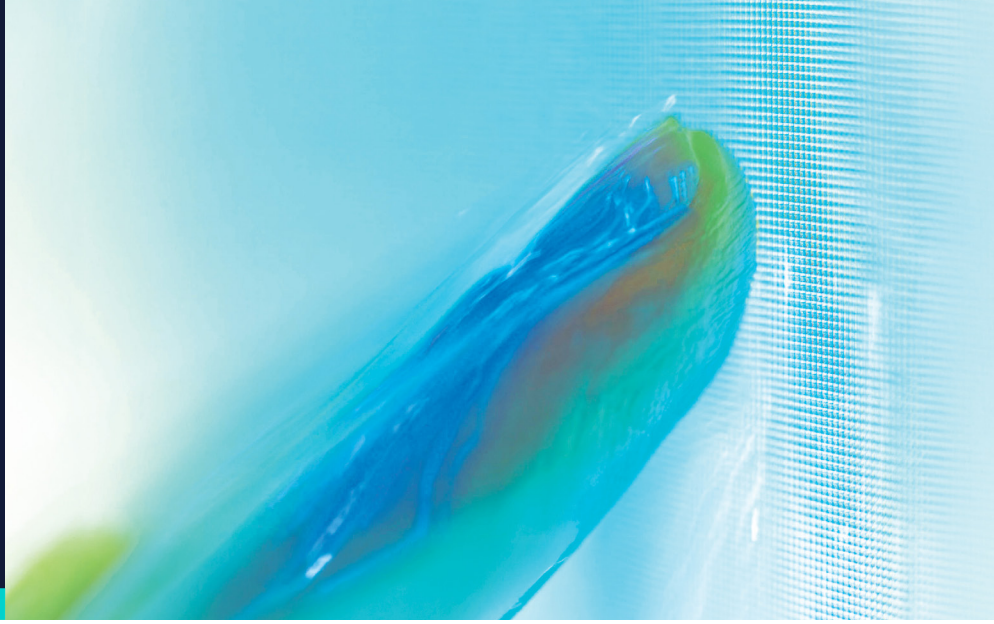
Industry white paper

AMLR

Navigating AMLR from a Dutch Perspective:
Key Changes and Their Impact Across the
Financial Services Sector in The Netherlands

Capgemini

Table of Contents



Executive Summary

AMLR turns AML into a data-driven, regulator testable discipline, forcing financial institutions to invest first in data quality, risk models and evidence.

The Anti Money-Laundering Regulation (AMLR)[1] fundamentally reshapes the European AML/CFT framework by introducing a directly applicable "single rulebook", supported by Regulatory Technical Standards, Guidelines and Implementing Technical Standards. National regimes, such as the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (Wwft)[2], will be replaced by a harmonised European framework with less scope for national interpretation.

This white paper explains how the AMLR will reshape AML/CFT compliance across the (non)financial services sector by making the risk based approach more harmonised and operationally testable, and by introducing a new supervisory architecture under AMLA. It also highlights how EU level harmonisation will continue to interact with national implementation choices where discretion remains, with specific attention to the Dutch context, and points to the key areas institutions should prioritise as they prepare for the new framework to apply.

What changes most (and why it matters)

A core change under the AMLR is the evolution of the risk-based approach. While risk and proportionality remain guiding principles, the AMLR shifts risk assessment towards a data-driven, more standardised and fully testable system. Through RTS, common indicators, datasets and methodologies for assessing risk are prescribed. Institutions retain risk-based judgement, but within a more prescriptive structure that increases expectations around consistency, traceability, and evidencing.

Supervisory arrangements are designed to support greater convergence across Member States, reflected in harmonised supervisory approaches and shared risk methodologies. In practice, institutions will be expected to apply AML/CFT requirements in a consistent and auditable manner across jurisdictions.

Where implementation pressure will show up first

AMLA's draft RTS on Customer Due Diligence under Article 28(1) AMLR moves the market towards a single, EU-wide execution standard by setting granular expectations for standard and enhanced due diligence (including minimum data sets, non-face-to-face verification options, UBO/PEP controls and discrepancy reporting). This greater standardisation will materially affect financial institutions' onboarding, periodic reviews and evidencing requirements, even where proportionality and the risk-based approach are acknowledged. The AMLR provides a risk-sensitive grace period to phase the uplift of existing customers and avoid an immediate full-population remediation.

1. Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (PbEU R 1624).
2. Wet ter voorkoming van witwassen en financieren van terrorisme 2008.

National implementation choices remain relevant wherever discretion exists. Although the Netherlands has stated its ambition to minimise regulatory burden through a proportional, risk based approach, the draft Implementing Act (Iwt)[3] leaves several operational aspects unresolved and preserves certain national elements that may go beyond the AMLR framework.

