Bersch Consulting

EXECUTIVE WHITEPAPER

Das neue EU-AML-Paket

Der Transformationsfahrplan für Banken bis zum 10. Juli 2027

Wie Governance, Customer Due Diligence, Beneficial Ownership, Sanktionen, Kontrollen und Technologie auf die neuen europäischen AML-Anforderungen ausgerichtet werden müssen

Executive Advisory Paper für Banken und Finanzinstitute

Inhalt

Executive Summary

Mit dem neuen EU-AML-Paket verändert Europa nicht nur einzelne Vorschriften zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung. Es verändert die Architektur, nach der AML-Compliance reguliert, beaufsichtigt und innerhalb von Finanzinstituten operationalisiert wird.

Im Mittelpunkt steht ein stärker harmonisiertes europäisches Regelwerk. Die EU-AML-Verordnung bringt zentrale Verpflichtungen unmittelbar auf europäische Ebene. Die sechste Geldwäscherichtlinie ordnet unter anderem nationale Aufsicht, Financial Intelligence Units und Register neu. Mit der Anti-Money Laundering Authority – AMLA – entsteht zugleich eine europäische Behörde, die Aufsichtskonvergenz, technische Standards, Leitlinien und künftig auch die direkte Beaufsichtigung ausgewählter Finanzunternehmen prägt. Die Geldtransferverordnung ergänzt dieses System insbesondere für Transfers von Kryptowerten. Gemeinsam bilden diese vier Rechtsakte den Kern des neuen europäischen AML/CFT-Rahmens.

Für Banken bedeutet diese Entwicklung nicht, dass das bestehende AML-System vollständig ersetzt wird. Wesentliche Grundprinzipien – insbesondere der risikobasierte Ansatz und die Systematik allgemeiner, vereinfachter und verstärkter Sorgfaltspflichten – bleiben erhalten. Gleichzeitig werden jedoch zahlreiche Anforderungen detaillierter, verbindlicher und stärker miteinander verzahnt.

Besonders relevant sind Veränderungen bei:

- Governance und Management-Verantwortung,
- unternehmensweiter Risikoanalyse,
- Customer Due Diligence und KYC-Daten,
- Ermittlung wirtschaftlich Berechtigter,
- AML- und Sanktionsschnittstellen,
- Monitoring und Verdachtsmeldewesen,
- Outsourcing und gruppenweiten Prozessen,
- Datenhaltung, Aufbewahrung und Registermeldungen.

Diese Veränderungen greifen tief in bestehende Operating Models ein. Richtlinien allein werden deshalb nicht ausreichen. Institute müssen überprüfen, ob ihre Prozesse, Rollen, Datenmodelle, Systeme, Kontrollen, Dienstleisterstrukturen und Management-Informationen tatsächlich in der Lage sind, die neuen Anforderungen End-to-End zu erfüllen.

Der entscheidende Fixpunkt ist der 10. Juli 2027. Ab diesem Datum gilt die EU-AML-Verordnung grundsätzlich unmittelbar (Art. 90 AMLR). Die AMLD6 ist grundsätzlich bis zum 10. Juli 2027 in nationales Recht umzusetzen; für einzelne Vorschriften gelten abweichende Umsetzungsfristen (Art. 78 AMLD6).

Damit ergibt sich eine klare Management-Implikation:

Der 10. Juli 2027 ist kein Starttermin für die Transformation. Er ist der Termin, zu dem die Transformation operativ funktionieren muss.

Banken, die erst kurz vor dem Stichtag Richtlinien aktualisieren, riskieren, die eigentliche Komplexität zu unterschätzen. Denn wesentliche Änderungen können KYC-Datenfelder, Beneficial-Ownership-Logiken, Screening-Populationen, Risikoscoring, Monitoring, Archivierung, Outsourcing und gruppenweite Informationsflüsse betreffen.
Ein belastbares Transformationsprogramm muss deshalb drei Fragen beantworten:

DREI LEITFRAGEN

1. **Was verändert sich regulatorisch?**
2. **Welche Auswirkungen hat das auf unser bestehendes Operating Model?**
3. **Welche Änderungen müssen bis zum 10. Juli 2027 umgesetzt, getestet und nachgewiesen sein?**

1 Warum das neue EU-AML-Paket mehr ist als eine regulatorische Anpassung

Das bisherige europäische AML-Framework basiert in wesentlichen Teilen auf Richtlinien, die von den Mitgliedstaaten in nationales Recht umgesetzt werden. Diese Struktur hat über Jahre zu unterschiedlichen Auslegungen, unterschiedlichen Aufsichtspraktiken und teilweise fragmentierten nationalen Anforderungen geführt.

Das neue EU-AML-Paket verfolgt bewusst einen stärkeren Harmonisierungsansatz.

Die EU-AML-Verordnung soll gemeinsam mit technischen Standards und Leitlinien ein europäisches Single Rulebook schaffen. Gleichzeitig erhält AMLA eine zentrale Rolle bei der Standardsetzung und bei der Konvergenz der Aufsicht. Ziel ist ein europaweit konsistenteres AML/CFT-Framework mit stärker harmonisierten Anforderungen und einer einheitlicheren Anwendung.

Diese Harmonisierung verändert die Implementierungslogik.

Für Institute reicht es künftig weniger aus, nationale Anforderungen isoliert zu betrachten. Richtlinien, Prozesse und Kontrollen müssen zunehmend gegen ein europäisches Regelwerk und dessen Level-2-Konkretisierung ausgerichtet werden.

RTS, ITS und AMLA-Leitlinien konkretisieren den Level-1-Rechtsrahmen. Stand 17. August 2026 sind zentrale CDD-, Geschäftsbeziehungs- und Gruppen-RTS noch nicht final veröffentlicht; Leitlinien zum laufenden Monitoring und die ITS zum Verdachtsmeldeformat befinden sich noch in Konsultation. Entwürfe werden hier nur als Entwicklungsstand berücksichtigt.

Damit verändert sich auch die Art regulatorischer Transformation.

> **DIE ZENTRALE HERAUSFORDERUNG LAUTET NICHT**
>
> *„Welche Paragraphen müssen wir in unseren Richtlinien ändern?“*
>
> **SONDERN**
>
> **„Welche Teile unseres AML Operating Models müssen verändert werden, damit die neuen Anforderungen in der täglichen Praxis zuverlässig funktionieren?“**

Diese Unterscheidung ist entscheidend.

Eine regulatorisch korrekte Richtlinie, die technisch nicht ausführbar ist, ist kein belastbares Kontrollmodell. Eine neue KYC-Pflicht, für die das Kundendatenmodell kein entsprechendes Feld besitzt, erzeugt manuelle Workarounds. Eine zusätzliche Screening-Anforderung ohne vollständige Eigentums- und Kontrolldaten erzeugt Kontrolllücken. Eine neue Management-Verantwortung ohne geeignetes Berichtswesen bleibt formal statt wirksam.

