BetterCo

FACHDOKUMENT · RECHTSSTAND AUGUST 2026

Von KYC zu ReKYC

Die EU-Geldwäscheverordnung ab dem 10. Juli 2027 — was sich gegenüber dem Geldwäschegesetz ändert, Schritt für Schritt

Was	Für wen	Wann starten
EU-Geldwäscheverordnung 2027	**jede neue und jede bestehende KYC-Akte**	**je eher desto einfacher**

Fachliche Information, keine Rechtsberatung im Einzelfall.
Aussagen, die auf noch nicht angenommenen Rechtsakten beruhen, sind im Dokument gekennzeichnet.

Founders1
www.betterco.ai

Über dieses Dokument

GEGENSTAND, AUFBAU UND LEITGEDANKE

Gegenstand

Die EU-Geldwäscheverordnung löst die bisherigen deutschen Regeln zu den Sorgfaltspflichten weitgehend ab: Sie gilt unmittelbar, ohne deutsches Umsetzungsgesetz, und regelt die KYC-Prüfung deutlich detaillierter als das Geldwäschegesetz. Dieses Dokument vergleicht beide Regime **Prüfschritt für Prüfschritt** und beantwortet je Prüfschritt drei Fragen: Was gilt heute? Was gilt ab dem 10. Juli 2027? Und ist der Unterschied wirklich neu, dieselbe Pflicht in größerer Tiefe — oder nur eine andere Formulierung?

Alle Aussagen zur AMLR sind am Verordnungstext geprüft. Ein Teil der Detailregeln steht allerdings nicht in der Verordnung selbst: Sie überlässt ihn **technischen Regulierungsstandards**, im EU-Sprachgebrauch **RTS** (*regulatory technical standards*). Das ist Recht der zweiten Ebene, ähnlich wie eine Rechtsverordnung zu einem Gesetz. Die Geldwäschebehörde AMLA entwirft sie, die Europäische Kommission setzt sie in Kraft. Danach gelten sie unmittelbar wie die Verordnung selbst. Bis dahin sind sie Entwurf. Aussagen, die darauf beruhen, sind in diesem Dokument **gelb markiert**. Bußgeldhöhen werden nicht genannt — die Verordnung enthält keine.

Für den Kundenbestand verlangt die Verordnung, die Daten jeder Geschäftsbeziehung aktuell zu halten; sie nennt diese Pflicht **Aktualisierung** (Art. 26 Abs. 2). In der Praxis heißt der Vorgang **ReKYC**: Die bestehende **KYC-Akte** wird erneut geprüft und auf den geforderten Stand gebracht. Die KYC-Akte ist dabei die dokumentierte Prüfung einer Geschäftsbeziehung — Stammdaten, wirtschaftlich Berechtigte, Screenings, Nachweise und Fristen. Dieses Dokument verwendet beide Begriffe: den Rechtsbegriff, wo es um die Vorschrift geht, ReKYC und KYC-Akte, wo es um die Durchführung geht.

Der Aufbau

Das Dokument folgt dem Ablauf einer KYC-Prüfung — von der Frage, wer die Regeln überhaupt anwenden muss, bis zu den Pflichten, die nicht die einzelne Prüfung betreffen, sondern die Organisation.

Kapitel 1 vergleicht den Kreis der Verpflichteten heute und ab 2027. Für Notariat, Rechtsberatung und Steuerberatung entscheidet dabei weiterhin das einzelne Kataloggeschäft darüber, ob die Pflichten greifen — und nicht das Unternehmen als solches.

Kapitel 2 enthält den vollständigen Vergleich in einer Tabelle. Für jeden Prüfschritt ist aufgeführt, was im Kern gleich bleibt und was sich ändert. Die neun Prüfschritte werden anschließend in den Unterkapiteln 2.1 bis 2.9 ausgeführt, die jeweils mit ihrer eigenen Detailtabelle beginnen.

KAP.	PRÜFSCHRITT	WORUM ES GEHT
2.1	**Auslöser und Kundenbegriff**	Wann eine Prüfung überhaupt beginnt: die Schwellenwerte, die neue Bargeldobergrenze — und die Regel, nach der bei vermittelten Geschäften beide Parteien Kunde sind.
2.2	**Identifizierung des Kunden**	Welche Daten Pflicht werden, welche zwei Wege der Überprüfung die Verordnung zur Wahl stellt, bis wann verifiziert sein muss und was die Selbstauskunft künftig noch trägt.
2.3	**Wirtschaftlich Berechtigte**	Wie Beteiligungen über alle Ebenen zu rechnen sind, wer als fiktiver Berechtigter gilt — und welche Fristen der Abgleich mit dem Register auslöst.
2.4	**Zweck und Geschäftstätigkeit**	Die fünf Angaben, die jede Geschäftsbeziehung künftig beschreiben müssen, und warum sie die Grundlage der späteren Überwachung sind.
2.5	**Screening**	Wie sich der Kreis der politisch exponierten Personen erweitert, warum die Sanktionsprüfung erstmals eine Sorgfaltspflicht wird und welche Grenzen für Medienrecherchen gelten.
2.6	**Risikoeinstufung, vereinfachte und verstärkte Sorgfalt**	Woran sich die Prüftiefe bemessen muss, was vereinfachte Sorgfalt noch erlaubt und in welchen Fällen verstärkte Prüfung ohne Ermessen Pflicht ist.

KAP.	PRÜFSCHRITT	WORUM ES GEHT
2.7	**Laufende Überwachung und Aktualisierung**	Die Aktualisierungs-Fristen von einem und fünf Jahren, warum fünf Jahre eine Obergrenze und kein Zielwert sind — und wie der Kundenbestand nachgezogen wird.
2.8	**Dokumentation, Abbruch und Meldewesen**	Was wie lange aufzubewahren und wann zu löschen ist, warum auch Ablehnungen dokumentiert werden müssen und wie weit die Auskunftspflicht reicht.
2.9	**Organisatorische Pflichten**	Was die Verordnung jenseits der einzelnen Prüfung verlangt: Risikoanalyse, zwei Compliance-Funktionen, Schulung und Auslagerung.

Kapitel 3 weist aus, was noch nicht feststeht. Ein erheblicher Teil der Detailregeln liegt in Rechtsakten, die noch nicht angenommen sind. Das Kapitel nennt deren Stand offen, damit Entwurf und geltendes Recht nicht verwechselt werden, und führt die Termine auf, zu denen mit den nächsten Konkretisierungen zu rechnen ist. Am Ende grenzt es die Geldwäscheverordnung gegen das Recht der elektronischen Identität ab, weil beide Stränge in der Diskussion häufig vermengt werden.

Kapitel 4 nimmt die Gliederung aus Kapitel 2 noch einmal auf, diesmal aus der Umsetzungsperspektive. Für jeden Prüfschritt ist getrennt aufgeführt, was ein Prozess ohnehin leisten muss und was ab 2027 hinzukommt. Nur der zweite Teil verursacht Umstellungsaufwand.

Kapitel 5 führt die Einzeländerungen zusammen. Es zeigt, was sie gemeinsam für den Aufwand je Prüfung bedeuten — und weshalb sie Neukunden sofort treffen, den Kundenbestand dagegen mit Verzögerung.

Kapitel 6 beschreibt das ReKYC-Vorgehen für den Kundenbestand in fünf Phasen. Sie beginnen mit der Analyse und nicht mit dem Prüfen, weil nicht jede KYC-Akte dieselbe Prüftiefe benötigt.

Der Leitgedanke

AMLR 2027 betrifft Neu- und Bestandskunden. Jetzt starten. Aber auf zwei verschiedenen Wegen.

Ab dem 10. Juli 2027 wird jede KYC-Prüfung aufwändiger: mehr Daten, mehr Personen, mehr Nachweise. Für **Neukunden** gibt es keine Übergangsfrist. Im **Kundenbestand** bekommt jede **KYC-Akte** ein **Fälligkeitsdatum** — ein Jahr bei hohem Risiko, maximal bis zu fünf Jahren bei niedrigem Risiko. Wie tief geprüft wird, bestimmt das Risiko. Wieviel Aufwand mit der Prüfung verbunden ist, entscheidet die vorhandene Datenqualität. Ein **intelligenter, abgestufter ReKYC-Prozess** berücksichtigt das und optimiert Kosten und Aufwand. **Kapitel 5 begründet das, Kapitel 6 beschreibt das ReKYC-Vorgehen.**

1 Wer verpflichtet ist — und was sich am Kreis der Verpflichteten ändert

WER DIE REGELN ANWENDEN MUSS

Der Kreis der Verpflichteten bleibt in seinem Kern derselbe, wird aber an mehreren Stellen erweitert und EU-weit vereinheitlicht. Bisher regelte ihn deutsches Recht (§ 2 GwG); künftig ergibt er sich unmittelbar aus der Verordnung (Art. 3).

GRUPPE	HEUTE (GWG)	AB 10.07.2027 (AMLR)
Kredit- und Finanzinstitute	verpflichtet	unverändert verpflichtet (Art. 3 Nr. 1, 2)
Steuerberatung und Prüfung	verpflichtet	verpflichtet, wenn Hilfe oder Beratung in Steuerangelegenheiten **Haupttätigkeit** ist — auch mittelbar über verbundene Personen (Nr. 3 lit. a)
Notariat und Rechtsberatung	verpflichtet bei Katalogtätigkeiten	verpflichtet bei Katalogtätigkeiten — der Katalog nennt nun ausdrücklich auch **Kryptowerte** (Nr. 3 lit. b)

GRUPPE	HEUTE (GWG)	AB 10.07.2027 (AMLR)
Immobilienvermittlung	verpflichtet	verpflichtet, ausdrücklich auch bei **Vermietung ab 10.000 € Monatsmiete** (lit. d)
Güterhandel	Güterhändler, Edelmetalle	Edelmetalle und -steine, hochwertige Güter, **Kulturgüter ab 10.000 €** — einschließlich Handel in **Freizonen und Zolllagern** (lit. e, f, i, j)
Neu hinzugekommen	—	**Crowdfunding-Dienstleister und -Vermittler**, **Kreditvermittler** für Immobiliar- und Verbraucherkredite, **Anbieter von Aufenthaltsrechten gegen Investition**, **gemischte Holdinggesellschaften** ohne Finanztätigkeit, **Fußballagenten und Profifußballvereine** (lit. h, k, l, m, n, o)

Rechtsberatende Berufe: das Kataloggeschäft entscheidet

Notarinnen und Notare, Rechtsanwältinnen und Rechtsanwälte sowie andere unabhängige Angehörige rechtsberatender Berufe sind **nicht durchgängig** verpflichtet, sondern nur, wenn sie im Namen und für Rechnung des Kunden an einer Finanz- oder Immobilientransaktion mitwirken oder bei der Planung oder Durchführung folgender Geschäfte helfen (Art. 3 Nr. 3 lit. b):

- Kauf und Verkauf von Immobilien oder von Unternehmen
- Verwaltung von Geld, Wertpapieren oder sonstigen Vermögenswerten des Kunden — **einschließlich Kryptowerten**
- Eröffnung oder Verwaltung von Bank-, Spar-, Wertpapier- oder **Kryptowerte-Konten**
- Beschaffung der zur Gründung, zum Betrieb oder zur Verwaltung von Gesellschaften erforderlichen Mittel
- Gründung, Betrieb oder Verwaltung von Trusts, Gesellschaften, Stiftungen oder ähnlichen Strukturen

> **Was daran neu ist**
>
> Die Systematik entspricht der heutigen Rechtslage — die Verpflichtung knüpft weiterhin an das einzelne Geschäft an, nicht an das Unternehmen als solches. Neu ist die ausdrückliche Erstreckung auf **Kryptowerte** in zwei Katalogpunkten. Wer Geschäfte mit digitalen Vermögenswerten begleitet, fällt damit klarer in den Anwendungsbereich als bisher.

Die Verordnung erkennt die Besonderheit der rechtsberatenden Tätigkeit an mehreren Stellen an: bei der Beendigungspflicht (Art. 21 Abs. 2), bei der Unstimmigkeitsmeldung (Art. 24 Abs. 4) und bei der Verdachtsmeldung (Art. 70 Abs. 2). Die Ausnahmen gelten jeweils für Informationen aus der **Beurteilung der Rechtslage** sowie aus der Verteidigung und Vertretung in Verfahren — und sie entfallen bei Beteiligung an Geldwäsche oder Kenntnis entsprechender Zwecke.

2 Die Übersicht: was sich je Prüfschritt ändert

ALLE PRÜFSCHRITTE AUF EINEN BLICK

Die folgende Tabelle zeigt für jeden Prüfschritt, was im Kern gleich bleibt und was die Verordnung ändert. Die Nummer in der ersten Spalte ist zugleich die Kapitelnummer: Die neun Prüfschritte werden in den Unterkapiteln 2.1 bis 2.9 ausgeführt, jeweils beginnend mit ihrer Detailtabelle.