What institutions should prioritise now

- AMLR is a shift from judgement to proof. Supervisors will increasingly test whether AML decisions are replicable, evidence-based and traceable, not just "reasonable" on paper.
- Time is the main risk variable. With AMLR directly applicable from 10 July 2027, boards should treat 2026 as the mobilisation year to build a credible delivery runway and de-risk timeline slippage.
- This is a transformation programme, not a compliance refresh. The operating model must function as an integrated system, spanning processes, data, controls, and documentation, underpinned by clear delivery sequencing and robust programme governance.
- Start with a bank-owned Business-Wide Risk Assessment (BWRA) anchored gap & impact assessment. Priority one is a gap-led refresh anchored in a BWRA that translates expectations on consistency/traceability/ evidence into a remediation plan, kept proportionate by design.
- National discretion doesn't disappear, it becomes an execution risk. Even where discretion remains, Dutch implementation choices (e.g. via the draft Iwt) can leave operational aspects unresolved and potentially introduce national elements beyond the AMLR baseline.

How Capgemini's FCC practice can support: Capgemini supports financial institutions across the full AMLR journey, combining regulatory advisory, technology enhancement and operational services. We help translate regulatory requirements into institution specific impact assessment and a prioritised roadmap aligned to supervisory expectations.

We support implementation across the full KYC domain to allow for scalable, auditable and sustainable compliance. Nowadays this is often enabled by technology-driven enhancements such as automated screening, intelligent risk scoring and compliance analytics, embedded within appropriate governance and privacy controls. Managed services can support the industrialisation of high-volume due diligence and investigation activities.

Together, this integrated approach helps institutions achieve timely compliance, reduce remediation risk and build longer-term regulatory resilience.

3. Implementing rules for Directive (EU) 2024/1640 and Regulation (EU) 2024/1624 on preventing the use of the financial system for money laundering or terrorist financing (Implementatiewet ter voorkoming van witwassen en terrorismefinanciering).

1. Introduction

The Anti-Money Laundering Regulation (AMLR) is a core pillar of the European Union's AML Package. Together with the sixth Anti-Money Laundering Directive (AMLD6)[4] and the establishment of the Anti-Money Laundering Authority (AMLA)[5], it creates a more harmonised and consistent framework for preventing the misuse of the financial system for money laundering and terrorist financing. Alongside these three core instruments, the EU AML Package is complemented by the recast Transfer of Funds Regulation (the "Travel Rule")[6], strengthening transparency and traceability requirements for transfers of funds and certain crypto-asset transfers, and is already in effect, reflecting the EU's response to emerging financial technologies and associated regulatory risk considerations.

Unlike earlier AML directives, the AMLR is directly applicable and from 10 July 2027 it will replace national transpositions (e.g., the Dutch AML/CFT Act), significantly reducing national discretion. Obliged entities will operate under a single rulebook, further detailed through Regulatory Technical Standards (RTSs), Guidelines (GLs) and Implementing Technical Standards (ITSs) that specify how requirements must be applied in practice.

The AMLR introduces important structural and operational changes for both financial sector and non-financial sector obliged entities. These include a redefined risk-based approach, increased standardisation of client due diligence (CDD) requirements, enhanced supervisory convergence, as well as a stronger emphasis on data quality, evidencing, and comparability. While the AMLR seeks to preserve proportionality and risk sensitivity, it also introduces more prescriptive requirements that directly affect how institutions design their AML/CFT frameworks, processes, and controls.

This white paper analyses the most significant changes introduced by the AMLR and their impact on the (non) financial services sector. It focuses on how the new European framework reshapes the application of the risk-based approach, the evolving supervisory architecture under AMLA, and the interaction between EU-level harmonisation and national implementation choices, with specific attention to the Dutch context.

In the second half of the paper, a deep dive is provided of AMLA's draft RTS on CDD under Article 28(1) AMLR. This deep dive explores how the AMLR's high-level principles are translated into concrete operational requirements, including non-face-to-face identification, BO verification, PEP screening, and the risk-sensitive transition of existing customers.

Together, these elements provide an overview of how the AMLR reshapes AML/CFT compliance in practice and highlight the key areas that require attention as institutions prepare for the application of the new European framework.

4. Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849 (PbEU, L 1640).
5. Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 (PbEU, R 1620).
6. Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (PbEU R 1113).