Das EU-AML-Paket ist deshalb nicht nur ein Compliance-Projekt.

Es ist für viele Banken ein Operating-Model-, Daten- und Technologie-Transformationsprogramm.

2 Das neue europäische AML-System und der Stichtag 10. Juli 2027

Die vier Komponenten des EU-AML-Pakets greifen ineinander.

AMLA-Verordnung

Mit AMLA entsteht eine neue europäische Aufsichts- und Koordinierungsbehörde mit Sitz in Frankfurt.

Zu den zentralen Aufgaben der AMLA gehören insbesondere:

- die Koordination nationaler Aufsichtsbehörden,
- die Förderung einheitlicher Aufsichtsmethoden,
- die Zusammenarbeit mit den nationalen FIUs,
- die Entwicklung technischer Standards,
- die Veröffentlichung von Leitlinien und Empfehlungen,
- sowie künftig die direkte Aufsicht über ausgewählte Unternehmen des Finanzsektors.

AMLA beginnt den ersten Auswahlprozess für direkt beaufsichtigte Verpflichtete am 1. Juli 2027 und schließt ihn innerhalb von sechs Monaten ab. Die direkte Aufsicht über die ausgewählten Verpflichteten beginnt sechs Monate nach Veröffentlichung der ersten Auswahlliste (Art. 13 AMLAR).

Auch Institute, die nicht unmittelbar durch AMLA beaufsichtigt werden, sind jedoch betroffen. Standards, Leitlinien und die stärkere Konvergenz nationaler Aufsicht wirken wesentlich breiter.

EU-AML-Verordnung

Die EU-AML-Verordnung bildet den operativen Kern des neuen Regelwerks für Verpflichtete.

Sie umfasst unter anderem:

- internes Risikomanagement,
- Richtlinien, Verfahren und Kontrollen,
- gruppenweite Pflichten,
- Customer Due Diligence,
- wirtschaftlich Berechtigte,
- PEPs,
- verstärkte und vereinfachte Sorgfaltspflichten,
- gezielte finanzielle Sanktionen,
- Outsourcing,
- Verdachtsmeldungen,
- Aufzeichnung und Aufbewahrung.

Die EU-AML-Verordnung gilt grundsätzlich ab dem 10. Juli 2027 unmittelbar in den Mitgliedstaaten (Art. 90 AMLR).

AMLD6

Die sechste Geldwäscherichtlinie adressiert insbesondere die institutionelle Infrastruktur der Mitgliedstaaten. Dazu gehören nationale Aufsichtsbehörden, FIUs, Transparenz- und weitere Register.

Die AMLD6 ist grundsätzlich bis zum 10. Juli 2027 in nationales Recht umzusetzen. Art. 78 AMLD6 sieht für einzelne Vorschriften abweichende Fristen vor.

Geldtransferverordnung

Die Neufassung der Geldtransferverordnung erweitert AML-bezogene Anforderungen auf Kryptowerte-Transaktionen und bildet damit eine wichtige Schnittstelle zwischen klassischer Financial-Crime-Compliance und Digital Assets.

> **MANAGEMENT-IMPLIKATION**
>
> Die vier Rechtsakte sollten aus Sicht eines Instituts nicht als vier unabhängige regulatorische Projekte behandelt werden.
>
> Gemeinsam verändern sie:
>
> **Regelwerk → Aufsicht → Governance → Prozesse → Daten → Kontrollen → Nachweise.**
>
> Genau diese End-to-End-Perspektive sollte deshalb auch das Transformationsprogramm bestimmen.

3 Sieben strukturelle Veränderungen für Banken

3.1 Governance und Management-Verantwortung werden konkreter

Die EU-AML-Verordnung differenziert künftig ausdrücklich zwischen Verantwortlichkeiten auf Leitungsebene und der Funktion des Geldwäschebeauftragten.

Art. 11 AMLR ordnet die Compliance-Funktionen klarer zu: Verpflichtete benennen grundsätzlich einen Compliance-Manager aus dem Leitungsorgan in seiner Leitungsfunktion und einen Geldwäschebeauftragten für die tägliche Umsetzung der AML/CFT-Anforderungen. Geschäftsleitung und Aufsichtsorgan werden zugleich über die Art. 10 und 11 stärker in Risikoanalyse, Genehmigung, Ressourcenausstattung, Berichterstattung und Aufsicht eingebunden.

Besonders relevant ist die unternehmensweite Risikoanalyse: Sie soll weiterhin vom Geldwäschebeauftragten erstellt und dokumentiert werden, künftig aber durch die Geschäftsleitung genehmigt und auch dem Aufsichtsorgan übermittelt werden. Für Gruppen soll sie vom Mutterunternehmen gruppenweit erstellt werden und dabei auch Gruppenunternehmen berücksichtigen, die selbst keine Verpflichteten sind.

Parallel steigen die Berichts- und Steuerungsanforderungen. Der Compliance-Manager berichtet dem Leitungsorgan regelmäßig und mindestens jährlich über die Umsetzung der internen Strategien, Verfahren und Kontrollen. Der Geldwäschebeauftragte muss direkt an das Leitungsorgan in seiner Leitungsfunktion und – sofern vorhanden – in seiner Aufsichtsfunktion berichten und Bedenken unabhängig adressieren können (Art. 11 AMLR).

Damit wird AML noch stärker zu einer Frage institutioneller Verantwortlichkeit.

Für Banken ergeben sich daraus konkrete Prüfbereiche:

> **Governance**
> Sind Vorstand, Compliance Manager, Geldwäschebeauftragter, erste Verteidigungslinie und Aufsichtsorgan klar voneinander abgegrenzt?
>
> **Entscheidungsrechte**
> Wer genehmigt Risikoanalyse, Richtlinien, Verfahren und Kontrollen?
>
> **Management-Informationen**
> Erhält das Management ausreichend Informationen über Risiken, Kontrollwirksamkeit, Feststellungen und Remediation?
>
> **Eskalation**
> Sind Warn-, Eskalations- und Entscheidungswege dokumentiert und tatsächlich nutzbar?

Die entscheidende Veränderung liegt deshalb nicht nur in zusätzlichen Aufgaben.

Sie liegt in der Nachweisbarkeit von Verantwortung.

3.2 Customer Due Diligence bleibt im Kern vertraut – wird aber granularer

Die Grundsystematik der Sorgfaltspflichten bleibt bestehen: allgemeine, vereinfachte und verstärkte Sorgfaltspflichten sowie ein risikobasierter Ansatz.

Gleichzeitig werden einzelne Anforderungen wesentlich detaillierter.