KAP.	GEGENSTAND	WAS IM KERN GLEICH BLEIBT	WAS SICH ÄNDERT
1	**Wer verpflichtet ist**	Die Pflicht knüpft an die Tätigkeit und an das einzelne Geschäft an	Kreis erweitert um Crowdfunding, Kreditvermittler, Investitionsaufenthalte und Fußball; **Kryptowerte ausdrücklich im Kataloggeschäft**
2.1	**Auslöser und Kundenbegriff**	Schwellenwerte lösen die Prüfung aus; Kunde ist der Auftraggeber	EU-Bargeldobergrenze und Identifizierung ab 3.000 €; bei vermittelten Geschäften **zwei Kunden statt einem**
2.2	**Identifizierung des Kunden**	Ausweisdaten erheben, prüfen und dokumentieren	fester EU-Datensatz mit mehr Feldern; eID und qualifizierte Vertrauensdienste EU-weit anerkannt; Verifizierung grundsätzlich **vor** Beginn; Selbstauskunft genügt nicht mehr allein

KAP.	GEGENSTAND	WAS IM KERN GLEICH BLEIBT	WAS SICH ÄNDERT
2.3	**Wirtschaftlich Berechtigte**	ab einer Beteiligungsschwelle ermitteln und dokumentieren	Schwelle „ab 25 %“; **jede Ebene durchrechnen**; alle Berechtigten verifizieren; fiktive Berechtigte = ganze Geschäftsleitung; Registernachweis; 14-Tage-Frist bei Abweichung
2.4	**Zweck und Geschäftstätigkeit**	Zweck der Geschäftsbeziehung erfassen	**fünf Pflichtangaben statt Freitext** — darunter Herkunft und Verwendung der Mittel bei jeder Beziehung
2.5	**Screening**	politisch exponierte Personen und Sanktionen prüfen	PEP-Kreis größer, EU-Liste der Ämter; Sanktionsprüfung wird **eigene Sorgfaltspflicht** und reicht durch die Beteiligungskette; Reputation als verbindliche Risikovariable
2.6	**Risikoeinstufung und Prüftiefe**	risikobasiert arbeiten, Prüftiefe abstufen	Einstufung an vorgegebene Faktoren gebunden und jederzeit nachweispflichtig; verstärkte Prüfung in bestimmten Fällen **immer** Pflicht
2.7	**Überwachung und Aktualisierung**	laufend überwachen, Daten aktuell halten	feste Aktualisierungs-Fristen; **jede Geschäftsbeziehung bekommt ein Fälligkeitsdatum**
2.8	**Dokumentation und Meldewesen**	Unterlagen aufbewahren, Verdacht melden, Auskunft geben	ungeschwärzt und einschließlich eID-Daten; **auch Ablehnungen** dokumentieren; Löschpflicht nach Fristablauf; Auskunft über fünf Jahre auch zu beendeten Beziehungen
2.9	**Organisatorische Pflichten**	Risikoanalyse, Beauftragter, Schulung	sechs verbindliche Eingangsgrößen für die Risikoanalyse; **zwei Compliance-Funktionen** mit Verankerung im Leitungsorgan; Schutz- und Berichtspflichten

Das Muster hinter der Tabelle

Bei keinem Prüfschritt entsteht eine völlig neue Pflicht. Was sich ändert, folgt drei Mustern: Die Prüfung wird **aufwändiger** — mehr Datenfelder, mehr zu prüfende Personen. Sie wird **verbindlich** — aus Ermessen wird Pflicht, aus „angemessen“ wird eine Frist. Und sie wird **nachweispflichtig** — die Aufsicht kann jede Entscheidung einzeln abfragen.

2.1 Auslöser und Kundenbegriff

WANN GEPRÜFT WIRD UND WER ZU PRÜFEN IST

GEGENSTAND	HEUTE (GWG)	AB 10.07.2027 (AMLR)
Auslöser und Schwellen	keine generelle Bargeldobergrenze in Deutschland	EU-Obergrenze **10.000 €** für Waren und Dienstleistungen; Identifizierung bereits ab **3.000 €** Bartransaktion
Kundenbegriff	der Auftraggeber	bei vermittelten Transaktionen **beide Parteien**, wenn nur eine rechtsberatende Person vermittelt

Die Auslöser

Die Anlässe entsprechen weitgehend der bekannten Systematik: Begründung einer Geschäftsbeziehung, Einzeltransaktion ab **10.000 €**, Mitwirkung an der Gründung von Gesellschaften oder Rechtsgestaltungen unabhängig vom Wert, Verdachtsfall sowie Zweifel an früher erhobenen Angaben (Art. 19 Abs. 1). Hinzu kommt eine gesonderte Schwelle: Bei einer **Bareinzeltransaktion ab 3.000 €** ist mindestens der Kunde zu identifizieren (Abs. 4).

Neu ist außerdem eine EU-weite **Bargeldobergrenze von 10.000 €** für Waren *und* Dienstleistungen — auch bei mehreren, offenkundig zusammenhängenden Zahlungen (Art. 80). Sie gilt für jede berufliche Tätigkeit; ausgenommen sind Zahlungen zwischen Privatpersonen. Niedrigere nationale Grenzen bleiben zulässig.

Aus einem Vorgang können zwei KYC-Prüfungen werden

Vermittelt eine Notarin, ein Rechtsanwalt oder eine andere rechtsberatende Person eine Transaktion und ist sie dabei die **einzige** vermittelnde Person, so gelten **beide Parteien** der Transaktion als Kunden (Art. 19 Abs. 6 lit. b). Für die Immobilienvermittlung gilt dasselbe (lit. c); beim Handel mit hochwertigen Gütern tritt der Lieferant hinzu (lit. a).

> **Zahl der Prüfungen statt Aufwand je Prüfung**
>
> Alle übrigen Änderungen erhöhen den Aufwand **je KYC-Prüfung**. Diese Regel erhöht die **Zahl der Prüfungen**. Ein vermittelter Kaufvertrag erzeugt zwei vollständige Sorgfaltsprüfungen statt einer — mit allem, was in den folgenden Kapiteln steht, zweimal.

2.2 Identifizierung des Kunden

DATEN, METHODE, ZEITPUNKT UND DIE ROLLE DER SELBSTAUSKUNFT

GEGENSTAND	HEUTE (GWG)	AB 10.07.2027 (AMLR)
Pflichtdaten Kunde	Ausweis und Register, nationale Praxis	feste EU-Datenliste: alle Staatsangehörigkeiten, Nominee-Gesellschafter namentlich, Registernummer, Steuernummer, LEI soweit vorhanden
Handelnde Person	identifizieren **und** Vertretungsbefugnis prüfen (§ 10 Abs. 1 Nr. 1)	im Kern **unverändert** — die Verordnung fasst beides in einer Vorschrift zusammen (Art. 20 Abs. 1 lit. i)
Verifizierungsmethode	Präsenz, VideoIdent, eID — je Land unterschiedlich anerkannt	eIDAS-Identifizierung der Stufen „substanziell“ und „hoch“ **sowie qualifizierte Vertrauensdienste** EU-weit anerkannt
Zeitpunkt	Praxis uneinheitlich	grundsätzlich **vor** Begründung; Aufschub nur risikobasiert und begründet
Selbstauskunft	trägt den Nachweis in der Praxis	bleibt Pflicht des Kunden, genügt als Nachweis aber nicht mehr allein

Der Pflichtdatensatz

Für natürliche Personen sind zu erheben: alle Vor- und Nachnamen, Geburtsort und vollständiges Geburtsdatum, **alle Staatsangehörigkeiten** — die Verordnung verwendet ausdrücklich den Plural — beziehungsweise Staatenlosigkeit oder Schutzstatus, die nationale Ausweisnummer, falls es eine gibt, der gewöhnliche Wohnsitz sowie die Steuernummer, falls vorhanden (Art. 22 Abs. 1).

Für juristische Personen: Rechtsform und Name, Anschrift des Sitzes und, falls abweichend, der Hauptniederlassung, das Gründungsland, die Namen der gesetzlichen Vertreter sowie — soweit vorhanden — Registernummer, Steuernummer und die **LEI** — die international einheitliche Kennnummer für Unternehmen. Ausdrücklich zu erfassen sind zudem die Namen von **Nominee-Gesellschaftern und Nominee-Direktoren**. **Neu gegenüber dem Geldwäschegesetz sind davon drei Angaben:** die Steuernummer, die LEI und die Nominee-Verhältnisse. Rechtsform, Sitz, Gründungsland, Registernummer und die Namen der gesetzlichen Vertreter gehören bereits heute zum Pflichtdatensatz.

Die für den Kunden auftretende Person ist auf ihre Vertretungsbefugnis zu prüfen *und* selbst zu identifizieren (Art. 20 Abs. 1 lit. i). Das ist **keine Neuerung**: § 10 Absatz 1 Nummer 1 GwG verlangt beides bereits heute. Ebenso wenig neu sind die Namen der gesetzlichen Vertreter — § 11 Absatz 4 Nummer 2 GwG verlangt sie heute schon, und zwar für alle Mitglieder des Vertretungsorgans, nicht nur für das handelnde.

Zwei Wege stehen zur Wahl

Die Verordnung beschreibt, wie die Identität zu überprüfen ist, in einem einzigen Absatz. Die Verpflichteten holen die notwendigen Informationen, Unterlagen und Daten danach „auf **einem der folgenden Wege**“ ein (Art. 22 Abs. 6). Es sind also zwei gleichrangige Wege, zwischen denen gewählt werden darf — nicht zwei Anforderungen, die nebeneinander zu erfüllen wären.

WEG	WAS ER VERLANGT	WANN ER PRAKTISCH TRÄGT
a — Ausweisvorlage	Personalausweis, Pass oder ein gleichwertiges Ausweisdokument, erforderlichenfalls ergänzt um Informationen aus verlässlichen und unabhängigen Quellen	überall dort, wo der Kunde persönlich erscheint oder ein Ausweisdokument vorlegt
b — elektronisch	ein elektronisches Identifizierungsmittel nach der eIDAS-Verordnung mit dem Sicherheitsniveau „substanziell“ oder „hoch“ oder ein einschlägiger qualifizierter Vertrauensdienst	bei Identifizierung aus der Ferne

Was daraus folgt

Wer den Ausweis vorgelegt bekommt, geht Weg a. An diesem Weg ändert die Verordnung nichts Grundsätzliches: Es bleibt beim Ausweisdokument, ergänzt um weitere Quellen, wo das Risiko es verlangt. Ein elektronisches Identifizierungsmittel oder ein qualifizierter Vertrauensdienst ist dafür **nicht vorgeschrieben**. Die Anforderungen des folgenden Abschnitts betreffen im Kern die Identifizierung aus der Ferne.

Die Methode wird EU-weit einheitlich

Heute entscheidet jeder Mitgliedstaat, welche Fernidentifizierung er anerkennt — in Deutschland vor allem das Videoidentifizierungsverfahren nach dem **BaFin-Rundschreiben 3/2017 (GW)** sowie der Online-Ausweis. Die AMLR erkennt **elektronische Identifizierungsmittel nach der eIDAS-Verordnung mit dem Sicherheitsniveau „substanziell“ oder „hoch“** sowie qualifizierte Vertrauensdienste ausdrücklich an (Art. 22 Abs. 6 lit. b). Wer grenzüberschreitend arbeitet, muss damit nicht mehr für jedes Land einzeln prüfen, welches Verfahren dort akzeptiert wird.

Das Rundschreiben ist bis heute nicht aufgehoben; die BaFin hat es zuletzt als Brückentechnologie ausdrücklich fortgeführt. Seine Grundlage ist das Geldwäschegesetz. Weil die AMLR die Sorgfaltspflichten ab dem 10. Juli 2027 unmittelbar regelt, verliert diese nationale Grundlage ihre Tragfähigkeit, ohne dass es dafür einer förmlichen Aufhebung bedarf. Das Verfahren selbst bleibt zulässig — künftig aber an der Stelle, die der folgende Absatz beschreibt.

AUS DEM ENTWURF DER TECHNISCHEN REGULIERUNGSSTANDARDS

Der Entwurf legt eine **Rangfolge** fest: Bei nicht persönlicher Identifizierung ist vorrangig ein eIDAS-Mittel oder ein qualifizierter Vertrauensdienst zu nutzen. Nur wenn das nicht verfügbar oder nicht zumutbar ist, darf auf eine dokumentenbasierte Fernidentifizierung ausgewichen werden — dann aber mit definierten Sicherungen (Abgleich Person und Lichtbild, gesicherte Übertragung, lesbare und zeitgestempelte Aufzeichnung, Abbruch bei Störungen) und mit der Pflicht, gegenüber der Aufsicht zu **begründen, warum** nicht vorrangig identifiziert wurde.

ENTWURF, ANNAHME STEHT AUS

Qualifizierte Vertrauensdienste

Neben den elektronischen Identifizierungsmitteln — englisch *electronic identification means*, kurz **eID** — nennt die Verordnung ausdrücklich die **qualifizierten Vertrauensdienste** nach der eIDAS-Verordnung als zulässigen Weg der Verifizierung (Art. 22 Abs. 6 lit. b). Im englischen Text heißen sie *qualified trust services*, die Anbieter *qualified trust service provider*, abgekürzt **QTSP**. Die Sicherheitsniveaus „substanziell" und „hoch" entsprechen *substantial* und *high*.