2. From Judgement to Metrics: The New Risk-Based Approach

The AMLR marks the beginning of a new phase in European AML supervision: one directly applicable rulebook, one central supervisory authority and one harmonised methodology for assessing risk. While the risk based approach has always been the foundation of financial crime compliance, what changes under the AMLR is the way this approach is operationalised and how it becomes more structured. The risk based approach shifts from an institution defined assessment philosophy to a data driven, standardised and fully testable system.

The EU's intention is clear: to eliminate the fragmentation of national interpretations by introducing a tightly harmonised framework that obliges supervisors to apply the same risk methodology and requires institutions to use the same indicators, datasets and scoring principles. This harmonisation will be enforced through new RTS, in which the AMLA precisely defines how inherent risk, control quality and residual risk must be assessed. The objective is consistency and proportionality, but the consequence is reduced room for institution specific interpretation of the risk based approach.

For many institutions, this shift might feel paradoxical: the risk based approach should be risk based, yet the expanding set of mandatory data points and scoring mechanisms increasingly feels rule based. EBA emphasizes that extensive data collection is essential to achieve comparable risk assessments across all Member States and stresses that institutions must supply sufficient information to make such harmonisation possible. As a result, the risk based approach evolves from a judgement driven to a data driven discipline. Narrative assessments give way to standardised, reproducible risk models, obliging institutions to build their risk frameworks on fixed indicators and data driven scoring logic.

The AMLR's design is therefore deliberate: less interpretation and more measurability. This ensures that EU wide uniform logic, rather than divergent national practices, forms the basis of AML assessments.

Re-centring the risk-based approach

A clear example of this tension can be seen in the successive drafts of the RTS on CDD under Article 28(1) AMLR and AMLA's efforts to address it. EBA's initial version of the RTS in March 2025 provided little space for a genuine risk based application, instead presenting an extensive list of mandatory data points that reinforced the perception of a purely rule driven approach[7]. In the second draft of October 2025, however, AMLA introduced a brand-new Article 1, placed deliberately at the very beginning of the RTS.

This article states:

> ***" Proportionality and risk-based approach***
>
> *This Commission Delegated Regulation shall be applied in line with the risk-based approach. The extent and the nature of the information to be obtained and the measures to be applied by obliged entities shall be commensurate with the type and level of risk identified and shall enable obliged entities to manage and mitigate that risk appropriately. "*

Its prominent positioning almost feels like a statement: a clear reaffirmation, despite the prescriptive RTS structure and the large volume of required datapoints, the risk based approach is not merely a theoretical principle but a practical cornerstone of the AMLR. By opening the RTS with an explicit reference to proportionality and risk based judgement, AMLA appears to rebalance the framework: acknowledging the operational impact of standardisation while re anchoring the risk based approach as the guiding mechanism for CDD measures in practice.

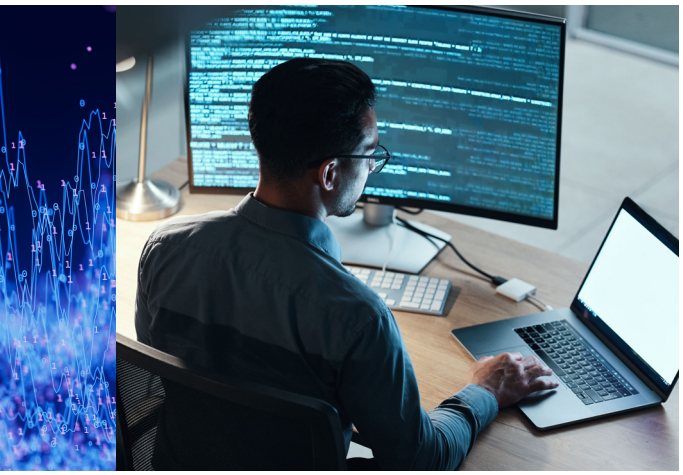
7. European Banking Authority (EBA), 'The EBA consults on new rules related to the anti-money laundering and countering the financing of terrorism package', The EBA consults on new rules related to the anti- money laundering and countering the financing of terrorism package | European Banking Authority (accessed 20 April 2026).

As a result, the core philosophy of the risk based approach remains intact. Risks remain central, the depth of measures must remain proportionate, and institutions must direct resources where threats are most significant. What changes, however, is the structural foundation supporting this principle.

Stronger and stricter: the new operating model reality

These developments produce a new balanced reality: institutions retain risk based judgement, but the freedom to apply that judgement is framed by a rule based structural foundation. The reasoning of European legislators and supervisors is straightforward: without standardisation, proportional risk management cannot be assessed consistently, and without data driven uniformity, cross border supervision is unworkable. The AMLR therefore makes the risk based approach simultaneously stronger and stricter: stronger because the approach becomes more robust and verifiable, stricter because institutions have significantly less freedom to design their own risk approach. As a result, institutions will need to reshape their operating models towards a data centric approach to AML compliance, incorporating integrated KYC and transaction risk models, strengthened governance structures and real time monitoring capabilities.