Art. 20 der EU-AML-Verordnung umfasst unter anderem:

- Identifizierung des Kunden,
- Ermittlung und Identifizierung des wirtschaftlich Berechtigten,
- Verständnis von Zweck und angestrebter Art der Geschäftsbeziehung,
- Prüfung gezielter finanzieller Sanktionen,
- kontinuierliche Überwachung,
- PEP-Prüfung,

- Identifizierung eines Veranlassers,
- und die Identifizierung bestimmter für den Kunden handelnder Personen.

Auch die KYC-Datensätze werden konkreter.

Für natürliche Personen verlangt Art. 22 AMLR unter anderem Namen, Geburtsort und vollständiges Geburtsdatum, Staatsangehörigkeiten sowie den gewöhnlichen Aufenthaltsort; weitere Identifikationsmerkmale sind je nach Verfügbarkeit beziehungsweise Anwendbarkeit zu erfassen. Für juristische Personen gehören unter anderem Rechtsform und Name, Sitzanschrift, Gründungsstaat, gesetzliche Vertreter sowie vorhandene Register-, Steuer- oder Rechtsträgerkennungen zum Datensatz.

Das klingt zunächst wie eine Detailanpassung.

Operativ kann daraus jedoch erheblicher Aufwand entstehen.

Denn zusätzliche Informationen betreffen nicht nur das Onboarding. Sie können Auswirkungen haben auf:

- Kundendatenmodelle,
- Pflichtfelder,
- Dokumentenlogik,
- Verifikationsverfahren,
- Schnittstellen,
- Datenqualität,
- Bestandskunden,
- Screening,
- Monitoring,
- Archivierung.

Besonders relevant ist deshalb der Kundenbestand. Die CDD-Anforderungen werden durch den RTS nach Art. 28 Abs. 1 AMLR weiter konkretisiert. AMLA hat hierzu vom 9. Februar bis 8. Mai 2026 einen überarbeiteten Entwurf konsultiert; in der AMLA-Instrumentenübersicht mit Stand 21. Juli 2026 wird dieser RTS weiterhin mit dem Status „Konsultation geschlossen“ und noch nicht mit einem veröffentlichten Abschlussbericht geführt. Für die Umsetzungsplanung sollte deshalb klar zwischen bereits verbindlichen Level-1-Anforderungen und noch nicht finalisierten Level-2-Details unterschieden werden. Schon der Level-1-Rechtsrahmen macht jedoch deutlich, dass Datenhaushalt, Verifikation, Beneficial Ownership, Screening und Aktualisierungsprozesse frühzeitig auf Umsetzungsfähigkeit geprüft werden müssen.

> **MANAGEMENT-IMPLIKATION**
>
> Die entscheidende Frage lautet nicht:
>
> *„Welche neuen Daten müssen wir erheben?“*
>
> Sondern:
>
> **„Welche Daten fehlen heute, bei wie vielen Kunden fehlen sie, wo werden sie gespeichert und welche nachgelagerten Prozesse hängen davon ab?“**

3.3 Beneficial Ownership wird zu einem Rechts-, Prozess- und Datenthema

Die Ermittlung wirtschaftlich Berechtigter gehört zu den Bereichen mit besonders hohem Umsetzungspotenzial.

Die EU-AML-Verordnung differenziert Eigentum und Kontrolle und enthält detaillierte Vorgaben für mehrstufige Beteiligungs- und Kontrollstrukturen. Die Art. 51 ff. AMLR verlangen, Eigentums- und Kontrollwege nachvollziehbar zu bestimmen und die letztlich wirtschaftlich berechtigten natürlichen Personen zu ermitteln. Damit steigt insbesondere bei komplexen Gesellschafts- und Beteiligungsstrukturen die Bedeutung einer konsistenten Daten- und Nachweislogik.

Zugleich wird die Figur des wirtschaftlich Berechtigten klarer von anderen Rollen getrennt.

Der sogenannte Veranlasser wird als eigenständige CDD-Rolle behandelt. Kann nach Ausschöpfung aller Identifizierungsmöglichkeiten kein wirtschaftlich Berechtigter ermittelt werden und bestehen keine Verdachtsgründe, sind nach Art. 63 Abs. 4 AMLR Angaben zu den Senior Managing Officials zu erfassen; diese Personen werden dadurch jedoch nicht selbst zu wirtschaftlich Berechtigten.

Für Institute entsteht damit eine komplexe Umsetzungskette:

Eigentumsstruktur verstehen → Kontrolle verstehen → relevante Personen ermitteln → Daten erheben → verifizieren → screenen → dokumentieren → laufend aktualisieren

Eine Schwäche an einer Stelle wirkt sich unmittelbar auf nachgelagerte Kontrollen aus.

Wenn beispielsweise eine Eigentumsstruktur nicht vollständig im Kernsystem abbildbar ist, können daraus insbesondere folgende Probleme entstehen:

- PEP-Screening,
- Sanktions-Screening,
- Kundenrisikoeinstufung,
- Laufende Überwachung,
- Transparenzregister-Prozessen,
- Kontenregistermeldungen

Beneficial Ownership darf deshalb nicht als isolierte juristische Definitionsfrage behandelt werden.

Es ist ein Thema des End-to-End-Kontrolldesigns.

3.4 AML und gezielte finanzielle Sanktionen rücken enger zusammen

Eine der sichtbarsten inhaltlichen Veränderungen ist die stärkere Einbindung gezielter finanzieller Sanktionen in AML-Prozesse.

Die EU-AML-Verordnung bindet Risiken der Nichtumsetzung oder Umgehung gezielter finanzieller Sanktionen ausdrücklich in Risikomanagement, interne Strategien, Verfahren und Kontrollen sowie in die Customer Due Diligence ein (insbesondere Art. 9, 10 und 20 AMLR).

Wichtig ist dabei die Abgrenzung:

Dabei bleibt die rechtliche Abgrenzung wesentlich: Die AMLR ersetzt die regelbasierten Pflichten zur Anwendung gezielter finanzieller Sanktionen nicht. Sie ergänzt diese um risikobasierte Anforderungen zur Identifikation, Steuerung und Minderung von Umgehungs- und Nichtumsetzungsrisiken. Bestehende Sanktionspflichten aus anderen Unions- oder nationalen Rechtsakten bleiben daneben bestehen.

Operativ ist diese Schnittstelle hoch relevant.

Art. 20 Abs. 1 lit. d AMLR verlangt die Prüfung, ob der Kunde oder wirtschaftlich Berechtigte gezielten finanziellen Sanktionen unterliegt. Bei juristischen Personen ist zusätzlich zu prüfen, ob sanktionierte natürliche oder juristische Personen die Gesellschaft kontrollieren oder einzeln beziehungsweise gemeinsam mehr als 50 % der Eigentumsrechte oder eine Mehrheitsbeteiligung halten. Art. 26 Abs. 4 AMLR verlangt eine regelmäßige erneute Prüfung; Kredit- und Finanzinstitute müssen diese außerdem bei jeder neuen Benennung im Rahmen gezielter finanzieller Sanktionen durchführen. Die weitere Level-2-Konkretisierung der CDD-Anforderungen bleibt Gegenstand des noch nicht finalisierten RTS nach Art. 28 Abs. 1 AMLR.