Die Begründung der Verordnung empfiehlt diesen Weg besonders dort, wo sich die Identität schwer prüfen lässt. Genannt sind der **Aufenthaltsstatus** in einem Mitgliedstaat und der **Wohnsitz in einem Drittstaat**. Der Vertrauensdienst steht dort also als *Ersatz* für ein nicht verfügbares Identifizierungsmittel — er tritt nicht zusätzlich neben eines, das vorhanden ist.

Die eIDAS-Verordnung kennt mehrere qualifizierte Vertrauensdienste. Für die Identitätsprüfung ist neben der qualifizierten elektronischen Signatur vor allem die **qualifizierte elektronische Attributsbescheinigung** von Bedeutung — englisch *qualified electronic attestation of attributes*, abgekürzt **QEAA**. Sie bescheinigt einzelne geprüfte Merkmale einer Person, etwa eine Steuernummer oder eine Anschrift. Damit ist sie das Instrument, mit dem sich genau die Lücke schließen lässt, die der Entwurf der technischen Standards beschreibt: Deckt ein Identifizierungsmittel nicht alle Pflichtattribute ab, sind die fehlenden Angaben auf anderem Weg zu beschaffen und zu überprüfen.

Eine **technische Norm** für die Identitätsprüfung schreibt die Verordnung nicht vor. Weder in der AMLR noch im Entwurf der technischen Standards kommt eine ETSI-Norm vor. Verweise auf solche Normen stammen aus dem Recht der Vertrauensdienste und nicht aus dem Geldwäscherecht.

Für die Planung ist allerdings der **Verfügbarkeitsstand** maßgeblich, nicht die Rechtslage allein. Attributsbescheinigungen darf nur ausstellen, wer als qualifizierter Vertrauensdiensteanbieter zugelassen und in die Vertrauensliste eingetragen ist; die Aufsicht führt in Deutschland die Bundesnetzagentur. Für diesen Dienst weist sie **derzeit keinen zugelassenen Anbieter in Deutschland aus**. Hinzu kommt eine praktische Hürde: Wer ein Merkmal bescheinigt, muss es gegen die amtliche Stelle prüfen können, die es führt. Die Anschrift liegt bei den kommunalen Meldebehörden, die Steuernummer beim Bundeszentralamt für Steuern.

AUS DEM ENTWURF DES DIGITALE-IDENTITÄTEN-GESETZES

Der Entwurf verpflichtet **Behörden des Bundes**, nach Ablauf von 24 Monaten nach Verkündung auf Antrag auch elektronische Attributsbescheinigungen auszustellen. Länder und Kommunen erfasst die Vorschrift **nicht** — und damit nicht das Meldewesen. Für die Anschrift ist ein flächendeckender Bescheinigungsweg deshalb auf absehbare Zeit nicht zu erwarten. ENTWURF, VERABSCHIEDUNG STEHT AUS

Was daraus folgt

Die Attributsbescheinigung ist der **rechtlich vorgesehene**, aber nicht der **heute verfügbare** Weg, fehlende Angaben zu schließen. Wer 2027 vollständige Datensätze braucht, wird sie zunächst auf dem klassischen Weg erheben und belegen müssen: Bescheinigung, Registerauszug, dokumentierte Kundenangabe.

Natürliche und juristische Personen werden getrennt behandelt

Der Entwurf der technischen Standards ordnet jedem Pflichtfeld (Art. 22 Abs. 1) ein konkretes Attribut zu — in **zwei getrennten Listen** für natürliche und juristische Personen. An deren Umfang entscheidet sich, wie weit ein elektronisches Identifizierungsmittel trägt. ENTWURF, ANNAHME STEHT AUS

PFLICHTFELD	NATÜRLICHE PERSON	JURISTISCHE PERSON
Name	Vor- und Nachnamen	eingetragener Name und Rechtsform; dazu ein **dauerhafter Identifikator** des ausstellenden Mitgliedstaats für die grenzüberschreitende Zuordnung
Herkunft	Geburtsort und -datum, Staatsangehörigkeiten, gegebenenfalls Status als staatenlos oder schutzberechtigt	Gründungsland

PFLICHTFELD	NATÜRLICHE PERSON	JURISTISCHE PERSON
Anschrift	Wohnsitz, aufgeschlüsselt nach Land, Region, Ort, Postleitzahl, Straße und Hausnummer	Sitzanschrift und, falls abweichend, weitere Anschriften
Kennnummern	nationale Verwaltungsnummer und Steuernummer, soweit vorhanden	**LEI**, Umsatzsteuer- oder Steuernummer, Registernummer — jeweils soweit vorhanden
Personenbezug	—	Namen der gesetzlichen Vertreter sowie der **Nominee-Gesellschafter und -Direktoren**, einschließlich des Hinweises auf diesen Status

> **Was daraus folgt**
>
> Für **natürliche Personen** deckt ein elektronisches Identifizierungsmittel den Pflichtdatensatz weitgehend ab. Für **juristische Personen** gilt das nicht: Namen der gesetzlichen Vertreter, Registernummern und vor allem die Nominee-Verhältnisse liefert heute kein Identifizierungsmittel vollständig mit. Bei Gesellschaften bleibt die Verifizierung deshalb ein **zusammengesetzter Vorgang** aus elektronischer Identifizierung, Registerabruf und Unterlagen.

Der Unterschied zeigt sich schon an der Schreibweise der beiden Listen. Für natürliche Personen benennt der Entwurf **feste Feldnamen** — Familienname, Geburtsdatum, Postleitzahl des Wohnsitzes. Für juristische Personen stehen dagegen fast durchgehend Umschreibungen: „sonstige vorhandene Attribute, die die Rechtsform abdecken“, „… die Namen der gesetzlichen Vertreter abdecken“, „… die Registernummer abdecken“. Benannte Felder gibt es dort nur drei: eingetragener Name, aktuelle Anschrift und LEI. Der Grund steht in der Fußnote des Anhangs: Die Feldnamen stammen aus der Durchführungsverordnung zum EUDI-Wallet — und dieses Datenmodell ist um **Menschen** herum gebaut. Für Gesellschaften existiert kein entsprechender Satz.

Was deutsche Identifizierungsmittel tatsächlich liefern

Die Lückenschlusspflicht wird dort praktisch, wo man die Attributliste gegen die Mittel hält, die in Deutschland zur Verfügung stehen: die **Online-Ausweisfunktion des Personalausweises** und den Personendatensatz des künftigen **EUDI-Wallets**.

PFLICHTANGABE	ONLINE-AUSWEISFUNKTION	WALLET (PERSONENDATENSATZ)
Namen, Geburtsdatum, Geburtsort	enthalten	enthalten
Staatsangehörigkeit	enthalten	enthalten
Anschrift	**enthalten** (§ 18 Abs. 3 PAuswG)	**nicht enthalten**
Nationale Verwaltungsnummer	nicht vorhanden	nicht vorhanden
Steuernummer	**nicht enthalten**	**nicht enthalten**

Zwei Punkte verdienen eine Einordnung. Deutschland kennt **keine allgemeine Personenkennziffer**; die Angabe entfällt daher regelmäßig. Ob die **Steuer-Identifikationsnummer** diese Rolle inzwischen einnimmt, weil das Identifikationsnummerngesetz sie zur registerübergreifenden Ordnungsnummer bestimmt hat, ist bislang nicht geklärt. Für die Praxis ist die Frage nachrangig: Die Verordnung verlangt die Steuernummer ohnehin, „falls verfügbar“ (Art. 22 Abs. 1 lit. a Ziff. iv) — und in Deutschland hat jede gemeldete Person eine.

> **Der Kern in einem Satz**
>
> Selbst die vollständige elektronische Identifizierung einer natürlichen Person hinterlässt in Deutschland mindestens **ein ungedecktes Pflichtfeld**. Das ist keine Randerscheinung, sondern der Regelfall — und es bedeutet, dass jede Prüfung einen zweiten, dokumentierten Erhebungsschritt braucht.

AUS DEM ENTWURF DER TECHNISCHEN REGULIERUNGSSTANDARDS

Der Entwurf widmet eID und qualifizierten Vertrauensdiensten einen eigenen Abschnitt. **Erstens** legt er die genannten Attributlisten fest; bei vereinfachter Sorgfalt genügt ein reduzierter Satz. **Zweitens** enthält er eine **Lückenschlusspflicht**: Deckt das Identifizierungsmittel oder der Vertrauensdienst nicht alle erforderlichen Attribute ab, muss der Verpflichtete die fehlenden Angaben auf anderem Weg beschaffen *und überprüfen*. **Drittens** nennt der Entwurf als verstärkte Maßnahme ausdrücklich ein **höheres Sicherheitsniveau oder die Ergänzung des Identifizierungsmittels um einen qualifizierten Vertrauensdienst**. Die Attributbezeichnungen stützt der Entwurf auf die Durchführungsverordnung zum EUDI-Wallet. Die Namen der Datenfelder stammen also aus dem Wallet-Standard, auch wenn die AMLR selbst keine Wallet vorschreibt. ENTWURF, ANNAHME STEHT AUS

Was das für ein System bedeutet

Aus den Attributlisten und der Lückenschlusspflicht folgen fünf Anforderungen. Alle fünf betreffen nicht den Abruf selbst, sondern das, was *nach* dem Abruf mit den gelieferten Daten geschieht.

ANFORDERUNG	WAS DAS SYSTEM LEISTEN MUSS
Attribute zuordnen	Die gelieferten Attributnamen des Wallet-Standards auf die eigenen Pflichtfelder abbilden — als **Konfiguration**, nicht fest verdrahtet, weil sich die Liste mit dem Rechtsakt noch ändern kann
Vollständigkeit prüfen	Nach jedem Abruf automatisch feststellen, welche Pflichtfelder gedeckt sind und welche fehlen — **getrennt für natürliche und juristische Personen** und abhängig von der Prüftiefe, da bei vereinfachter Sorgfalt weniger verlangt ist
Lücken weiterreichen	Fehlende Felder nicht nur anzeigen, sondern in eine **Nacherhebung überführen** und deren Abschluss überwachen — offene Felder dürfen die Prüfung nicht als abgeschlossen erscheinen lassen
Herkunft je Feld festhalten	Für jedes Feld speichern, **woher** der Wert stammt — elektronische Identifizierung, Vertrauensdienst, Register oder Kundenangabe — und wie er überprüft wurde. Die über eID gewonnenen Daten sind ausdrücklich aufbewahrungspflichtig
Verfahren risikoabhängig wählen	Das Sicherheitsniveau und die Kombination aus eID und Vertrauensdienst müssen von der **Risikoklasse** abhängen können. Wird nicht elektronisch identifiziert, muss das System die **Begründung erzwingen und speichern**

Was hier nicht geregelt ist

Die Verordnung regelt die **Identitätsprüfung**, nicht die Unterschrift. Eine qualifizierte elektronische Signatur ist an keiner Stelle der AMLR vorgeschrieben — sie kann aus Formvorschriften erforderlich sein, gehört aber nicht zu den Sorgfaltspflichten.

Der Zeitpunkt

Die Verifizierung erfolgt grundsätzlich **vor** Begründung der Geschäftsbeziehung oder Durchführung der Einzeltransaktion (Art. 23 Abs. 1). Ein Aufschub ist zulässig, wenn ein niedriges Risiko ihn rechtfertigt oder der normale Geschäftsablauf sonst unterbrochen würde. Die Prüfung ist dann so bald wie praktisch möglich nachzuholen (Abs. 2). Bei vereinfachter Sorgfalt beträgt die Höchstdauer **60 Tage** (Art. 33 Abs. 1 lit. a). Der bislang oft beiläufige Satz „Ausweis reichen wir nach“ wird damit zu einer begründungspflichtigen Entscheidung.

Die Selbstauskunft: vom Nachweis zum Ausgangspunkt

In der Praxis ist das unterschriebene Selbstauskunftsformular oft der einzige Beleg in den Unterlagen. Schon heute ist der Vertragspartner zur Mitwirkung verpflichtet: Er muss offenlegen, ob er für einen wirtschaftlich Berechtigten handelt, dessen Identität nachweisen und Änderungen unverzüglich mitteilen (§ 11 Abs. 6 GwG). Zugleich darf sich der Verpflichtete nicht ausschließlich auf das Transparenzregister stützen (§ 11 Abs. 5 GwG).

Die AMLR bewegt die Selbstauskunft in zwei Richtungen zugleich. **Rechtlich wird sie stärker.** Juristische Personen *müssen* Verpflichteten bei der Sorgfaltsprüfung Angaben zu ihren wirtschaftlich Berechtigten liefern, und wirtschaftlich

Berechtigte wie Zwischengesellschaften müssen der Gesellschaft zuliefern. Die Gesellschaft selbst muss ihre Angaben **mindestens jährlich** prüfen und Änderungen **binnen 28 Kalendertagen** an das Register melden (Art. 63 Abs. 1 und 2).

Als Nachweis verliert sie zugleich die Alleinstellung. Der Registerabgleich wird zur Pflicht, und je neuer Geschäftsbeziehung tritt ein Registernachweis hinzu. Weicht die Erklärung vom Register ab, läuft eine Meldefrist von 14 Tagen (dazu Kapitel 2.3).

> **Der Unterschied in einem Satz**
>
> Heute reicht das Register allein nicht — künftig reicht die Selbstauskunft allein nicht. Aus dem Dokument, das die Prüfung **abschließt**, wird das Dokument, das sie **auslöst**.