In essence, the AMLR transforms the European risk based approach into a structured, uniform and fully testable system: one that does not replace professional judgement but defines and constrains it within a common European framework. For financial crime and banking leaders, the guiding question is no longer whether the risk based approach is changing, but how to position their organisations within this new reality: a reality in which risk remains central, yet data forms the unambiguous foundation.



3. A new EU supervisory engine: what AMLA changes (and why it matters)

AMLA's mandate doesn't just strengthen the EU single rulebook; it adds a new operating layer for supervision. In practice, that means a European system built on three levers: direct EU supervision for a small set of high-impact banks, EU-driven convergence across the wider financial sector via national supervisors, and EU-level oversight mechanisms that extend into parts of the non-financial sector. The common thread is simple: less divergence, more comparability, and more testable outcomes.

Direct supervision (of the financial sector)

Direct supervision

From 2028, AMLA is expected to directly supervise 40 of the EU's most impactful financial institutions from 2028, with a first selection process in 2027 and preparatory work in 2026 focused on risk analysis, selection methodology and data collection to calibrate the approach. The direction of travel is clear: supervisory scope and intensity will increasingly be anchored in comparable data and a shared risk logic, rather than national supervisory tradition alone.

Indirect supervision

Beyond the limited group under direct supervision, AMLA has indirect supervisory powers across the entire financial sector, explicitly aimed at convergence. The practical mechanism is structured cooperation with national competent authorities, using common approaches, thematic work, benchmarking and shared risk frameworks to reduce variation in supervisory expectations and outcomes. The result for firms is not theoretical: it's more standardised supervisory interactions and a sharper, more consistent evidence bar. The NCAs for the Netherlands are the Dutch central bank (DNB)[8] and the Financial Supervisory Authority of the Netherlands (AFM)[9].

8. De Nederlandsche Bank (DNB).
9. Autoriteit Financiële Markten (AFM)

Oversight of non-financial sectors.

In the non-financial space, the change is less about day-to-day EU supervision of every obliged entity and more about raising consistency and effectiveness. AMLA's approach is to build convergence tools:

- Mapping and benchmarking supervisory practices across diverse non-financial sectors, EU-wide.
- Combine supervisory findings and FIU insights into a more coherent risk picture (important because non-financial sectors are heterogeneous and risk signals are often fragmented).
- Use peer mechanisms (including supervisory colleges) to pull practice closer together across Member States

What this means for banks

AMLA's new EU oversight layer is designed to reduce national divergence by building a European supervisory system: direct EU supervision for a limited set of institutions, and EU-driven supervisory convergence across the wider financial sector via NCAs. In 2026, AMLA develops harmonised approaches for indirect supervision with a common supervisory model/manual and thematic reviews, supported by EU-wide risk mapping and benchmarking. For banks, this means more standardised supervisory interactions and more structured evidence expectations, and, where relevant, earlier engagement linked to selection methodology, data collection and cooperation procedures for direct supervision.

The AML/CFT Central Database: the backbone of a data-driven model

To deliver on its mandate; advancing supervisory convergence, enabling robust operational financial intelligence, and deepening the understanding of risks, AMLA will need a comprehensive data strategy. The AML/CFT Central Database will underpin both direct and indirect supervision across the Union. By collecting structured data from supervisory authorities, it will enhance risk identification, monitoring, and enforcement, and promote supervisory convergence and cross-border insights. AMLA's current data collection exercise is designed to test and calibrate its risk-assessment models.[10]

While the exercise collects structured data from supervisors, it will indirectly affect banks and other obliged entities by driving more standardised supervisory expectations, benchmarking and risk-driven selection/scoping. AMLA published its final report containing the RTS on the assessment of the inherent and residual risk profile of obliged entities under Article 40(2) AMLR, introducing a risk-based methodology and contains a core set of datapoints that applies to all entities and is complemented by datapoints that are specific to each sector. This methodology will assess and classify institutions' inherent risk, the quality of AML/CFT controls, and the resulting residual risk, supported by a common set of datapoints.

Although AMLA operates within a broader EU data universe that ultimately serves both the supervisory and FIU pillars, the Central Database is deliberately limited to supervisory authorities. Within the wider AMLA data ecosystem, AMLA will also leverage information gathered by FIUs and shared with AMLA, particularly strategic intelligence and aggregated data that improve understanding of EU-wide threats.