Dadurch verbinden sich bislang teilweise getrennt behandelte Themen:

KYC → Beneficial Ownership → Beteiligungskette → Sanktions-Screening → Fallbearbeitung → Dokumentation

Die Designfrage lautet daher nicht, ob AML und Sanktionen zu einer einzigen Funktion verschmelzen sollten.

Sie lautet:

Wie werden die Schnittstellen so gestaltet, dass Daten, Verantwortlichkeiten und Kontrollen konsistent funktionieren, ohne unterschiedliche rechtliche Kontrolllogiken zu verwischen?

3.5 Monitoring und Verdachtsmeldewesen werden stärker End-to-End gedacht

Auch das Verdachtsmeldewesen bleibt nicht isoliert.

Art. 69 AMLR verlangt eine Bewertung relevanter Tatsachen und Informationen, wenn Kenntnisse, Verdacht oder berechtigte Gründe für die Annahme bestehen, dass Gelder aus kriminellen Tätigkeiten stammen oder mit Terrorismusfinanzierung in Verbindung stehen. Für die operative Fallbearbeitung sind deshalb Kundenmerkmale, Gegenparteien, Transaktionsmuster, Herkunft und Verwendung von Geldern sowie die Vereinbarkeit von Aktivitäten mit dem bekannten Kunden- und Risikoprofil zusammenzuführen.

Damit entsteht eine stärkere Verbindung zwischen:

CDD → Kundenrisiko → Transaction Monitoring → Alert → Fallanalyse → Verdacht → Meldung

Besonders relevant ist Art. 26 für die laufende Überwachung.

Art. 26 AMLR verlangt bereits im Level-1-Text eine kontinuierliche Überwachung der Geschäftsbeziehung einschließlich der Transaktionen. Umfasst eine Geschäftsbeziehung mehrere Produkte oder Dienstleistungen, müssen die Sorgfaltsmaßnahmen alle diese Produkte und Dienstleistungen abdecken; bei Gruppen sind zudem relevante Informationen über weitere Geschäftsbeziehungen desselben Kunden innerhalb der Gruppe zu berücksichtigen. AMLA konkretisiert diese Pflichten derzeit mit Leitlinien nach Art. 26 Abs. 5 AMLR; die öffentliche Konsultation läuft bis zum 3. September 2026, die Leitlinien sind damit noch nicht final.

Dies hat potenziell erhebliche Auswirkungen auf Datenintegration und Monitoring-Architektur.

Denn ein Institut kann eine End-to-End-Kundensicht nur herstellen, wenn Kundendaten, Produktnutzung, Gruppenbeziehungen und Transaktionsinformationen miteinander verbunden werden können.

Auch operative Reaktionszeiten werden relevant. Nach Art. 69 AMLR sind Informationsersuchen der FIU grundsätzlich innerhalb von fünf Arbeitstagen zu beantworten. In begründeten dringenden Fällen kann die FIU eine kürzere Frist setzen, einschließlich einer Frist von weniger als 24 Stunden; sie kann eine Frist bei entsprechender Begründung auch verlängern.

> **MANAGEMENT-IMPLIKATION**
>
> Monitoring-Transformation ist deshalb nicht primär ein Szenario-Tuning-Projekt.
>
> Sie ist eine Frage von:
>
> **Datenverfügbarkeit · Kundenbild · Gruppentransparenz · Regelwerk · Alert-Bearbeitung · Fallanalyse · Case Management · Berichtswesen · Nachweisführung**

3.6 Outsourcing muss gegen neue Grenzen geprüft werden

Viele Banken haben AML-Prozesse über Jahre industrialisiert und teilweise ausgelagert.

KYC Operations, Dokumentenprüfung, Screening, Alert-Bearbeitung und andere Tätigkeiten werden häufig in Shared Service Centern, Gruppengesellschaften oder bei externen Dienstleistern erbracht.

Die EU-AML-Verordnung stellt Auslagerungsmodelle nicht grundsätzlich infrage. Art. 18 AMLR erlaubt die Auslagerung von Aufgaben, belässt die volle Verantwortung jedoch beim Verpflichteten. Der Verpflichtete muss Qualifikation und Umsetzung durch den Dienstleister kontrollieren, die Auslagerung vorab dem Aufseher mitteilen und nachweisen können, dass er Vorgehen und Risikominderung des Dienstleisters versteht.

Gleichzeitig enthält Art. 18 Abs. 3 AMLR ausdrückliche Auslagerungsverbote für bestimmte Kernentscheidungen.

Dazu gehören beispielsweise:

- Vorschlag beziehungsweise Genehmigung der unternehmensweiten Risikobewertung,
- Genehmigung interner Richtlinien, Verfahren und Kontrollen,
- Entscheidung über das Kundenrisikoprofil,
- Entscheidung über Aufnahme einer Geschäftsbeziehung,
- bestimmte Meldeentscheidungen,
- Genehmigung von Kriterien zur Erkennung verdächtiger oder ungewöhnlicher Aktivitäten.

Damit wird für Institute eine systematische Überprüfung bestehender Auslagerungsmodelle erforderlich.

Die Leitfrage sollte sein:

> **Welche Tätigkeiten werden heute wo erbracht – und enthält dieses Modell Entscheidungen, Verantwortlichkeiten oder Kontrollschritte, die künftig nicht oder nicht in derselben Form ausgelagert werden dürfen?**

Das betrifft nicht nur klassische Outsourcing-Verträge.

Auch gruppeninterne Modelle, Centres of Excellence, Nearshore-Einheiten und Managed Services sollten überprüft werden.

3.7 Aufbewahrung, Register und Datenhaltung erzeugen technische Folgeeffekte

Ein Teil der größten Implementierungsrisiken liegt in Anforderungen, die auf den ersten Blick wenig strategisch wirken.

Ein Beispiel ist die Aufbewahrung.

Art. 77 AMLR sieht für die dort erfassten Unterlagen und Informationen grundsätzlich eine Aufbewahrungsfrist von fünf Jahren vor. Die Frist beginnt mit der Beendigung der Geschäftsbeziehung, der Durchführung einer Gelegenheitstransaktion oder der Ablehnung einer Geschäftsbeziehung beziehungsweise Gelegenheitstransaktion. Unter bestimmten Voraussetzungen kann eine weitere Aufbewahrung für höchstens fünf zusätzliche Jahre verlangt oder zugelassen werden.