2.3 Wirtschaftlich Berechtigte

ERMITTLUNG, FIKTIVE BERECHTIGTE, VERIFIZIERUNG, REGISTER

GEGENSTAND	HEUTE (GWG)	AB 10.07.2027 (AMLR)
Ermittlung	„mehr als 25 %“, oft nur oberste Ebene	„ab 25 %“; jede Ebene durchrechnen, parallele Stränge addieren; Eigentum und Kontrolle nebeneinander
Fiktive wirtschaftlich Berechtigte	eine gesetzliche Vertretung	**alle** Mitglieder der Geschäftsleitung, gleiche Prüftiefe, dokumentierte Begründung
Verifizierung	Name erfassen, grob auf Stimmigkeit prüfen	Identität **aller** Berechtigten risikoangemessen prüfen; Ausweisnummer im Datensatz
Registerabgleich	Abgleich, kein alleiniges Verlassen darauf	Pflichtabgleich **plus** gültiger Registernachweis je neuer Geschäftsbeziehung
Unstimmigkeitsmeldung	Meldepflicht ohne feste Frist	**14 Kalendertage**, mit Fallunterscheidung; Ausnahme für rechtsberatende Berufe

Die Ermittlung wird zur Rechenaufgabe

Die Schwelle sinkt von „mehr als 25 %“ auf **„ab 25 %“**. Wichtiger als der halbe Prozentpunkt ist die Rechenweise: Beteiligungen sind über **jede Ebene** der Struktur zu ermitteln — entlang einer Kette werden die Quoten multipliziert, parallele Stränge addiert. Eigentum und Kontrolle sind **nebeneinander** zu prüfen, nicht alternativ (Art. 51–54).

> **Beispiel**
>
> Eine Person hält 20 % unmittelbar und weitere 14,4 % mittelbar über eine Tochtergesellschaft. Zusammen sind das **34,4 %** — sie ist wirtschaftlich Berechtigte, obwohl kein einzelner Strang die Schwelle erreicht. Nach heutiger Praxis, die häufig auf der obersten Ebene ansetzt, bliebe sie unentdeckt.

Fiktive wirtschaftlich Berechtigte

Lässt sich über Eigentum und Kontrolle niemand ermitteln, tritt heute **eine** Person an diese Stelle — in der Praxis die gesetzliche Vertretung. Künftig gelten **alle** Personen als fiktive wirtschaftlich Berechtigte, die der Geschäftsleitung angehören; die Verordnung spricht von den geschäftsführenden Mitgliedern des Leitungsorgans und den Personen, die die Tagesgeschäfte verantworten (Art. 63 Abs. 4 lit. b).

Dazu kommen zwei Dokumentationspflichten: Die Schritte der erfolglosen Ermittlung sind **aufzuzeichnen** (Abs. 3), und es ist zu **begründen**, warum kein wirtschaftlich Berechtigter ermittelt werden konnte (Abs. 4 lit. a). Aus einem Eintrag im Formular wird damit ein belegter Vorgang.

> **AUS DEM ENTWURF DER TECHNISCHEN REGULIERUNGSSTANDARDS**
>
> Für fiktive wirtschaftlich Berechtigte sind **dieselben Daten** zu erheben und **dieselbe Verifizierungstiefe** anzuwenden wie für echte wirtschaftlich Berechtigte. Zulässig ist lediglich, statt der Privatanschrift die Anschrift des Gesellschaftssitzes zu verwenden. ENTWURF, ANNAHME STEHT AUS

Alle Berechtigten müssen verifiziert werden

Heute genügt es, den wirtschaftlich Berechtigten namentlich zu erfassen und risikoangemessen zu plausibilisieren; eine Ausweisprüfung ist nicht verlangt. Künftig ist die **Identität aller** wirtschaftlich Berechtigten zu überprüfen — mit „angemessenen Maßnahmen“ (Art. 20 Abs. 1 lit. b, Art. 22 Abs. 7). Der Datensatz umfasst zudem die **Nummer des Ausweisdokuments** (Art. 62 Abs. 1).

„Angemessene Maßnahmen“ bedeutet **nicht**, dass jede Person per VideoIdent zu identifizieren wäre. Der Entwurf der technischen Regulierungsstandards nennt als zulässige Wege unter anderem öffentliche Register außerhalb des Zentralregisters, Auskünfte seriöser Datenanbieter, aktuelle Bestätigungen von Kreditinstituten oder Gesellschaftsunterlagen mit beglaubigter Identitätsangabe. ENTWURF, ANNAHME STEHT AUS Die Zahl der zu prüfenden **Personen** steigt — nicht zwingend die Eingriffstiefe je Person.

Registerabgleich und Registernachweis

Der Abgleich mit dem Zentralregister wird zur **Pflicht** (Art. 22 Abs. 7). Zusätzlich ist bei jeder neuen Geschäftsbeziehung mit einer Gesellschaft, einem Trust oder einer ähnlichen Konstruktion ein **gültiger Registrierungsnachweis oder ein aktueller Registerauszug** einzuholen, der die Gültigkeit der Eintragung bestätigt (Art. 23 Abs. 4). Es genügt also nicht, das Register anzusehen — der Beleg gehört datiert in die Unterlagen.

Abgleich und Nachweis sind dabei **zwei verschiedene Dinge**. Der Abgleich mit dem Zentralregister ist Pflicht. Für die *Überprüfung* der wirtschaftlich Berechtigten verweist die Verordnung dagegen auf Quellen „einschließlich öffentlicher Register, **die keine Zentralregister sind**“ (Art. 22 Abs. 7 lit. b), und der Entwurf der technischen Standards wiederholt diese Einschränkung. Das Transparenzregister ist ein Zentralregister. Es allein trägt die Verifizierung also nicht — neben dem Pflichtabgleich braucht es **mindestens eine zweite, unabhängige Quelle**. Der Sache nach ist das die Fortschreibung des heutigen § 11 Abs. 5 GwG, nun mit ausdrücklicher Benennung der zulässigen Alternativen.

Die Unstimmigkeitsmeldung bekommt eine Frist

Weichen die eigenen Erkenntnisse von den Registerangaben ab, ist dies unverzüglich, **spätestens binnen 14 Kalendertagen** zu melden — mit Begründung und mit Angabe, wen man selbst für wirtschaftlich berechtigt hält (Art. 24 Abs. 1).

Bei geringfügigen Abweichungen darf stattdessen der Kunde aufgefordert werden, **binnen 14 Tagen** selbst zu korrigieren — etwa bei Schreibfehlern, abweichender Transliteration oder veralteten Daten, während die Lage im Kern klar ist. Bleibt er untätig, ist doch zu melden (Abs. 2 und 3). Bei hohem Risiko entfällt diese Erleichterung. Für Notariat, Rechtsberatung, Prüfung und Steuerberatung gilt die Vorschrift **nicht**, soweit Informationen aus der Beurteilung der Rechtslage oder aus der Vertretung in Verfahren stammen (Abs. 4).

2.4 Zweck und Geschäftstätigkeit

WAS ÜBER DIE GESCHÄFTSBEZIEHUNG SELBST ZU ERHEBEN IST

GEGENSTAND	HEUTE (GWG)	AB 10.07.2027 (AMLR)
Zweck und Tätigkeit	Kurznotiz, häufig Freitext	**fünf Pflichtangaben**: Zweck, erwartetes Volumen, Mittelherkunft, Mittelverwendung, Beruf oder Branche

Wo heute häufig eine Zeile Freitext steht, verlangt die Verordnung **fünf Angaben bei jeder Geschäftsbeziehung** (Art. 25):

ANGABE	WAS GEMEINT IST
Zweck und wirtschaftlicher Hintergrund	Grund der Beauftragung, beabsichtigte Nutzung der Leistung
Erwartetes Volumen	geschätzter Umfang der vorgesehenen Tätigkeiten
Herkunft der Mittel	welche Tätigkeit die Mittel erzeugt hat — Arbeitseinkommen, Unternehmenserlöse, Darlehen, Erbschaft und Ähnliches
Verwendung der Mittel	erwartete Empfänger und Zieljurisdiktionen
Geschäftstätigkeit oder Beruf	Branche, Beschäftigungsstatus, ob die Tätigkeit reguliert ist

Zwei der fünf Angaben verändern die Praxis stärker als die übrigen. Erstens die **Mittelherkunft**: Sie gehört heute zur verstärkten Sorgfalt und wird künftig zum Standardinhalt *jeder* Geschäftsbeziehung. Zweitens die **Geschäftstätigkeit oder der Beruf** — sie gehören zwar nicht zum Identifizierungsdatensatz (Art. 22), sind aber ausdrücklich zu erheben und zu bewerten (Art. 25; Art. 20 Abs. 1 lit. e).

Diese Angaben sind zugleich die Grundlage der laufenden Überwachung: Ohne ein erwartetes Tätigkeitsprofil lässt sich nicht feststellen, ob eine Transaktion davon abweicht.

2.5 Screening: politisch exponierte Personen, Sanktionen, Reputation

ABGLEICHE GEGEN EXTERNE QUELLEN

GEGENSTAND	HEUTE (GWG)	AB 10.07.2027 (AMLR)
Politisch exponierte Personen	Selbstauskunft, nationale Auslegung	erweiterter Kreis ab 50.000 Einwohnern; EU-Liste der **Ämter**; erneute Prüfung auch bei Listenänderung
Sanktionen	kein Abgleich im GwG — Bindung über EU-Verordnungen und AWG	eigene Sorgfaltspflicht; Kunde, Berechtigte und kontrollierende Personen; über 50 % **aggregiert**
Reputation	keine ausdrückliche Pflicht	verbindliche **Risikovariable**; Medienrecherche anerkannt, begrenzt durch die Vorgaben zur Datenverarbeitung (Art. 76)

Politisch exponierte Personen

Der Personenkreis wächst: Als wichtiges öffentliches Amt gelten künftig auch die Leitungen regionaler und lokaler Behörden ab **50.000 Einwohnern** (Art. 2 Nr. 34). Der Angehörigenkreis umfasst Geschwister, allerdings nur bei den höchsten Funktionen (Nr. 35). Zu prüfen sind Kunde, wirtschaftlich Berechtigte und die Person, für die gehandelt wird (Art. 20 Abs. 1 lit. g), und zwar jeweils auch deren Familienmitglieder und nahestehende Personen (Art. 46).

Die Mitgliedstaaten führen Listen der **genauen Ämter**, die Kommission ergänzt die Unionsebene. Beides fügt sie zu einer einzigen Liste zusammen, die im Amtsblatt veröffentlicht und von der AMLA bereitgestellt wird (Art. 43). Diese Liste enthält **Ämter, keine Namen** — rund 1.400 Funktionseinträge aus 27 Mitgliedstaaten. Die Zuordnung einer konkreten Person zu einem Amt bleibt Aufgabe des Verpflichteten.

Bei einem Treffer sind drei Maßnahmen zwingend: **Zustimmung der Führungsebene**, Ermittlung von **Vermögens- und Mittelherkunft**, **verstärkte laufende Überwachung** (Art. 42 Abs. 1). Nach dem Ausscheiden aus dem Amt endet die Behandlung nicht automatisch. Das fortwirkende Risiko ist zu berücksichtigen, und mindestens eine verstärkte Maßnahme ist anzuwenden, solange das Risiko besteht — **in jedem Fall zwölf Monate** (Art. 45). Die zwölf Monate sind eine Untergrenze, kein Verfallsdatum.

Sanktionen: vom Verbot zum Verfahren

Die Sanktionsprüfung ist bislang keine Pflicht des Geldwäscherechts. Wer sie schon heute für eine solche hält, unterschätzt, was 2027 hinzukommt.

	HEUTE	AB 10.07.2027
Grundlage	unmittelbar geltende EU-Sanktionsverordnungen sowie das Außenwirtschaftsgesetz (§§ 4, 6 AWG) — **kein** Abgleich in den Sorgfaltspflichten des GwG	zusätzlich Art. 20 Abs. 1 lit. d AMLR als Bestandteil der Sorgfaltspflichten
Adressaten	**jedermann**, unabhängig von der Verpflichteteneigenschaft	weiterhin jedermann, zusätzlich alle Verpflichteten — auch im Nichtfinanzsektor
Geschuldet	das **Ergebnis**: nicht verfügen, nicht bereitstellen. Ein Verfahren ist nicht vorgeschrieben	das **Verfahren**: Prüfumfang, Anlässe und Datenattribute sind vorgegeben
Umfang	rechtlich offen, praktisch meist nur der Vertragspartner	Kunde, wirtschaftlich Berechtigte und **kontrollierende Personen**; bei Umgehungsverdacht auch die auftretende Person
Wiederholung	nicht geregelt	verpflichtend, risikobasiert getaktet (Art. 26 Abs. 4); Institute zusätzlich bei jeder neuen Listung

Die Prüfung reicht dabei in die Beteiligungsstruktur hinein: Zu prüfen ist auch, ob gelistete Personen die Gesellschaft **kontrollieren** oder **mehr als 50 % der Eigentumsrechte** halten — ausdrücklich „einzeln oder gemeinsam“. Halten zwei gelistete Personen je 30 %, ist die Gesellschaft selbst betroffen, ohne auf einer Liste zu stehen.