Conclusion

In short, AMLA is building a distinctly European supervision model: direct EU supervision for a small set of high-impact banks from 2028, and EU-driven convergence for the rest of the financial sector via harmonised methods, benchmarking and thematic reviews, while extending a convergence agenda into parts of the non-financial sector. The operational enabler is data: the AML/CFT Central Database and common risk methodologies are designed to reduce national divergence and lift expectations for consistent, evidence-grade AML/CFT execution across the Union.

10. Anti-Money Laundering Authority (AMLA), 'AMLA launches data collection exercise to test risk assessment models', AMLA launches data collection exercise to test risk assessment models - AMLA (accessed 20 April 2026).

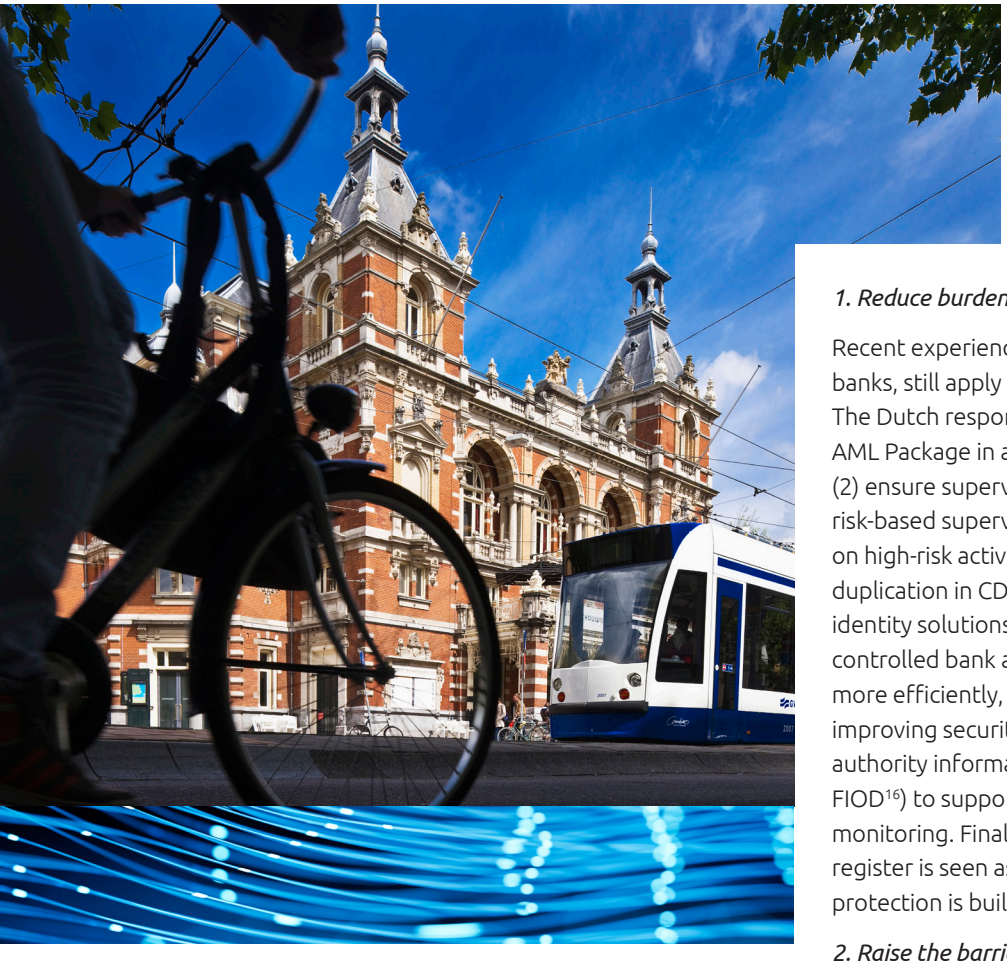
4. Implementing the EU AML Package with Minimal Regulatory Burden: The Dutch Approach

The Dutch government has made a clear political commitment: implement the EU AML Package in a way that minimises unnecessary burden. That intent is set out in the May 2025 parliamentary letter ("Kamerbrief") on the government's anti-money laundering programme,[11] alongside an overview of burden-minimising implementation choices.[12] The message is consistent: keep continuity where possible, apply proportionality in practice, and align with existing supervisory approaches.

The government explicitly recognises what many banks have experienced first-hand: the gatekeeper role has been hard to fulfil effectively, and enforcement pressure has contributed to large remediation programmes. It also acknowledges a real behavioural shift in the market: from risk-based to rule-based working, driven by fear of Wwft non-compliance and fines, and the resulting "over-compliance" burden on low-risk, bona fide customers. The policy goal under the new EU framework is to avoid repeating that cycle.