Für lang laufende Kundenbeziehungen bedeutet dies, dass relevante CDD- und Transaktionsunterlagen während der Geschäftsbeziehung verfügbar bleiben und sich die fünfjährige Aufbewahrungsfrist erst an das Ende der Beziehung anschließt. Archivierungs-, Lösch- und Datenschutzkonzepte müssen deshalb frühzeitig auf den neuen Fristbeginn und mögliche Anschlussfristen abgestimmt werden.

Auch die künftigen Bankkontenregister-Anforderungen sind datenrelevant.

Art. 16 AMLD6 verlangt zentrale automatisierte Mechanismen, über die unter anderem Zahlungskonten beziehungsweise Bankkonten mit IBAN einschließlich virtueller IBAN, Depotkonten, Kryptowertkonten und Schließfächer identifiziert werden können. Die Richtlinie sieht daneben zusätzliche Identifikationsinformationen zu Kontoinhabern, vertretungsberechtigten Personen und wirtschaftlich Berechtigten vor; die unionsweite Verknüpfung über BARIS ist bis zum 10. Juli 2029 vorgesehen.

Damit wird deutlich:

Aufbewahrung, Kundenstammdaten und regulatorisches Berichtswesen sind Teil der AML-Transformation – nicht technische Nebenprojekte.

4 Fünf Fehlmuster in der Vorbereitung auf den 10. Juli 2027

Regulatorisches Mapping statt Operating-Model-Transformation

Viele Institute beginnen richtigerweise mit einem Artikel-für-Artikel-Gap-Assessment.

Problematisch wird es, wenn das Projekt dort stehen bleibt.

Ein juristisches Gap ist noch kein implementierter Prozess. Jede relevante Anforderung muss deshalb bis auf Rollen, Prozesse, Daten, Systeme, Kontrollen und Nachweisführung heruntergebrochen werden.

> **TYPISCHES ERGEBNIS DES FEHLMUSTERS**
>
> Die regulatorische Analyse ist vollständig, aber niemand kann sagen, welches System oder welcher Prozess konkret geändert werden muss.

Richtlinienfokus statt End-to-End-Design

Richtlinien sind notwendig – aber sie sollten nicht das Zielbild ersetzen.

Wenn Richtlinienaktualisierungen vor Prozess- und Systemdesign abgeschlossen werden, entsteht häufig ein Sollzustand, der operativ nicht abbildbar ist.

> **TYPISCHES ERGEBNIS DES FEHLMUSTERS**
>
> Die Richtlinie verlangt zusätzliche Informationen oder Kontrollen, die Frontend, Workflow oder Datenmodell nicht unterstützen.

KYC-Remediation wird unterschätzt

Zusätzliche Datenanforderungen wirken bei einem einzelnen Kunden überschaubar.

Im Kundenbestand multipliziert sich der Aufwand jedoch schnell.

Besonders kritisch sind Änderungen, die gleichzeitig Beneficial Ownership, Screening, PEP-Logik, Kundenrisikoeinstufung und Dokumentation betreffen.

> **TYPISCHES ERGEBNIS DES FEHLMUSTERS**
>
> Das Institut erkennt zu spät, dass nicht nur Neugeschäft, sondern große Teile des Bestands betroffen sind.

AML, Sanktionen, Monitoring und Daten bleiben in Silos

Die neue Regulatorik schafft stärkere Abhängigkeiten zwischen Bereichen, die organisatorisch häufig getrennt sind.

Wenn KYC beispielsweise Eigentums- und Kontrolldaten erhebt, Sanktionskontrollen andere Daten verwenden und Monitoring nur einen Ausschnitt der Kundenbeziehung sieht, entsteht keine belastbare End-to-End-Kontrolle.

> **TYPISCHES ERGEBNIS DES FEHLMUSTERS**
>
> Jede Funktion ist formal regelkonform – das Gesamtmodell bleibt fragmentiert.

Der 10. Juli 2027 wird als Projekttermin statt als Operational-Readiness-Termin verstanden

Der regulatorische Stichtag darf nicht gleichzeitig der letzte Projekttag sein.

Kritische Änderungen müssen vorher implementiert, migriert, getestet, dokumentiert und fachlich abgenommen sein.

> **TYPISCHES ERGEBNIS DES FEHLMUSTERS**
>
> Das Institut erreicht den Stichtag mit offenen Datenmigrationen, Übergangslösungen und ungetesteten Kontrollen.

5 Das Target Operating Model für AML unter den neuen europäischen Anforderungen

Ein belastbares AML Target Operating Model sollte sieben miteinander verbundene Ebenen enthalten.

5.1 Governance & Verantwortlichkeiten

KERNELEMENTE

Management-Steuerung | Compliance Manager | Geldwäschebeauftragter | Three Lines | Entscheidungsrechte | Eskalation | Management-Berichtswesen

ZIEL

Es muss eindeutig erkennbar sein, wer Risiken identifiziert, wer Richtlinien genehmigt, wer operative Entscheidungen trifft, wer kontrolliert und wer gegenüber Management und Aufsicht berichtet.

5.2 Risikomanagement

KERNELEMENTE

Unternehmensweite Risikoanalyse | Kundenrisiko | Produktrisiko | geografisches Risiko | Kanalrisiko | Sanktionsrisiko | Gruppenrisiko

ZIEL

Die unternehmensweite Risikoanalyse darf nicht isoliert neben den Kontrollen stehen. Risiken müssen nachvollziehbar in Kundenrisiko, Kontrollen, Monitoring und Management-Informationen übersetzt werden.

5.3 Customer Due Diligence

KERNELEMENTE

Kundenidentifizierung | Verifizierung | Zweck & Art | Beneficial Ownership | PEP | Sanktionen | EDD | SDD | Kundenlebenszyklus

ZIEL

CDD muss als vollständiger Kundenlebenszyklus verstanden werden – vom Pre-Onboarding über Aufnahme und laufende Aktualisierung bis zur Beendigung.

5.4 Monitoring & Fallbearbeitung

KERNELEMENTE

Laufende Überwachung | Transaction Monitoring | Alert-Bearbeitung | Fallanalyse | Case Management | Kundenreview | Eskalation

ZIEL

Monitoring muss KYC-, Risiko- und Transaktionsinformationen zu einem nachvollziehbaren Kontrollprozess verbinden.

5.5 Berichtswesen & FIU-Interaktion

KERNELEMENTE

Verdachtsmeldewesen | FIU-Anfragen | Dokumentation | Tipping-off-Kontrollen | Nachweisführung | Audit Trail

ZIEL

Entscheidungen müssen nicht nur richtig, sondern auch zeitnah, reproduzierbar und gegenüber interner wie externer Prüfung verteidigbar sein.