Dazu kommt eine Aufzeichnungspflicht für die Übergangsphase. Zwischen der Veröffentlichung einer Finanzsanktion der Vereinten Nationen und ihrer Umsetzung in der Union sind die verwalteten Vermögenswerte sowie die **versuchten** und die ausgeführten Transaktionen zu dokumentieren (Art. 27). Die neue Sorgfaltspflicht ersetzt das Sanktionsrecht **nicht** — das stellt die Verordnung ausdrücklich klar (Art. 26 Abs. 4).

> **AUS DEM ENTWURF DER TECHNISCHEN REGULIERUNGSSTANDARDS**
>
> Sowohl für die PEP-Feststellung als auch für den Sanktionsabgleich sieht der Entwurf **automatisierte Werkzeuge als Regelfall** vor. Eine rein manuelle Prüfung bleibt nur zulässig, soweit sie zu Größe, Geschäftsmodell und Komplexität des Unternehmens verhältnismäßig ist. Zu screenen sind Namen im Original **und in Transliteration**, abweichende Namen, Aliase und Handelsnamen sowie — soweit gelistet — Wallet-Adressen. Anlässe sind die Aufnahme, **jede neue oder geänderte Listung** und jede wesentliche Änderung der Kundendaten. ENTWURF, ANNAHME STEHT AUS

Reputation und Adverse Media

Die Begriffe „Adverse Media“ und „Negative News“ kommen im Verordnungstext **nicht vor**. Verankert ist gleichwohl die Sache. Die **Reputation** von Kunde und wirtschaftlich Berechtigtem gehört zu den Risikovariablen des Anhangs I. Für die Bestimmung des Prüfumfangs sind sie verbindlich (Art. 20 Abs. 2). Die Bewertung ist damit Pflicht, die Methode bleibt frei; Veröffentlichungen seriöser Medien sind als Nachweisquelle ausdrücklich anerkannt.

Den Rahmen setzt die Verordnung beim Datenschutz (Art. 76). Treffer aus Medienrecherchen sind regelmäßig Daten über Straftaten und dürfen nur verarbeitet werden, soweit dies unbedingt erforderlich ist. Voraussetzung sind Information des Kunden, zuverlässige, richtige und aktuelle Quellen, ein hohes Sicherheitsniveau und das Verbot voreingenommener oder diskriminierender Entscheidungen. Für Straftatendaten kommt hinzu, dass die internen Verfahren zwischen **Vorwurf,**

Ermittlung, laufendem Verfahren und Verurteilung unterscheiden müssen. Eine Nutzung zu kommerziellen Zwecken ist untersagt.

> **Automatisierte Verfahren und KI**
>
> Automatisierte Entscheidungen, Profiling und KI-Systeme sind ausdrücklich erlaubt (Art. 76 Abs. 5) — unter drei Bedingungen: Die Datenbasis bleibt auf die nach Kapitel III erhobenen Daten beschränkt, jede Entscheidung über Aufnahme, Ablehnung, Fortführung oder Prüftiefe unterliegt einer **wirksamen menschlichen Letztentscheidung**, und der Kunde kann eine **Erklärung verlangen und die Entscheidung anfechten**. Ausgenommen sind Verdachtsmeldungen.

2.6 Risikoeinstufung, vereinfachte und verstärkte Sorgfalt

WIE VIEL PRÜFUNG WANN VERLANGT WIRD

GEGENSTAND	HEUTE (GWG)	AB 10.07.2027 (AMLR)
Risikoeinstufung	freie Risikomatrix	Einstufung anhand vorgegebener Variablen und Faktoren, jederzeit nachweisbar
Vereinfachte Sorgfalt	Katalog nach GwG	definierte Erleichterungen; Überwachung bleibt zwingend; Fristen bleiben unberührt
Verstärkte Sorgfalt	vor allem PEP und Hochrisikoländer	**immer Pflicht**, unabhängig von der eigenen Einschätzung — auch bei auffälligen Transaktionen

Der risikobasierte Ansatz bleibt das Grundprinzip, wird aber deutlich stärker geführt. Der Umfang der Sorgfaltspflichten ist anhand der **Risikovariablen des Anhangs I** und der **Risikofaktoren der Anhänge II und III** zu bestimmen. Zugleich muss der Verpflichtete der Aufsicht **jederzeit** nachweisen können, dass die gewählten Maßnahmen angemessen waren (Art. 20 Abs. 2 und 4). Eine Einstufung ohne belegbare Herleitung ist damit nicht mehr tragfähig.

Die Faktoren hinter jeder Einstufung

Zu den Variablen zählen unter anderem Geschäftstätigkeit, **Reputation** sowie Art und Verhalten von Kunde und wirtschaftlich Berechtigtem (Anhang I). Hinzu kommen die betroffenen Jurisdiktionen, Zweck und Dauer der Beziehung, Transparenz und Komplexität des Produkts sowie der Vertriebsweg.

Als Faktoren erhöhten Risikos gelten unter anderem persönliche Vermögenshaltungsvehikel, Nominee-Gesellschafter oder Inhaberaktien und bargeldintensive Geschäfte (Anhang III). Dazu kommen **ungewöhnlich oder übermäßig komplexe Eigentümerstrukturen**, Gesellschaften ohne echtes Geschäft am Sitzort sowie Aufenthaltsrechte gegen Investition. Bei den geografischen Faktoren stehen neben Sanktions- und FATF-Bezügen ausdrücklich Staaten, die **Finanzgeheimhaltung ermöglichen**, etwa durch fehlende zentrale Register. Umgekehrt sind die Faktoren aufgeführt, die für ein geringes Risiko sprechen (Anhang II). Beide Listen sind ausdrücklich nicht abschließend.

Vereinfachte Sorgfalt und ihre Grenzen

Bei nachgewiesen niedrigem Risiko sind Erleichterungen zulässig: Aufschub der Verifizierung um bis zu 60 Tage, geringere Aktualisierungsfrequenz, reduzierter Erhebungsumfang, seltenere Transaktionsprüfung (Art. 33 Abs. 1). Drei Grenzen sind zentral:

- Eine **ausreichende Überwachung bleibt zwingend** — ungewöhnliche und verdächtige Transaktionen müssen weiterhin erkannt werden.
- Die Erleichterungen sind je Kundentyp in den internen Verfahren zu **benennen**, zusätzliche Niedrigrisikofaktoren zu **dokumentieren** (Abs. 2).
- Die Erleichterung **endet sofort** bei Zweifeln an den Angaben, Wegfall der Niedrigrisikofaktoren, entgegenstehenden Überwachungsergebnissen, Geldwäscheverdacht oder Verdacht auf Sanktionsumgehung (Abs. 5).

Verstärkte Sorgfalt ist künftig Pflicht, keine Ermessensfrage

Neben den Katalogfällen ist eine Untersuchung von Hintergrund, Herkunft, Ziel und Zweck **zwingend**, sobald eine Transaktion auch nur eines der folgenden Merkmale erfüllt: komplex, ungewöhnlich groß, ungewöhnliches Muster oder

ohne erkennbaren wirtschaftlichen oder rechtmäßigen Zweck (Art. 34 Abs. 2). Die häufige Einschätzung „bei uns ist das niedriges Risiko“ trägt hier nicht mehr.

Möglich sind: zusätzliche Informationen zu Kunde und Berechtigten, zusätzliche Informationen zur Art der Beziehung, Ermittlung von **Mittel- und Vermögensherkunft**, Klärung der Transaktionsgründe, **Zustimmung der Führungsebene**, verstärkte Überwachung mit höherer Prüffrequenz sowie Erstzahlung über ein Konto bei einem regulierten Kreditinstitut (Abs. 4).

2.7 Laufende Überwachung und Aktualisierung

DIE FRISTEN UND WAS SIE TATSÄCHLICH BEDEUTEN

GEGENSTAND	HEUTE (GWG)	AB 10.07.2027 (AMLR)
Überwachung und Aktualisierung	„angemessener Abstand“ — unbestimmt	Aktualisierungs-Fristen: **1 Jahr** bei hohem Risiko, maximal **5 Jahre** bei niedrigem Risiko; laufende Überwachung kommt hinzu

Aus der unbestimmten Anforderung, Kundendaten „in angemessenem zeitlichem Abstand“ zu aktualisieren, werden feste **Aktualisierungs-Fristen** (Art. 26 Abs. 2). Daneben besteht die kontinuierliche Überwachung nach Absatz 1 unverändert fort, ebenso die Pflicht, bei geänderten Umständen sofort zu aktualisieren (Abs. 3).

Die Fristen sind Obergrenzen, keine Zielwerte

Der Verordnungstext kennt **zwei** Kategorien — hohes Risiko und „alle übrigen“. Daraus folgt aber nicht, dass alle übrigen Kunden im Fünfjahresrhythmus zu prüfen wären. Die fünf Jahre sind die Grenze, die *in keinem Fall* überschritten werden darf; welcher Abstand angemessen ist, bestimmt weiterhin der risikobasierte Ansatz.

RISIKO	WAS DIE VERORDNUNG VORGIBT	WAS DARAUS PRAKTISCH FOLGT
Hoch	Obergrenze **1 Jahr** (Abs. 2 lit. a)	jährliche Überprüfung als Regelfall; bei verstärkter Sorgfalt zusätzlich engmaschigere Überwachung
Mittel	fällt unter „alle übrigen“ — Obergrenze **5 Jahre**	**Fünf Jahre sind hier nicht angemessen.** Der risikobasierte Ansatz verlangt kürzere, sachlich begründete Abstände; die Wahl des Intervalls ist zu dokumentieren
Niedrig	Obergrenze **5 Jahre** (Abs. 2 lit. b)	Ausschöpfung der Frist vertretbar, sofern das niedrige Risiko belegt ist und die laufende Überwachung funktioniert

Wer alle nicht als hoch eingestuften Kunden pauschal auf fünf Jahre setzt, kehrt den risikobasierten Ansatz um. Er nutzt eine Obergrenze als Standardwert und muss diese Wahl gleichwohl gegenüber der Aufsicht rechtfertigen (Art. 20 Abs. 4). Umgekehrt verlängert auch die vereinfachte Sorgfalt die Frist **nicht** über die fünf Jahre hinaus.

Unabhängig von jeder Frist ist zu aktualisieren, wenn sich die Umstände ändern, wenn gesetzlich ohnehin Kontakt aufzunehmen ist oder wenn relevante Tatsachen bekannt werden (Abs. 3). Die Frist ist damit die äußere Grenze, nicht der Auslöser.

Der Kundenbestand

> **AUS DEM ENTWURF DER TECHNISCHEN REGULIERUNGSSTANDARDS**
>
> Für Kunden, deren Geschäftsbeziehung vor Veröffentlichung der Delegierten Verordnung begründet wurde, sind Unterlagen, Daten und Informationen **risikobasiert** nachzuziehen. Der Entwurf setzt dafür eine Grenze: „in allen Fällen jedoch nicht später als innerhalb der Fristen des Artikels 26 Absatz 2“. Nach der Begründung des Entwurfs beginnen diese Fristen für den Kundenbestand erst mit dem **Anwendungsbeginn der Delegierten Verordnung** zu laufen.
>
> ENTWURF, ANNAHME STEHT AUS

Daraus folgt erstens: Es gibt **keinen Stichtag**, zu dem die Daten des gesamten Kundenbestands auf dem neuen Stand sein müssten — die Fristen laufen je Geschäftsbeziehung und damit rollierend. Zweitens ist der Weg dorthin ausdrücklich

risikobasiert; der Aufwand darf sich dort konzentrieren, wo das Risiko liegt. Jede KYC-Akte läuft damit in ihrem eigenen ReKYC-Zyklus.

> **Was die Frist bedeutet — und was nicht**
>
> Zwei Dinge sind auseinanderzuhalten. Für **Neukunden** gibt es keine Übergangsfrist: Wer ab dem 10. Juli 2027 eine Geschäftsbeziehung begründet, prüft sie von Beginn an vollständig nach den neuen Regeln. Bei **Bestandskunden** ist die Frist keine Schonfrist, sondern eine Nachziehpflicht: Die KYC-Akte muss bis zum Fristende dem AMLR-Stand entsprechen. Eine Prüfung nach heutigem Recht nimmt Ihnen diese Aktualisierung **nicht** ab — sie entscheidet aber darüber, wie aufwändig sie ausfällt. Was daraus folgt, steht in Kapitel 5.

2.8 Dokumentation, Abbruch und Meldewesen

WAS NACHWEISBAR BLEIBEN MUSS

GEGENSTAND	HEUTE (GWG)	AB 10.07.2027 (AMLR)
Dokumentation	nationales Verständnis	5 Jahre, **ungeschwärzt**, einschließlich eID-Daten; danach Löschpflicht
Abbruch und Ablehnung	Abbruch, wenn die Prüfung nicht abgeschlossen werden kann	Beendigung; **auch die Ablehnung** ist prüffest zu dokumentieren
Meldewesen	GwG-Meldewesen, Weg über die Kammer möglich	EU-einheitlich gefasst; Kammerweg bleibt zulässig; Ausnahmen für rechtsberatende Berufe
Auskunft an die Meldestelle	Auskunft auf Anfrage	**Systeme**, die über **fünf Jahre** vollständig und schnell Auskunft geben — auch zu beendeten Beziehungen

Aufbewahrung und Löschung

Aufzubewahren sind Kopien sämtlicher Sorgfaltsunterlagen — **einschließlich der über elektronische Identifizierung gewonnenen Daten** —, die Bewertungen auffälliger Transaktionen samt Ergebnis, und zwar **auch dann, wenn keine Verdachtsmeldung erfolgt**, sowie die Transaktionsbelege. Die Unterlagen dürfen **nicht geschwärzt** sein (Art. 77 Abs. 1).