This aligns with the broader direction of the AMLR discussed earlier: the risk-based approach remains the anchor, but it becomes more harmonised and operationally testable, supported by EU-level standard-setting.

11. Rijksoverheid, 'Kamerbrief over uitwerking regeerprogramma ten aanzien van anti-witwasbeleid', Kamerbrief over uitwerking regeerprogramma ten aanzien van anti-witwasbeleid | Kamerstuk | Rijksoverheid.nl (accessed on 20 April 2026).
12. Rijksoverheid, 'Overzicht lastenluwe implementatiekeuzes AML-pakket', Overzicht lastenluwe implementatiekeuzes AML-pakket | Publicatie | Rijksoverheid.nl (accessed on 20 April 2026).



To counter the development into rule-based working, the government states that whenever the EU AML Package allows national implementation choices, the Netherlands will consistently choose for those that minimise administrative burden for obliged entities. Obliged entities can enforce risk-based working by making choices in their designs, focusing controls on the specific risks associated with their clients, while being compliant with the EU AML Package.

The new AML approach the Netherlands is signalling

Dutch parliamentary papers on the future of the financial sector frame the agenda around two outcomes: reducing burdens for bona fide businesses and citizens, and raising barriers for criminals.[13] The EU AML Package is a major step towards harmonised AML rules, making it harder to launder money or finance terrorism anywhere in the EU, and closing weak links criminals can exploit. With limited room for national tailoring under a regulation, the focus must be on burden-minimising implementation, minimising impact on citizens and businesses.[14]

1. Reduce burden where risk is low

Recent experience shows that gatekeepers, especially banks, still apply the risk-based approach inconsistently. The Dutch response is threefold: (1) implement the EU AML Package in a burden-minimising, risk-based way; (2) ensure supervisors continue to apply and improve risk-based supervision; and (3) refocus gatekeepers on high-risk activity, not low-risk customers. To cut duplication in CDD, the Netherlands is backing digital identity solutions (including eID wallets) and exploring controlled bank access to the BRP[15] to verify identity data more efficiently, reducing repeat document requests and improving security. In parallel, it is strengthening bank–authority information sharing (including with FIU-NL and FIOD[16]) to support more targeted CDD and transaction monitoring. Finally, improving the quality of the UBO register is seen as a key enabler, provided personal data protection is built in.

2. Raise the barrier for criminals

At the same time, the Dutch government frames organised crime disruption as a top priority, aiming to strengthen the ability to identify and interrupt high-risk flows. A stronger focus on the highest ML risks implies closer, more targeted cooperation between the financial sector, FIU-NL and law enforcement, so effort shifts away from low-value "tick-box" checks and towards intelligence-led action. This is done by the Dutch government by the following actions:

- EU harmonisation: the EU AML Package further harmonises AML legislation across the EU, making cross-border money laundering more difficult.
- Towards AMLA: they will push for clear, consistent and workable indicators to identify and report suspicious transactions.
- Cash payments: in addition to restrictions on cash payments for goods above a threshold, the implementation of the AML Package will introduce restrictions on cash payments for services above a threshold.

13. Kamerstukken II, 2024/2025, 32013-302, p. 9.
14. Kamerstukken II, 2024/2025, 32013-302, p. 10.
15. Basisregistratie Personen (BRP).
16. Fiscale Inlichtingen en OpsporingsDienst (FIOD).

The draft Iwt: the ambition is clear, the operational picture is not (yet)

The draft Implementing Act (Iwt) translates the AMLR and AMLD6 into Dutch legislation. It is the first real look at how Dutch discretion could translate into national rules. In principle, that's exactly what the market needs: a translation layer that clarifies what changes (and what doesn't). The concern is execution risk: key operational rules appear to be deferred to later instruments (orders in council/secondary regulation) and future EU guidance, leaving obliged entities with obligations before the "how" is fully specified.

Where these risks show up

- **FIU powers:** the broadened ability to suspend transactions/relationships illustrates the risk. While the underlying objectives are clear, the draft legislation offers little explanation of how suspensions of transactions, accounts or business relationships should operate in practice. Legitimate customers may be harmed through no fault of their own. The draft Iwt offers insufficient clarity on effective judicial protection for citizens and obliged entities impacted by FIU decisions.
- **UBO register:** the draft is not clear that certain entity types are not required to identify UBOs or SMOS, nor to register in the UBO register. If an entity is not required to register UBOs, banks should not be required to determine or record them nonetheless. This is aligned with the AMLR's risk-based approach.