5.6 Daten & Technologie

KERNELEMENTE

Kundenstammdaten | Beneficial-Ownership-Daten | Screening | Risk Engines | Monitoring | Case Management | regulatorisches Berichtswesen | Aufbewahrung | Datenqualität

ZIEL

Das Datenmodell muss die fachliche Kontrolllogik unterstützen. Manuelle Nebenlisten dürfen nicht dauerhaft strukturelle Lücken der Kernarchitektur kompensieren.

5.7 Gruppen- & Drittanbietersteuerung

KERNELEMENTE

Gruppenrichtlinien | Shared Services | Outsourcing | Drittanbieter | Niederlassungen | Tochterunternehmen | Informationsaustausch | Assurance

ZIEL

Zentralisierung und Outsourcing müssen mit klarer Verantwortung, angemessener Steuerung und regulatorisch zulässigen Entscheidungsrechten verbunden werden.

> **ZIELBILD**
>
> Ein regulatorisch belastbares AML Operating Model funktioniert nicht als Ansammlung einzelner Kontrollen.
>
> Es funktioniert als Kette:
>
> **Risiko → Kunde → Daten → Kontrollen → Monitoring → Fallanalyse → Berichtswesen → Nachweise → Management-Steuerung**
>
> Genau diese Kette sollte das Transformationsprogramm abbilden.

6 Daten & Technologie: Wo regulatorische Anforderungen operativ werden

Die größten Umsetzungsprobleme entstehen häufig nicht bei der Interpretation einer Norm, sondern bei ihrer Übersetzung in bestehende Systeme.

Das neue EU-AML-Paket kann insbesondere Auswirkungen erzeugen auf:

Bereich	Möglicher Transformationsbedarf
Kundenstammdaten	neue oder angepasste KYC-Felder
Beneficial Ownership	Abbildung mehrstufiger Eigentums- und Kontrollstrukturen
Screening	Erweiterung relevanter Personen und Gesellschaften
Kundenrisikoeinstufung	neue Risikofaktoren und Governance
Laufende Überwachung	stärkere Verknüpfung von Kunde, Produkt und Aktivität
Transaction Monitoring	umfassendere Kunden- und Gruppenperspektive
Case Management	neue Entscheidungs- und Dokumentationslogik
Regulatorisches Berichtswesen	standardisierte Daten und Meldeprozesse
Aufbewahrung	neuer Fristbeginn und Löschlogik
Bankkontenregister	zusätzliche Meldeinformationen und Objekttypen

Der Transformationsbedarf ist bereits im Level-1-Text sichtbar: Art. 22 AMLR erweitert beziehungsweise konkretisiert Identifikationsdaten, Art. 20 und 26 verbinden CDD stärker mit Sanktionsprüfung und laufender Überwachung, Art. 77 verändert den Fristbeginn der Aufbewahrung und Art. 16 AMLD6 erweitert die Registerlogik. Die noch laufende Level-2-Arbeit der AMLA wird einzelne Anforderungen weiter präzisieren und sollte deshalb als eigener regulatorischer Workstream in die Umsetzungssteuerung aufgenommen werden.

Das hat eine wichtige Konsequenz für die Transformationssteuerung.

Compliance sollte die Anforderungen definieren.

Aber Compliance allein kann sie nicht implementieren.

Notwendig ist eine integrierte Steuerung aus:

Compliance + Operations + Daten + Technologie + Fachbereich + Recht + interne Kontrollen

Die richtige Reihenfolge lautet deshalb:

> **Anforderung → Kontrollziel → Zielprozess → Datenanforderung → Technologieänderung → Test → Nachweis**
>
> Nicht:
>
> **Regulierung → IT-Ticket.**

7 Transformations-Roadmap bis zum 10. Juli 2027

Der regulatorische Stichtag ist gesetzt. Daraus sollte rückwärts geplant werden.

Die folgende Roadmap ist eine Bersch-Transformationslogik für die Umsetzung und keine regulatorisch vorgegebene Projektplanung. Sie plant bewusst rückwärts vom Anwendungsstichtag 10. Juli 2027 und berücksichtigt den aktuellen Stand der noch laufenden Level-2-Konkretisierung.

Q3 2026 — Readiness- und Impact-Assessment

ZIEL

Klarheit darüber schaffen, wo das Institut tatsächlich betroffen ist.

SCHWERPUNKTE

- Regulatorischer Anforderungskatalog
- Ist-Prozessaufnahme
- Governance-Abgleich
- KYC/CDD-Gap-Assessment
- Auswirkungen auf Beneficial Ownership
- AML-/Sanktions-Schnittstellen
- Monitoring und Berichtswesen
- Outsourcing und Gruppenmodell
- Auswirkungen auf Daten & Technologie
- Bestandskundenanalyse

ERGEBNIS

EU-AML-Paket Impact Map

mit klarer Trennung zwischen:

- Kein Anpassungsbedarf,
- Richtlinienanpassung,
- Prozessanpassung,
- Datenanpassung,
- Technologieanpassung,
- Governance-Anpassung,
- Wesentlicher Transformationsbedarf.

Q4 2026 — Target Operating Model und Design

ZIEL

Aus der Impact Map ein belastbares Zielbild entwickeln.

SCHWERPUNKTE

- Governance und Entscheidungsrechte
- zukünftige Rollen von Compliance Manager und GwB
- CDD-Zielprozess
- Beneficial-Ownership-Logik
- Integration der Sanktionskontrollen
- Kundenrisiko

- Monitoring-Architektur
- Zieldatenmodell
- Outsourcing und Drittanbietermodell
- Aufbewahrung und Berichtswesen

ERGEBNIS

AML Target Operating Model 2027

inklusive:

- Prozesse,
- Kontrollen,
- Rollen,
- Daten,
- Systeme,
- Verantwortlichkeiten,
- Umsetzungsprioritäten.

Q1 2027 — Umsetzung und Remediation

ZIEL

Zielbild technisch und operativ umsetzen.

SCHWERPUNKTE

- Systemkonfiguration
- neue Datenfelder
- Workflow-Anpassungen
- Screening-Änderungen
- Kundenrisikoeinstufung
- Monitoring
- Berichtswesen
- Aktualisierung von Richtlinien und Verfahren
- KYC-Remediation
- Outsourcing-Anpassungen

ERGEBNIS

technisch und fachlich implementierter Sollprozess

Noch nicht nur dokumentiert, sondern ausführbar.

April–Mai 2027 — Integration und Migration

ZIEL

Einzellösungen zu einem End-to-End-Prozess verbinden.

SCHWERPUNKTE

- Datenmigration
- Bestandskunden
- Schnittstellen

- Screening-Populationen
- Gruppeninformationen
- Monitoring-Daten
- Case Management
- regulatorische Meldelogik
- Aufbewahrung

ERGEBNIS

produktiver beziehungsweise produktionsnaher End-to-End-Prozess

Juni 2027 — Validierung und Operational Readiness

ZIEL

Nachweisen, dass das Zielmodell funktioniert.

