieser ausschließlich auf eigenes Risiko.

GSK Stockmann und auch die in dieser Mandanteninformation namentlich genannten Partner oder Mitarbeiter übernehmen keinerlei Garantie oder Gewährleistung, noch haftet GSK Stockmann und einzelne Partner oder Mitarbeiter in irgendeiner anderen Weise für den Inhalt dieser Mandanteninformation. Aus diesem Grund empfehlen wir, in jedem Fall eine persönliche Beratung einzuholen.

www.gsk.de

YOUR PERSPECTIVE.
GSK.DE | GSK-LUX.COM

GSK Stockmann
Rechtsanwälte Steuerberater Partnerschaftsgesellschaft mbB

BERLIN
Anton-Wilhelm-Amo-Str. 42
10117 Berlin
T +49 30 203907 - 0
F +49 30 203907 - 44
berlin@gsk.de

HEIDELBERG
Europaplatz 3
69115 Heidelberg
T +49 6221 4566 - 0
F +49 6221 4566 - 44
heidelberg@gsk.de

FRANKFURT/M.
Bockenheimer Landstr. 24
60323 Frankfurt am Main
T +49 69 710003 - 0
F +49 69 710003 - 144
frankfurt@gsk.de

MÜNCHEN
Karl-Scharnagl-Ring 8
80539 München
T +49 89 288174 - 0
F +49 89 288174 - 44
muenchen@gsk.de

HAMBURG
Neuer Wall 69
20354 Hamburg
T +49 40 369703-0
F +49 40 369703-44
hamburg@gsk.de

LUXEMBURG
GSK Stockmann SA
44, Avenue John F. Kennedy
L - 1855 Luxemburg
T +352 271802 - 00
F +352 271802 - 11
luxembourg@gsk-lux.com

LONDON
GSK Stockmann International
Rechtsanwaltsgesellschaft mbH,
Zweigniederlassung London
Queens House, 8-9 Queen Street
London EC4N 1SP
United Kingdom
T +44 20 4512687-0
london@gsk-uk.com

Sitz der GmbH: München,
Amtsgericht München
HRB 281930
Geschäftsführer:
Dr. Mark Butt, York-Alexander
von Massenbach