Moreover, the draft Iwt appears to maintain or introduce national provisions that go further than AMLR and AMLD6, notably by broadening supervisory scope and retaining domestic obligations without a clear basis in the European rulebook. For example, the draft Iwt does not clarify whether national law is introducing a broader definition of predicate offences than the AMLR. Any deviation must be explicit and justified, because even small definitional differences can cascade into significantly wider information-sharing with national and foreign authorities.

Another example is that Article 6 of the Banking Information Reference Portal Act (Wet verwijzingsportaal bankgegevens) grants portal access to certain authorities that have no AML/CFT remit, such as the Benefits Agency of the Tax Administration (Belastingdienst Toeslagen) and the Netherlands Food and Consumer Product Safety Authority (Voedsel- en Warenautoriteit).[17] This means that banks' obligations under the AMLR and AMLD6, to provide competent AML/CFT authorities with access to customer data are effectively extended beyond what is necessary.

Granting referral-portal access to authorities without an AML/CFT mandate risks expanding data-sharing obligations beyond what the EU framework requires, undermining harmonisation and a low-burden implementation.

Conclusion

The Netherlands' stated objective is a risk-based, burden-minimising implementation of the EU AML Package, protecting low-risk clients while strengthening the fight against serious financial crime. However, the draft Iwt does not yet consistently deliver that promise: key operational rules are postponed to later instruments, while some national extensions (e.g., broader scope and wider data-access beyond AML/CFT authorities) risk increasing burden and diluting EU harmonisation.

17. Art. 6 Wet Verwijzingsportaal bankgegevens (Stb. 2020, 264).

5. One CDD Standard for Europe: The Draft RTS Blueprint

AMLA has kicked off the next step in making the AMLR operational: **a draft RTS under Article 28(1)** designed to ensure CDD is applied in the same way across Europe, for both financial institutions and designated non-financial sectors.[18] This follows the Lamfalussy logic endorsed in 2001. The AMLR is Level 1: the directly applicable rulebook setting core AML/CFT obligations. Level 2 then adds the technical detail through Commission measures, including technical- and implementing standards drafted by EU authorities.

> *This RTS will shape how firms design onboarding, review cycles and monitoring controls, and it will strongly influence supervisory expectations on what "proportionate, risk-based CDD" looks like in practice.*

AMLA positions this RTS around simplification, proportionality and a firmly risk-based approach: the risk-based principle is framed upfront as an overarching anchor and carried through the technical requirements. For obliged entities, this shift creates a clearer implementation target, enabling more streamlined CDD operating models, reduced rework across jurisdictions, and a more efficient path to compliance by aligning processes, data and controls to a single, EU-consistent standard.

The AMLR sets a single, EU-wide baseline for how CDD must be performed, requiring obliged entities to scale the information they collect and the controls they apply to the ML/TF risk of each customer, relationship or one-off transaction (adjusting scope, intensity and frequency accordingly). To pressure-test practicality and cross-sector applicability, AMLA has opened a public consultation (running 9 February-8 May 2026) to capture a wider range of views and resolve remaining implementation frictions before finalization, helping to drive supervisory convergence and more consistent oversight across the EU.

Value outcome: for firms, this convergence creates a clearer target state and accelerates delivery, enabling more standardised CDD operating models, less rework across jurisdictions, and more efficient compliance by aligning processes, data and controls to a single EU-consistent standard.

18. AMLA, 'Consultation Paper. Draft Regulatory Technical Standards under Article 28(1) of Regulation (EU) 2024/1624', 9 February 2026.

This draft RTS standardises **what to collect** for standard CDD, SDD and EDD, **how to handle non-face-to-face verification**, and **how to apply PEP and targeted financial sanctions screening**. It also requires AMLA to define:

1. the risk indicators supervisors should use when assessing limited CDD exemptions for certain prepaid/e-money products;
2. the reliable, independent sources firms can use to verify identity, and;
3. the minimum attributes electronic IDs and qualified trust services must contain to evidence customer identity and beneficial ownership/control.

Article 7 - Non-face-to-face verification measures

As digital onboarding becomes the norm, domestically and cross-border, non-face-to-face identification has shifted from a niche capability to a core control. Under Article 7, where the customer is not physically present during onboarding, the obliged entity must still obtain the required CDD data and verify identity using one remote method or a combination of methods. Corroborating customer-provided information against reliable, authentic public registers where appropriate. Compared with the EBA consultation draft, AMLA's revised RTS makes this more workable in practice: it addresses earlier concerns by removing the explicit consent requirement and replacing the prescriptive end-to-end encrypted video obligation with a technology-neutral safeguard.

Article 19 - Politically Exposed Person (PEP)

The draft RTS makes the EU's PEP framework far more "operational" by spelling out who must be screened, when, and how, linking the PEP controls to Article 20(1)(g) AMLR and the EU's single list of "prominent public functions".