SCHWERPUNKTE

- End-to-End-Tests
- Kontrollwirksamkeit
- Stichproben
- Datenqualität
- Fehlerbehebung und Remediation
- Management-Berichtswesen
- Training
- Verfahren für Ausnahmen
- regulatorische Nachweise
- Restrisikoentscheidungen

ERGEBNIS

Operational Readiness

> **EMPFOHLENES INTERNES ZIEL**
>
> **30. Juni 2027 — Freigabe der Operational Readiness**
>
> Die Bank sollte zu diesem Zeitpunkt fachlich und technisch bereit sein.
>
> Damit verbleibt ein begrenzter Puffer für kritische Restpunkte.

10. Juli 2027 — Regulatorischer Go-Live

Ab dem 10. Juli 2027 muss das AML Operating Model unter den neuen Anforderungen stabil, nachvollziehbar und kontrolliert arbeiten.

8 Management-Prioritäten

1. Transformation auf Vorstandsebene verankern

Das EU-AML-Paket sollte nicht als reines Compliance-Richtlinienprojekt geführt werden.

Governance, Risikoanalyse, Ressourcen und Management-Berichtswesen erhält eine stärkere Bedeutung. Das Programm braucht deshalb einen klar benannten Sponsor auf Vorstandsebene.

2. High-Impact-Anforderungen zuerst identifizieren

Nicht jede regulatorische Änderung erzeugt denselben Umsetzungsaufwand.

Besonders früh sollten Anforderungen adressiert werden, die:

- große Kundenbestände betreffen,
- IT-Entwicklung benötigen,
- Datenmigration erfordern,
- mehrere Funktionen verbinden,
- Outsourcing verändern,
- oder lange Testzyklen benötigen.

3. Bestandskunden früh quantifizieren

KYC-Transformation wird kritisch, wenn erst im Frühjahr 2027 festgestellt wird, dass hunderttausende oder Millionen Kunden nachbearbeitet werden müssen.

Deshalb früh klären:

> **Welche Daten fehlen?**
>
> **Bei welchen Segmenten?**
>
> **Wie können sie beschafft werden?**
>
> **Wie hoch ist der Automatisierungsgrad?**

4. Beneficial Ownership, KYC und Sanktionen gemeinsam gestalten

Beneficial-Ownership-Daten sind nicht nur ein CDD-Thema.

Sie speisen weitere Kontrollen.

Das Ziel sollte deshalb ein konsistentes Daten- und Kontrollmodell sein und nicht drei unterschiedliche Interpretationen derselben Kundenstruktur.

5. Outsourcing und Shared Services jetzt überprüfen

Bestehende Auslagerungsmodelle sollten gegen die expliziten Entscheidungs- und Governance-Grenzen der EU-AML-Verordnung abgeglichen werden.

Notwendige organisatorische Rückverlagerungen oder Vertragsänderungen brauchen Vorlauf.

6. Technologie nicht erst nach der fachlichen Konzeption einbinden

Daten und Technologie sind kein nachgelagerter Umsetzungskanal.

Sie bestimmen, was operativ möglich ist.

Technologieverantwortliche sollten deshalb bereits am Zieldesign beteiligt sein.

7. Juni 2027 als Zieltermin setzen – nicht den 10. Juli

Der 10. Juli 2027 sollte der regulatorische Go-Live sein.

Der interne Transformationsplan sollte spätestens Ende Juni auf Operational Readiness zielen.

9 EU-AML-Paket Readiness Assessment

Für viele Banken lautet die zentrale Frage heute nicht, ob sie betroffen sind.

Die entscheidendere Frage lautet:

Ist unser heutiges AML Operating Model tatsächlich bereit für den 10. Juli 2027?

Ein strukturiertes Readiness Assessment sollte mindestens acht Dimensionen betrachten.

Dimension	Diagnostische Leitfrage	Typisches Warnsignal
Governance	Sind Vorstand, Compliance Manager, GwB und operative Funktionen eindeutig abgegrenzt?	Entscheidungsrechte bleiben implizit
Risikomanagement	Ist die Risikoanalyse mit Richtlinien, Kontrollen und Management-Berichtswesen verbunden?	Risikoanalyse und Kontrollmodell laufen getrennt
CDD / KYC	Können neue beziehungsweise konkretisierte Kundendaten End-to-End verarbeitet werden?	manuelle Workarounds und fehlende Pflichtfelder
Beneficial Ownership	Können mehrstufige Eigentums- und Kontrollstrukturen korrekt abgebildet werden?	Beneficial-Ownership-Daten werden außerhalb der Kernsysteme dokumentiert
AML & Sanktionen	Sind Eigentums- und Kontrolldaten, Screening und Verantwortlichkeiten konsistent verbunden?	unterschiedliche Datenpopulationen und unklare Verantwortung für Eigentums- und Kontrolldaten
Monitoring & Berichtswesen	Entsteht eine vollständige Sicht auf Kunde, Produkte und relevante Aktivitäten?	Monitoring sieht nur Teilbeziehungen
Daten & Technologie	Unterstützt die technische Architektur die zukünftigen Kontrollziele?	Richtlinienanforderungen sind technisch nicht ausführbar
Gruppe & Drittanbieter	Sind Outsourcing, Shared Services und gruppenweite Prozesse regulatorisch tragfähig?	Kernentscheidungen liegen faktisch beim Dienstleister

Das Assessment sollte nicht mit einer langen Liste regulatorischer Artikel enden.

Es sollte drei managementfähige Ergebnisse produzieren.

1 Regulatory & Operating Model Gap Analysis

Strukturierte Bewertung der wesentlichen Abweichungen zwischen heutiger Organisation und Zielanforderungen.

Bewertet werden insbesondere:

Governance | Prozesse | Kontrollen | Daten | Technologie | Drittanbieter | Gruppenmodell | Nachweise

2 Implementation Risk Map

Priorisierung der Gaps nach:

- Regulatorische Kritikalität
- Umsetzungskomplexität
- Kunden-/Datenvolumen
- Technologischer Vorlauf
- Operationelles Risiko
- Abhängigkeiten

Dadurch wird sichtbar, welche Themen sofort gestartet werden müssen und welche später umgesetzt werden können.

3 Transformations-Roadmap bis zum 10. Juli 2027

Konkreter Fahrplan mit:

- Workstreams,
- Verantwortlichen,
- Entscheidungen,
- Abhängigkeiten,
- Meilensteinen,
- Tests,
- Readiness-Kriterien,
- Management-Gates.

> **DAS ZIEL**
>
> Aus mehreren hundert Seiten regulatorischer Anforderungen eine steuerbare Management-Antwort machen:
>
> **Was verändert sich?**
>
> **Wo sind wir betroffen?**
>
> **Was müssen wir wann konkret tun?**

Über Bersch Consulting

Bersch Consulting unterstützt Banken und Finanzinstitute bei komplexen regulatorischen Transformationsvorhaben.