Die Frist beträgt **fünf Jahre** ab Beendigung der Geschäftsbeziehung beziehungsweise ab der Einzeltransaktion oder ab der Ablehnung. Danach besteht eine **Löschpflicht** für personenbezogene Daten; eine Verlängerung ist nur einzelfallbezogen durch die Aufsicht und höchstens um weitere fünf Jahre möglich (Abs. 3). Aus der Aufbewahrung wird damit ein Vorgang mit zwei Terminen: Ablage und Löschung.

Abbruch und Ablehnung

Lässt sich die Sorgfaltspflicht nicht erfüllen, sind Transaktion und Begründung der Geschäftsbeziehung zu unterlassen, eine bestehende Beziehung ist zu **beenden**; eine Verdachtsmeldung ist zu prüfen (Art. 21 Abs. 1). Notariat, Rechtsberatung, Prüfung und Steuerberatung sind von der Beendigungspflicht ausgenommen, soweit sie die Rechtslage beurteilen oder in einem Verfahren vertreten — nicht jedoch bei Beteiligung an Geldwäsche oder Kenntnis entsprechender Zwecke (Abs. 2).

In jedem Fall sind sämtliche Bemühungen, Entscheidungen und Begründungen zu dokumentieren. **Die Ablehnung muss damit ebenso belegbar sein wie die Annahme**. In der heutigen Praxis werden abgelehnte Anfragen häufig gar nicht erst angelegt.

Meldewesen

Die Meldepflicht bei Verdacht bleibt der Sache nach bestehen (Art. 69), ebenso das Verbot, den Betroffenen zu informieren (Art. 73), und die Pflicht, die Transaktion zunächst zu unterlassen (Art. 71). Für Notariat und Rechtsberatung bleibt der **Weg über eine Selbstverwaltungseinrichtung** zulässig, sofern der Mitgliedstaat ihn vorsieht; diese leitet die Meldung „unverzüglich und ungefiltert“ an die zentrale Meldestelle weiter (Art. 70 Abs. 1). Die Ausnahme für Informationen aus Rechtsberatung und Verfahrensvertretung gilt auch hier (Abs. 2).

Auskunftsfähigkeit über fünf Jahre

Verpflichtete müssen **Systeme vorhalten**, die vollständig und schnell beantworten, ob in den vergangenen fünf Jahren eine Geschäftsbeziehung zu bestimmten Personen bestanden hat und welcher Art sie war. Die Auskunft läuft über sichere Kanäle und vertraulich (Art. 78). Das ist keine Dokumentations-, sondern eine **Auffindbarkeitsanforderung**: Sie gilt für den gesamten Kundenbestand, auch für beendete Geschäftsbeziehungen und lässt sich mit einer reinen Papier- oder Dateiablage kaum erfüllen.

2.9 Organisatorische Pflichten heute und ab 2027

WAS DAS UNTERNEHMEN SELBST VORHALTEN MUSS

Neben den Pflichten je Geschäftsbeziehung steht eine zweite Ebene: Anforderungen an die Organisation. Heute stehen sie im Geldwäschegesetz (§§ 4 bis 9), künftig gibt die Verordnung sie unmittelbar vor — an mehreren Stellen deutlich konkreter.

GEGENSTAND	HEUTE (GWG)	AB 10.07.2027 (AMLR)
Risikomanagement und interne Verfahren	Risikomanagement und interne Sicherungsmaßnahmen; wie das im Einzelnen aussieht, bleibt weitgehend dem Unternehmen überlassen	dokumentierte Grundsätze, Verfahren und Kontrollen mit vorgegebenem Mindestinhalt; interne Prüffunktion vorgesehen (Art. 9)
Unternehmensweite Risikoanalyse	Risikoanalyse zu erstellen und fortzuschreiben; Umfang in der Praxis sehr unterschiedlich	**sechs verbindliche Eingangsgrößen**: Anhänge I–III, EU-Risikobewertung, nationale und sektorale Bewertungen, Veröffentlichungen der Standardsetzer und der AMLA, Informationen der Aufsicht, eigene Kundenbasis. Zusätzlich **Vorabbewertung vor** neuen Produkten, Kanälen, Technologien und Kundensegmenten (Art. 10 Abs. 1)
Verantwortung dafür	Verantwortung beim Unternehmen, Zuordnung national ausgestaltet	erstellt vom **Compliance-Officer**, **genehmigt vom Leitungsorgan**, der Aufsicht auf Verlangen vorzulegen (Abs. 2)
Compliance-Funktionen	**ein** Geldwäschebeauftragter; Bestellpflicht abhängig von Größe, Risiko und aufsichtlicher Anordnung	**zwei** Funktionen: ein **Mitglied des Leitungsorgans** als Compliance-Manager, verantwortlich für Angemessenheit und Ressourcen, sowie ein **Compliance-Officer** mit ausreichend hoher hierarchischer Stellung für das Tagesgeschäft und als Ansprechpartner der Aufsicht (Art. 11 Abs. 1 und 2)
Stellung dieser Personen	Benachteiligungsverbot, aber ohne nähere Regeln	ausdrücklicher **Schutz vor Vergeltung, Diskriminierung und Benachteiligung**; Entscheidungen dürfen nicht durch kommerzielle Interessen beeinflusst werden; **direktes Berichtsrecht** an das Leitungsorgan; Abberufung nur nach vorheriger Anzeige, Meldung an die Aufsicht (Abs. 2, 4, 5)
Berichtswesen	nicht ausdrücklich getaktet	**mindestens jährlicher Bericht** des Compliance-Managers an das Leitungsorgan über die Umsetzung der internen Grundsätze (Abs. 6)
Kleine Unternehmen	Erleichterungen in der Praxis	beide Funktionen dürfen in **einer Person** zusammenfallen, wenn Art, Risiko, Komplexität und Größe es rechtfertigen; bei Einzelpersonen nimmt diese die Aufgaben selbst wahr (Abs. 7)
Schulung und Zuverlässigkeit	Unterrichtung der Beschäftigten, Zuverlässigkeitsprüfung	ausdrücklich geregelt, einschließlich Bewusstsein für die Anforderungen und Prüfung der Zuverlässigkeit (Art. 12, 13)
Auslagerung	zulässig, Verantwortung bleibt beim Unternehmen	zulässig unter Bedingungen; die **Verantwortung bleibt ausdrücklich** beim Verpflichteten (Art. 18)

GEGENSTAND	HEUTE (GWG)	AB 10.07.2027 (AMLR)
Rückgriff auf Dritte	Rückgriff auf Dritte möglich	Rückgriff auf andere Verpflichtete möglich, Verantwortung bleibt; Leitlinien der AMLA angekündigt (Art. 48–50)
Gruppen	gruppenweite Pflichten	gruppenweite Grundsätze, besondere Regeln für Gesellschaften in Drittstaaten (Art. 16, 17)

Die Verantwortung rückt ins Leitungsorgan

Die Aufteilung in **zwei** Compliance-Funktionen verankert die Verantwortung ausdrücklich **im Leitungsorgan**. Geldwäscheprävention ist damit formal keine Aufgabe mehr, die man an eine Stelle delegiert und dann dort belässt. In kleinen Unternehmen bleibt die Zusammenlegung möglich — die Verantwortung des Leitungsorgans bleibt davon jedoch unberührt.

Für Kredit- und Finanzinstitute sowie Anbieter von Kryptowerte-Dienstleistungen treten sektorspezifische Vorschriften hinzu, etwa zu Korrespondenzbeziehungen und zu Transaktionen mit selbstverwalteten Adressen (Art. 36–41).

3 Was noch nicht feststeht

OFFENER STAND DER RECHTSETZUNG

Viele Detailregelungen stehen nicht in der Verordnung selbst, sondern in nachgelagerten Rechtsakten und Leitlinien. Deren Stand ist unterschiedlich weit.

Technische Regulierungsstandards zur Sorgfaltspflicht
Konsultation im Frühjahr 2026 abgeschlossen, Vorlage an die Kommission für Juli 2026 vorgesehen, Annahme steht aus. Sie konkretisieren Dokumenten- und Datenlisten, Fernidentifizierung, Screening und den Übergang für Bestandskunden. **Alle darauf gestützten Aussagen sind in diesem Dokument gelb markiert.**

Rechtsakt zu Sanktionskategorien
Die AMLR nennt **keine Bußgeldhöhen**. Die Sanktionen bleiben den Mitgliedstaaten überlassen; für Verstoßkategorien und Bemessungskriterien ist ein delegierter Rechtsakt vorgesehen (Art. 68). Bezifferte Rahmen ergeben sich erst aus der Richtlinie und deren nationaler Umsetzung.

Zusätzliche PEP-Kategorien
Der delegierte Rechtsakt zu den PEP-Kategorien (Art. 43 Abs. 3) wurde im Oktober 2025 im Rahmen einer allgemeinen Priorisierung der Sekundärrechtsakte zurückgestellt; eine Annahme ist frühestens ab Oktober 2027 vorgesehen. Die Standards zur Sorgfaltspflicht sind davon nicht betroffen.

Leitlinien der AMLA
Angekündigt sind unter anderem Leitlinien zu Risikovariablen, zum Inhalt der unternehmensweiten Risikoanalyse und zur laufenden Überwachung sowie — mit Frist Juli 2027 — zu nahestehenden Personen und zur Risikoabstufung bei politisch exponierten Personen.

Der Zeitplan der offenen Rechtsakte

Die AMLA arbeitet die Detailregelungen in einer Reihe von Konsultationen ab. Der folgende Überblick zeigt den Stand zum Rechtsstand dieses Dokuments und damit, wann mit welcher Konkretisierung zu rechnen ist.

FRIST	GEGENSTAND DER KONSULTATION	STAND	BEZUG IN DIESEM DOKUMENT
27.01.2026	Technische Durchführungsstandards zur Aufsichtsmethodik	abgeschlossen	
09.03.2026	Geldbußen, Verwaltungsmaßnahmen und Zwangsgelder	abgeschlossen	legt **Kriterien und Schweregrade** fest, keine Beträge
08.05.2026	**Sorgfaltspflichten (Art. 28 Abs. 1 AMLR)**	abgeschlossen	die in diesem Dokument gelb markierten Aussagen
08.05.2026	Kriterien für Geschäftsbeziehung und Einzeltransaktion	abgeschlossen	betrifft die Auslöser aus Kapitel 2.1
15.06.2026	Gruppenweite Mindestanforderungen	abgeschlossen	
15.07.2026	Leitlinien zur unternehmensweiten Risikoanalyse	abgeschlossen	konkretisiert Kapitel 2.9
03.09.2026	Leitlinien zur laufenden Überwachung	**läuft**	konkretisiert Kapitel 2.7
20.09.2026	Meldung von Verdachtsfällen	**läuft**	betrifft Kapitel 2.8
27.09.2026	Bewertung des Risikoprofils	**läuft**	betrifft Kapitel 2.6
06.10.2026	Grenzüberschreitender Informationsaustausch	**läuft**	

Stand der Sorgfaltspflichten-Standards

Die Konsultation endete am 8. Mai 2026. Die Vorlage an die Kommission war zum **10. Juli 2026** vorgeschrieben. Eine **Endfassung hat die AMLA bislang nicht veröffentlicht** — maßgeblich und öffentlich zugänglich ist weiterhin die Konsultationsfassung vom 9. Februar 2026, auf der die Angaben dieses Dokuments beruhen. Bis zur Annahme durch die Kommission und der Veröffentlichung im Amtsblatt bleibt der Entwurfscharakter bestehen; erfahrungsgemäß vergehen dafür mehrere Monate.

Der Standard zu Geldbußen und Verwaltungsmaßnahmen regelt **Indikatoren für die Schwere eines Verstoßes und Kriterien für die Bemessung**. Er soll erreichen, dass derselbe Verstoß in allen Mitgliedstaaten gleich bewertet wird. Konkrete Beträge enthält auch er nicht; die ergeben sich erst aus der Richtlinie und ihrer nationalen Umsetzung.

Was daneben läuft: elektronische Identität und Wallet

Neben der Geldwäscheverordnung ändert sich das Recht der elektronischen Identität. Beide Stränge werden häufig vermengt, betreffen aber unterschiedliche Adressaten. Die folgenden Termine gehören **nicht** zur AMLR.

TERMIN	WAS GILT	FÜR WEN
24.12.2026	Die Mitgliedstaaten stellen mindestens ein EUDI-Wallet bereit (Art. 5a Abs. 1 eIDAS)	Pflicht der Staaten, nicht der Unternehmen
10.07.2027	Die AMLR gilt unmittelbar und löst die nationalen Sorgfaltspflichten ab	alle Verpflichteten
24.12.2027	Bestimmte private Unternehmen müssen das Wallet akzeptieren können (Art. 5f Abs. 2 eIDAS)	nur der unten beschriebene Kreis

Beide Fristen der eIDAS-Verordnung laufen ab dem Inkrafttreten der zugehörigen Durchführungsrechtsakte. Diese wurden am 4. Dezember 2024 im Amtsblatt veröffentlicht und traten am zwanzigsten Tag danach in Kraft, also am 24. Dezember 2024. Daraus ergeben sich die 24 und die 36 Monate der Tabelle.