Die Beratung verbindet regulatorisches Verständnis, Operating-Model-Kompetenz und Umsetzungsarchitektur, um Financial-Crime- und Compliance-Funktionen nicht nur formal regelkonform, sondern operativ belastbar aufzustellen.

Zu den relevanten Fähigkeiten zählen insbesondere:

- AML Transformation und Remediation
- AML Target Operating Models
- Customer Due Diligence und KYC
- Financial Crime Governance
- Beneficial Ownership
- Prozess- und Kontrollarchitektur
- Daten- und Technologie-Transformation
- regulatorische Readiness Assessments
- Programmdesign und Implementierungs-Governance

Nächster Schritt

Empfohlener Einstiegspunkt: EU-AML-Paket Readiness Review

Ein fokussiertes Readiness Review hilft Management-Teams, die Auswirkungen des EU-AML-Pakets auf ihr bestehendes Operating Model strukturiert zu bewerten und kritische Handlungsfelder frühzeitig zu priorisieren.

Das Review liefert drei managementfähige Ergebnisse:

Regulatory & Operating Model Gap Analysis
Lücken in Governance, CDD, Beneficial Ownership, Sanktionen, Monitoring, Kontrollen, Daten, Technologie und Outsourcing.

Implementation Risk Map
Priorisierung nach regulatorischer Kritikalität, Umsetzungsaufwand, Abhängigkeiten und notwendigem Vorlauf.

Transformations-Roadmap bis zum 10. Juli 2027
Managementfähiger Umsetzungsplan von Readiness und Zieldesign bis zu Tests und Operational Readiness.

Der Nutzen liegt nicht in einer weiteren regulatorischen Zusammenfassung. **Er liegt darin, aus regulatorischer Komplexität ein steuerbares Transformationsprogramm zu machen.**

ERSTGESPRÄCH ANFRAGEN

EU-AML-Paket Readiness Review

Erstgespräch anfragen

QR-Code scannen oder den Link anklicken.

Schlussgedanke

Das neue EU-AML-Paket schafft mehr Harmonisierung – aber nicht automatisch weniger Implementierungskomplexität.

Für Banken werden wesentliche Grundlagen der Geldwäscheprävention vertraut bleiben. Gleichzeitig verändern sich Verantwortlichkeiten, Detailanforderungen und Abhängigkeiten zwischen KYC, Beneficial Ownership, Sanktionen, Monitoring, Daten, Technologie und Governance.

Der entscheidende Wettbewerbsvorteil liegt deshalb nicht darin, jede neue Vorschrift zuerst zu interpretieren.

Er liegt darin, früh genug ein Operating Model aufzubauen, das diese Anforderungen konsistent, skalierbar und nachweisbar wirksam erfüllen kann.

Der 10. Juli 2027 ist kein Starttermin für die Transformation. Er ist der Termin, zu dem die Transformation operativ funktionieren muss.

Bersch Consulting

Bersch Management Consultancy GmbH · Bremen
Regulatorische Transformation · Financial Crime · AML Operating Models

Quellenverzeichnis

Regulatorischer Stand: 17. August 2026. Maßgeblich sind die geltenden Level-1-Rechtsakte. Entwürfe von RTS, ITS und Leitlinien werden nur entsprechend ihrem offiziellen AMLA-Verfahrensstatus berücksichtigt und nicht als geltendes Recht dargestellt. Die AMLA-Instrumentenübersicht war zum Prüfzeitpunkt zuletzt am 21. Juli 2026 aktualisiert.

Primärrecht

1. Verordnung (EU) 2024/1624 (AMLR) – Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder Terrorismusfinanzierung.
EUR-Lex – AMLR

2. Richtlinie (EU) 2024/1640 (AMLD6) – Mechanismen der Mitgliedstaaten zur Verhinderung der Nutzung des Finanzsystems für Geldwäsche oder Terrorismusfinanzierung.
EUR-Lex – AMLD6

3. Verordnung (EU) 2024/1620 (AMLAR) – Errichtung der Anti-Money Laundering Authority (AMLA).
EUR-Lex – AMLAR

4. Verordnung (EU) 2023/1113 (TFR) – Angaben bei Geldtransfers und Transfers bestimmter Kryptowerte.
EUR-Lex – TFR

AMLA – aktueller Level-2- und Leitlinienstand

5. AMLA, Regulatory Instruments – zentrale Übersicht über RTS, ITS, Leitlinien und deren Verfahrensstatus; letzte Aktualisierung der Übersicht: 21. Juli 2026.
AMLA – Regulatory Instruments

6. RTS-Entwurf nach Art. 28 Abs. 1 AMLR – Customer Due Diligence. Konsultation vom 9. Februar bis 8. Mai 2026; Status: Konsultation geschlossen, Ergebnisse und Finalisierung noch ausstehend.
AMLA – CDD RTS, Art. 28(1) AMLR

7. RTS-Entwurf nach Art. 19 Abs. 9 AMLR – Kriterien für Geschäftsbeziehungen, Gelegenheitstransaktionen, verbundene Transaktionen und niedrigere Schwellenwerte. Status: Konsultation geschlossen.
AMLA – RTS, Art. 19(9) AMLR

8. RTS-Entwurf nach Art. 16 Abs. 4 und Art. 17 Abs. 3 AMLR – gruppenweite Mindestanforderungen und zusätzliche Maßnahmen für Tochterunternehmen und Zweigniederlassungen in Drittländern. Status: Konsultation geschlossen.
AMLA – Group-wide RTS, Art. 16(4)/17(3) AMLR

9. Leitlinienentwurf nach Art. 10 Abs. 4 AMLR – unternehmensweite Risikobewertung. Konsultation vom 16. April bis 15. Juli 2026; Status: Konsultation geschlossen.
AMLA – Business-Wide Risk Assessment Guidelines

10. Leitlinienentwurf nach Art. 26 Abs. 5 AMLR – laufende Überwachung von Geschäftsbeziehungen. Konsultation vom 3. Juni bis 3. September 2026; Status zum Redaktionsstand: offen.
AMLA – Ongoing Monitoring Guidelines

11. ITS-Entwurf nach Art. 69 Abs. 3 AMLR – Format für Verdachtsmeldungen und Bereitstellung von Transaktionsaufzeichnungen. Konsultation vom 2. Juli bis 20. September 2026; Status zum Redaktionsstand: offen.
AMLA – Reporting ITS, Art. 69(3) AMLR

Hinweis: Der regulatorische Level-2-Rahmen befindet sich teilweise noch im Verfahren. Vor einer konkreten Umsetzung sollten die jeweils final veröffentlichten RTS, ITS und AMLA-Leitlinien erneut gegen den dann aktuellen Stand geprüft werden.