Wen die Pflicht zur Annahme wirklich trifft

Die Pflicht erfasst private Unternehmen nur, wenn sie nach Unionsrecht, nationalem Recht oder vertraglich verpflichtet sind, eine **Online-Identifizierung mit starker Nutzerauthentifizierung** vorzunehmen. Die Verordnung nennt dazu die Bereiche Verkehr, Energie, Bankenwesen, Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Trinkwasser, Postdienste, digitale Infrastrukturen, Bildung und Telekommunikation. **Kleinst- und kleine Unternehmen sind ausdrücklich ausgenommen.** Und auch dort, wo die Pflicht greift, gilt sie nur „auf das freiwillige Verlangen des Nutzers". Für Notariat, Rechtsberatung und Steuerberatung entsteht daraus **keine Pflicht**: Die geldwäscherechtliche Identifizierung ist keine Online-Identifizierung mit starker Nutzerauthentifizierung, und in der Bereichsliste kommen diese Berufe nicht vor.

AUS DEM ENTWURF DES DIGITALE-IDENTITÄTEN-GESETZES

Deutschland schafft mit dem **Digitale-Identitäten-Gesetz** die nationale Grundlage für das EUDI-Wallet. Der Entwurf greift dabei an drei Stellen in das Geldwäschegesetz ein. Erstens sind die Daten der Authentifizierung zu dokumentieren, wenn das Wallet für die Identifizierung genutzt wird (§ 8 Abs. 2 GwG-E). Zweitens gilt das Wallet als zulässiges Identifizierungsmittel, ausdrücklich schon vor dem 10. Juli 2027 (§ 12 Abs. 1 GwG-E). Drittens entfällt die **Referenzüberweisung**. Wer das Wallet einsetzen will, muss sich zuvor als vertrauender Beteiligter **registrieren** lassen. Für die Praxis heißt das: Das Wallet ist eine zusätzliche Möglichkeit mit einer Vorbedingung, keine Pflicht.

ENTWURF, VERABSCHIEDUNG STEHT AUS

Konsequenz für die Planung

Die **Struktur** der Anforderungen steht fest: welche Daten erhoben werden, wer zu prüfen ist, welche Fristen laufen, was dokumentiert werden muss. Offen sind Detailtiefe und einzelne Nachweisformen. Wer heute Prozesse aufsetzt, sollte sie deshalb an der Struktur ausrichten und die Details konfigurierbar halten.

4 Folgen für Prozesse und Systeme

JE KATEGORIE: WAS OHNEHIN NÖTIG IST UND WAS 2027 HINZUKOMMT

Die vorstehenden Kapitel beschreiben Rechtspflichten, keine Produktanforderungen. Nebeneinander gelesen haben fast alle Neuerungen aber eines gemeinsam: Sie haben ein **Datum**, sie **wiederholen sich**, und sie müssen **belegt** werden. Genau das sind Merkmale von Vorgängen, die sich schlecht von Hand und gut systemgestützt führen lassen.

Die Aufstellung folgt den Unterkapiteln 2.1 bis 2.9 aus Kapitel 2 und trennt zwei Dinge: was ein Prozess **ohnehin** leisten muss — auch nach heutigem Recht — und was **ab 2027 hinzukommt**. Nur die rechte Spalte verursacht Umstellungsaufwand.

KAP.	GEGENSTAND	GRUNDANFORDERUNG — GILT AUCH HEUTE	NEU AB 10.07.2027
2.1	**Auslöser und Kundenbegriff**	erkennen, wann eine Prüfung ausgelöst wird; Schwellen im Blick behalten	Bargeld- und Identifizierungsschwellen als Regel abbilden; bei vermittelten Geschäften **zwei verknüpfte Prüfungen** je Vorgang anlegen
2.2	**Identifizierung des Kunden**	Stammdaten strukturiert erfassen, Ausweisdaten prüfen und ablegen	erweiterter Pflichtdatensatz inklusive aller Staatsangehörigkeiten und Nominee-Namen; gelieferte Attribute auf die eigenen Pflichtfelder **abbilden** und je Fall prüfen, welche Felder **ungedeckt** bleiben — getrennt für natürliche und juristische Personen; Anschrift **strukturiert** und Steuernummer als eigene Felder führen, weil beide regelmäßig nachzuerheben sind; je Feld die **Herkunft** speichern; die Wahl des Verfahrens **begründen können**
2.3	**Wirtschaftlich Berechtigte**	Berechtigte erfassen, Struktur dokumentieren, Register abfragen	**Beteiligungsketten rechnen** statt Ebenen erfassen; alle Berechtigten verifizieren; fiktive Berechtigte mit gleicher Tiefe; Registernachweis speichern; **Abweichung erkennen und 14-Tage-Frist überwachen**
2.4	**Zweck und Geschäftstätigkeit**	Zweck der Beziehung festhalten	fünf Pflichtfelder **strukturiert statt als Freitext**; erwartetes Profil so speichern, dass die Überwachung später dagegen prüfen kann
2.5	**Screening**	Abgleich gegen PEP- und Sanktionslisten durchführen und dokumentieren	Screening auf Berechtigte und kontrollierende Personen ausweiten; **Beteiligungen über 50 % aggregieren**; Namensvarianten und Transliteration; **Auslöser** Neulistung und Datenänderung; Reputationsprüfung mit dokumentierter Quelle und menschlicher Letztentscheidung
2.6	**Risikoeinstufung und Prüftiefe**	Kunden nach Risiko einstufen	Einstufung **je Faktor nachvollziehbar** aus den Anhängen ableiten; Erleichterungen je Kundentyp konfigurieren samt Abbruchbedingungen; verstärkte Prüfung **regelbasiert automatisch auslösen**
2.7	**Überwachung und Aktualisierung**	Wiedervorlage führen, Änderungen nachtragen	**ReKYC-Fälligkeit je KYC-Akte** risikoabhängig berechnen und überwachen — mit kürzeren Abständen im mittleren Bereich; Kundenbestand rollierend planen; Ereignisse als zusätzlicher Auslöser neben der Frist
2.8	**Dokumentation und Meldewesen**	Unterlagen vollständig aufbewahren, Meldewege einhalten	ungeschwärzte Ablage einschließlich eID-Daten; **abgelehnte Fälle vollständig dokumentieren**; **Löschung nach Fristablauf automatisch**; **Personensuche über beendete Beziehungen** für die Auskunft an die Meldestelle
2.9	**Organisatorische Pflichten**	Risikoanalyse erstellen, Beauftragten benennen, schulen	Kundenbasis **auswertbar** halten, weil sie verbindliche Eingangsgröße der Risikoanalyse ist; die beiden Compliance-Rollen abbilden; jährliche Berichtspflicht bedienen; Auslagerung und Rückgriff nachweisbar führen

Wo die Schwierigkeit liegt

Keine dieser Fähigkeiten ist für sich genommen anspruchsvoll. Anspruchsvoll ist, dass sie **gleichzeitig und über den gesamten Kundenbestand** vorliegen müssen und dass ihre Einhaltung gegenüber der Aufsicht jederzeit belegbar sein muss. Drei Anforderungen fallen dabei ins Gewicht, weil sie sich mit Ablagen und Wiedervorlagen kaum abbilden lassen. Das sind die **risikoabhängige ReKYC-Fälligkeit je KYC-Akte**, die **Abweichungserkennung gegen das Register samt 14-Tage-Frist** und die **Personensuche über beendete Beziehungen**.

5 Warum der Zeitpunkt zählt

WAS DIE ÄNDERUNGEN ZUSAMMENGENOMMEN BEDEUTEN

Jede Prüfung wird aufwändiger. Bei **Neukunden wirkt das sofort, beim Kundenbestand mit Verzögerung**.

Erstens: Der Aufwand je Prüfung steigt

Sieben Änderungen aus den vorstehenden Kapiteln wirken unmittelbar auf den Aufwand je Prüfung:

AUFWANDSTREIBER	HEUTE	AB 10.07.2027	KAP.
Zu verifizierende Personen	eine handelnde Person; Berechtigte nur dem Namen nach	**alle** wirtschaftlich Berechtigten, jeweils mit Ausweisnummer im Datensatz	2.3
Ermittlung der Berechtigten	Beteiligung meist auf der obersten Ebene abgelesen	jede Ebene durchrechnen, parallele Stränge addieren, Kontrolle gesondert prüfen	2.3
Angaben zur Beziehung	Kurznotiz zum Zweck, häufig Freitext	**fünf Pflichtangaben**, darunter Herkunft *und* Verwendung der Mittel	2.4
Prüfungen je Vorgang	eine	bei vermittelten Geschäften **zwei** — beide Parteien sind Kunde	2.1
Screening	in der Praxis meist der Vertragspartner	Kunde, Berechtigte und kontrollierende Personen; Wiederholung bei jeder Listenänderung	2.5
Registerarbeit	Abfrage des Registers	Pflichtabgleich, Registernachweis je neuer Geschäftsbeziehung, **14-Tage-Frist** bei Abweichung	2.3
Nachweis	Akten nach nationalem Verständnis	ungeschwärzt, fünf Jahre, danach Löschpflicht — **auch für abgelehnte Fälle**	2.8

Keine dieser Änderungen ist für sich genommen groß. In der Summe verlängern sie jedoch jede einzelne Prüfung — und zwar dauerhaft, nicht einmalig.

Zweitens: Für Neukunden gibt es keine Übergangsfrist

Wer ab dem 10. Juli 2027 eine Geschäftsbeziehung begründet, muss sie **von Beginn an** nach dem vollen Pflichtenprogramm bearbeiten — mit allen Datenfeldern, allen zu verifizierenden Personen und der vollständigen Dokumentation. Der erhöhte Aufwand fällt damit ab der ersten neuen Prüfung in voller Höhe an.

Drittens: Jede KYC-Akte im Kundenbestand muss auf den neuen Stand

Für den Kundenbestand gelten die Aktualisierungs-Fristen aus Kapitel 2.7: ein Jahr bei hohem Risiko, maximal bis zu fünf Jahren bei niedrigem Risiko. Es gibt **keinen Stichtag**, zu dem alles fertig sein müsste — die Fristen laufen je Geschäftsbeziehung und damit rollierend.

> AUS DEM ENTWURF DER TECHNISCHEN REGULIERUNGSSTANDARDS
>
> Der Wortlaut ist hier genau zu lesen: Für Kunden, deren Geschäftsbeziehung vor Veröffentlichung der Delegierten Verordnung begründet wurde, sind Unterlagen, Daten und Informationen **„in Einklang mit den Anforderungen dieser Verordnung und der Verordnung (EU) 2024/1624 zu bringen“** — risikobasiert, in jedem Fall aber innerhalb der Fristen des Artikels 26 Absatz 2. Nach der Begründung des Entwurfs beginnen diese Fristen für den Kundenbestand erst mit dem Anwendungsbeginn der Delegierten Verordnung. ENTWURF, ANNAHME STEHT AUS

Die Frist ist damit **keine Schonfrist, sondern eine Nachziehpflicht**. Am Ende der Frist muss die KYC-Akte des Bestandskunden dem AMLR-Standard entsprechen — mit allen Pflichtfeldern, allen verifizierten wirtschaftlich Berechtigten und dem Registernachweis. Dieses Nachziehen ist ReKYC.

Was daraus nicht folgt

Es gibt **keinen Stichtag für den Kundenbestand**. Die Verordnung sieht ausdrücklich vor: ein Jahr bei hohem Risiko, maximal bis zu fünf Jahren bei niedrigem Risiko (Art. 26 Abs. 2). Wer mit einem Stichtag argumentiert, wird beim ersten Nachfragen widerlegt.

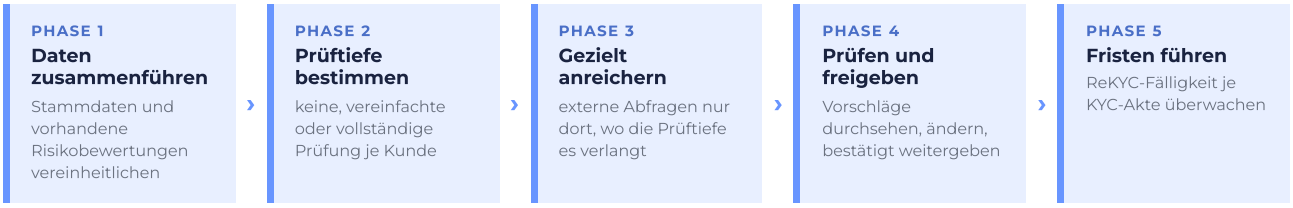
Und eine Prüfung nach heutigem Recht **ersetzt die spätere Aktualisierung nicht**. Wer einen Bestandskunden 2026 nach dem Geldwäschegesetz prüft, muss dessen Daten später trotzdem auf den AMLR-Stand bringen. Vorziehen spart die Aktualisierung nicht — es verändert nur, wie umfangreich sie ausfällt.

Damit ist die Frage nicht mehr, *ob* und *wann* der Kundenbestand nachgezogen werden muss, sondern **wie**.

6 ReKYC — Wie Sie vorgehen

VORGEHEN IN FÜNF PHASEN

Wie tief geprüft werden muss, ist von Kunde zu Kunde verschieden. Die Frist hängt am Risiko (Art. 26 Abs. 2), und das Nachziehen ist ausdrücklich **risikobasiert** vorgesehen. Ein Kundenbestand mit 500 KYC-Akten erfordert also keine 500 Vollprüfungen. Die fünf Phasen dieses Kapitels beschreiben das ReKYC-Vorgehen; sie sind so angeordnet, dass von Phase zu Phase weniger KYC-Akten zu bearbeiten bleiben.



Von Phase zu Phase bleiben weniger KYC-Akten übrig: Wird eine Akte in Phase 2 als aktuell und risikoarm eingestuft, ist sie dokumentiert abgeschlossen — die Phasen 3 und 4 entfallen für sie.

PHASE	WAS ZU TUN IST	WARUM AN DIESER STELLE	KAP.
1	**Bestandsdaten zusammenführen und je Kunde ein Risikoprofil bilden** Stammdaten und vorhandene Risikobewertungen aus den Quellsystemen zusammenführen und vereinheitlichen, sodass für jeden Kunden ein vergleichbares Profil entsteht.	Ohne einheitliche Datenbasis lässt sich weder die Prüftiefe bestimmen noch der Aufwand schätzen. Diese Phase kommt ohne externe Abfragen aus und kostet daher wenig.	2.3, 2.6
2	**Prüftiefe je Kunde bestimmen** Anhand definierter Kriterien entscheiden, wer keine, eine vereinfachte oder eine vollständige Prüfung benötigt: Risikoklasse, Alter der letzten Prüfung, Treffer aus dem Screening, Registeränderungen, Branche, Land, Komplexität der Struktur.	Das Nachziehen des Kundenbestands ist ausdrücklich risikobasiert vorgesehen; an dieser Einstufung hängt der Aufwand aller folgenden Phasen.	2.6, 2.7
3	**Externe Abfragen erst auslösen, wenn die vorhandenen Daten nicht ausreichen** Zuerst mit dem arbeiten, was vorliegt. Register- und Datenabfragen nur dort auslösen, wo die Prüftiefe es verlangt — und in dem Umfang, der zum Risiko passt.	Externe Abfragen sind der teuerste Teil der Aktualisierung. Wer sie pauschal auslöst, zahlt auch für Kunden, bei denen sich nichts geändert hat.	2.3, 2.5
4	**Ergebnisse durchsehen und gezielt auslösen** Die vorgeschlagene Prüftiefe je Kunde in einer Übersicht durchgehen. Wo die Einschätzung nicht passt, wird sie von Hand geändert — ein Kunde kann also von „vereinfacht“ auf „vollständig“ hochgestuft werden oder umgekehrt. In die Bearbeitung geht nur, was bestätigt wurde.	Die Einstufung muss gegenüber der Aufsicht begründbar bleiben. Dazu gehört, dass ein Mensch sie nachvollziehen und ändern kann.	2.6, 4
5	**Fälligkeitsdaten führen** Je KYC-Akte ein Datum, risikoabhängig berechnet und überwacht.	Ab hier ist die Aktualisierung Routine statt Projekt — und gegenüber der Aufsicht belegbar.	2.7, 4

Phase 1 und 2 kommen ohne externe Abfragen aus. Sind sie abgeschlossen, wissen Sie, bei wie vielen KYC-Akten eine vollständige Prüfung nötig ist und bei wie vielen nicht. Erfahrungsgemäß betrifft die vollständige Prüfung nur einen

kleinen Teil des Kundenbestands — und je genauer die Einstufung in Phase 2 ausfällt, desto kleiner wird dieser Teil.

Daneben: der Prozess für Neukunden

Die fünf Phasen betreffen den Kundenbestand. Unabhängig davon ist der Prozess für Neukunden vor dem Stichtag umzustellen — Datenfelder, Verifizierungswege, Screening-Auslöser und Dokumentation. Für Neukunden gibt es keine Übergangsfrist; wer den Prozess erst im Juli 2027 baut, baut ihn unter Last.

LEITGEDANKE

AMLR 2027 betrifft Neu- und Bestandskunden. Jetzt starten. Aber auf zwei verschiedenen Wegen.

Ab dem 10. Juli 2027 wird jede KYC-Prüfung aufwändiger: mehr Daten, mehr Personen, mehr Nachweise. Für **Neukunden** gibt es keine Übergangsfrist. Im **Kundenbestand** bekommt jede **KYC-Akte** ein **Fälligkeitsdatum** — ein Jahr bei hohem Risiko, maximal bis zu fünf Jahren bei niedrigem Risiko. Wie tief geprüft wird, bestimmt das Risiko. Wieviel Aufwand mit der Prüfung verbunden ist, entscheidet die vorhandene Datenqualität. Ein **intelligenter, abgestufter ReKYC-Prozess** berücksichtigt das und optimiert Kosten und Aufwand. **Damit beginnen Phase 1 und 2.**

A Anhang: Abkürzungen, Vorschriften und Quellen

BEGRIFFSKLÄRUNG UND BELEGE

Abkürzungen

KÜRZEL	BEDEUTUNG
AMLA	*Authority for Anti-Money Laundering* — die europäische Geldwäschebehörde mit Sitz in Frankfurt am Main, errichtet durch Verordnung (EU) 2024/1620. Entwirft die technischen Standards und Leitlinien.
AMLD6	Sechste Geldwäscherichtlinie, Richtlinie (EU) 2024/1640. Anders als die Verordnung **national umzusetzen**; regelt vor allem Aufsicht, Register und Sanktionen.
AMLR	*Anti-Money Laundering Regulation* — die EU-Geldwäscheverordnung, Verordnung (EU) 2024/1624. Gilt unmittelbar ab dem 10. Juli 2027, ohne deutsches Umsetzungsgesetz.
AWG / AWV	Außenwirtschaftsgesetz und Außenwirtschaftsverordnung — Grundlage der Finanzsanktionen neben den unmittelbar geltenden EU-Sanktionsverordnungen (Kapitel 2.5).
CDD	*Customer Due Diligence* — die Sorgfaltspflichten gegenüber Kunden, also der Gegenstand der Kapitel 2.1 bis 2.8.
DIdG	Digitale-Identitäten-Gesetz — das deutsche Gesetz, das die nationale Grundlage für das EUDI-Wallet schafft und dabei das Geldwäschegesetz ändert. **Noch im Gesetzgebungsverfahren** (Kapitel 3).
DSGVO	Datenschutz-Grundverordnung, Verordnung (EU) 2016/679 — maßgeblich für die Grenzen der Datenverarbeitung nach Artikel 76 AMLR (Kapitel 2.5).
EDD	*Enhanced Due Diligence*, verstärkte Sorgfaltspflichten (Kapitel 2.6).
eID	*electronic identification means*, elektronisches Identifizierungsmittel nach eIDAS — mit den Sicherheitsniveaus „substanziell“ (*substantial*) und „hoch“ (*high*).
eIDAS	Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste.
EUDI-Wallet	*European Digital Identity Wallet*, in der deutschen Fassung der Verordnung „europäische Brieftasche für die Digitale Identität“ — die von den Mitgliedstaaten bereitzustellende Anwendung, in der geprüfte Identitätsdaten und Bescheinigungen gehalten und geteilt werden. **Von der AMLR nicht vorgeschrieben** (Kapitel 3).
FATF	*Financial Action Task Force* — internationaler Standardsetzer für die Geldwäschebekämpfung; ihre Länderlisten sind Anknüpfungspunkt für geografische Risikofaktoren.
FIU	*Financial Intelligence Unit* — die zentrale Meldestelle, an die Verdachtsmeldungen gehen. **Jeder Mitgliedstaat hat eine eigene**, und sie sind institutionell unterschiedlich angebunden; **in Deutschland beispielsweise** ist sie bei der Generalzolldirektion angesiedelt, anderswo bei der Zentralbank, der Aufsicht oder der Polizei.
GwG	Geldwäschegesetz — das geltende deutsche Recht, mit dem in diesem Dokument verglichen wird.
ITS	*Implementing Technical Standards*, technische Durchführungsstandards. Wie RTS, aber als Durchführungsrechtsakt; regeln vor allem Formate, Vorlagen und Verfahren.
KYC	*Know Your Customer* — Sammelbegriff für die Prüfschritte, mit denen ein Verpflichteter seinen Kunden feststellt und einschätzt.
LEI	*Legal Entity Identifier* — die international einheitliche Kennnummer für Unternehmen und andere juristische Personen.
PEP	*Politically Exposed Person*, politisch exponierte Person (Kapitel 2.5).
QEAA	*Qualified Electronic Attestation of Attributes*, qualifizierte elektronische Attributsbescheinigung nach eIDAS — die Bescheinigung einzelner geprüfter Merkmale einer Person, etwa Steuernummer oder Anschrift. Geeignet, um Lücken im Pflichtdatensatz zu schließen (Kapitel 2.2).
QES	qualifizierte elektronische Signatur. **Nicht Gegenstand der AMLR** — die Verordnung regelt die

KÜRZEL	BEDEUTUNG
	Identitätsprüfung, nicht die Unterschrift. Das Wort kommt im Verordnungstext nicht vor.
QTSP	*Qualified Trust Service Provider*, Anbieter qualifizierter Vertrauensdienste nach eIDAS (Kapitel 2.2).
ReKYC	*Re-Know Your Customer* — die wiederkehrende KYC-Prüfung: Praxisbegriff für die Aktualisierungspflicht (Art. 26 Abs. 2). Die bestehende KYC-Akte wird erneut geprüft und auf den geforderten Stand gebracht (Kapitel 2.7 und 6).
RTS	*Regulatory Technical Standards*, technische Regulierungsstandards. Von der AMLA entworfen, von der Europäischen Kommission als **Delegierte Verordnung** angenommen — danach unmittelbar geltendes Recht. Solange sie nicht angenommen sind, sind sie Entwurf; in diesem Dokument gelb markiert.
SDD	*Simplified Due Diligence*, vereinfachte Sorgfaltspflichten bei nachgewiesen niedrigem Risiko (Kapitel 2.6).
wB / UBO	wirtschaftlich Berechtigter, englisch *Ultimate Beneficial Owner* — die natürliche Person, der ein Kunde letztlich gehört oder die ihn kontrolliert (Kapitel 2.3).

Herangezogene Vorschriften und Quellen

Verordnung (EU) 2024/1624 (AMLR) — Art. 2 (Begriffe, politisch exponierte Personen), 3 (Verpflichtete), 9–13 (interne Organisation, Compliance-Funktionen, Schulung, Zuverlässigkeit), 10 (unternehmensweite Risikoanalyse), 16–18 (Gruppen, Auslagerung), 19 (Anlässe, Kundenbegriff), 20 (Sorgfaltspflichten), 21 (Abbruch der Prüfung), 22 (Identifizierung und Verifizierung), 23 (Zeitpunkt, Registernachweis), 24 (Unstimmigkeitsmeldung), 25 (Zweck und Art), 26 (laufende Überwachung, Fristen), 27 (Sanktionen der Vereinten Nationen), 33 (vereinfachte Sorgfalt), 34 (verstärkte Sorgfalt), 42–46 (politisch exponierte Personen), 48–50 (Rückgriff auf Dritte), 51–54 (wirtschaftlich Berechtigte), 62–63 (Angaben und Pflichten juristischer Personen), 68 (Sanktionen), 69–73 (Meldewesen), 76 (Datenverarbeitung), 77–78 (Aufbewahrung, Auskunft), 80 (Bargeld); Anhänge I–III.

Weitere Rechtsakte: Richtlinie (EU) 2024/1640; Verordnung (EU) 2024/1620; Verordnung (EU) Nr. 910/2014 (eIDAS); EU-Sanktionsverordnungen sowie §§ 4 und 6 Außenwirtschaftsgesetz.

Nationales Recht: Geldwäschegesetz, insbesondere §§ 2, 4 bis 9 sowie § 11 Abs. 5 und 6.

Ergänzende Dokumente: Entwurf der technischen Regulierungsstandards der AMLA zu Artikel 28 Absatz 1 AMLR (Konsultationsfassung vom 9. Februar 2026 — zum Rechtsstand dieses Dokuments die aktuellste veröffentlichte Fassung; eine Endfassung liegt nicht vor); Merkblatt der Deutschen Bundesbank zur Einhaltung von Finanzsanktionen (Juni 2024); Leitlinien des Rates zur Umsetzung restriktiver Maßnahmen (Fassung Juli 2024); Amtsblattmitteilung zu wichtigen öffentlichen Ämtern.

Dieses Dokument gibt den Rechtsstand August 2026 wieder und dient der fachlichen Information; es ersetzt keine rechtliche Beratung im Einzelfall. Aussagen, die auf noch nicht angenommenen Rechtsakten beruhen, sind als Entwurfsstand gekennzeichnet. Bußgeldhöhen werden nicht genannt, da die Verordnung keine Beträge festlegt.