In practice, firms must determine PEP status upfront (before onboarding or an occasional transaction) for the customer, the beneficial owner and, where relevant, the person acting on behalf/for the benefit of the transaction, and then keep that assessment current through ongoing checks;

- at a risk-sensitive frequency, and;
- without delay when there is new/changed CDD information, or;
- when the EU list of prominent public functions is updated.

Obliged entities are expected to run automated screening with manual verification, with a limited carve-out for manual-only approaches where automation is demonstrably disproportionate to the institution's size, business model or complexity.

The AMLR also broadens and harmonises the PEP perimeter across the EU: political party leadership (including regional/local thresholds), state-owned controlled undertakings, and regional/local authority heads (with at least 50,000 inhabitants). The definition of PEP family members is expanded to include siblings of heads of state, heads of government, ministers and deputy or assistant ministers and equivalent EU-level functions.

In practice, the 12-month 'cooling-off' period for former PEPs already exists under the Wwft through a risk-based obligation with a 12-month floor; the AMLR largely mirrors this approach, but elevates it into a clear, uniform EU rule that applies directly across Member States.

Article 21 - Ultimate Beneficial Owner (UBO)

Under the AMLR, an ultimate beneficial owner (UBO) is the natural person who ultimately owns or controls a legal entity, trust or similar arrangement. Obliged entities must be able to evidence that conclusion through prescribed identification and verification steps. The AMLR raises the bar by tightening how ownership is determined (25%+, including multiplication and aggregation of indirect holdings across all layers) and by harmonising how firms must assess both ownership and control, explicitly recognising that "control" can exist beyond shareholding.

The draft RTS then turns this into an execution standard: it requires a defined information set for customers and UBOs, expects verification before onboarding (with only narrow, risk-based deferrals), and, where relevant, proof of the client's UBO-register entry, alongside a strict obligation to report discrepancies to central UBO registers within 14 days.

Net effect: a broader scope, tighter evidencing expectations, and a more consistent, EU-wide approach to identifying the real individuals behind legal structures, including relevant third-country arrangements.

Article 33 - Grace period

In the EBA draft RTS, Article 33 remained unclear on how the grace period should operate across low/medium versus high-risk customer segments. In practice, remediation of pre-existing customer files can only start once the CDD RTS applies, so the provision needed a clearer, risk-segmented sequencing and end-state deadline framework.

AMLA's draft RTS on CDD Article 33 reads as follows: "… the documents, data and information relating to those customers shall be brought in line with the requirements of this Regulation and of Regulation (EU) 2024/1624 on a risk-sensitive basis, but in all cases not later than within the periods set out in Article 26(2) of Regulation (EU) 2024/1624."

This creates a phased, risk-based transition for existing customers, prioritising high-risk customers first, with a one-year deadline for that segment, and up to five years for the remaining existing customers, reducing immediate operational pressure while preserving convergence under the AMLR regime.

Conclusion

These articles focus on where implementation will bite first: remote onboarding/verification, UBO identification and register checks, PEP controls, and the Article 33 transition of the back book. Together, they crystallise the direction of travel, towards a more standardised, evidence-intensive EU CDD model, rolled out through staged, risk-based and proportionate implementation.

In that context, the chapter illustrates how AMLA's draft RTS under Article 28(1) AMLR operationalises Level 1 texts, setting clearer expectations on what to collect across SDD to EDD, raising the bar for non-face-to-face verification, strengthening PEP and sanctions screening, and structuring delivery through a proportionate, phased uplift model.

Value outcome: for obliged entities, the net effect is a clearer target state and a more controllable transformation, supporting simpler, more repeatable CDD processes, more consistent evidence standards across jurisdictions, and a lower-disruption uplift path for existing customers by prioritising effort where risk is highest while still converging to one EU standard.

6. What the AMLR Really Means for Artificial Intelligence in AML

Obliged entities are rapidly scaling advanced analytics and AI to improve CDD and transaction monitoring. The AMLR does not "ban AI", but it does something more consequential: it permits AI-enabled processes while tightening accountability and fundamental rights safeguards, especially where AI influences customer impacting decisions. In parallel, the AMLR positions data protection and EU fundamental rights as hard constraints for AML/CFT data processing, which matters because AI systems tend to generate additional derived insights and risk indicators that can be difficult to explain or contest. This chapter sets out what the AMLR explicitly requires, why it is designed to be compatible with the AI Act's risk logic, and what banks should implement now as a defensible operating model.

Permitted AI, mandatory safeguards (Article 76(5) AMLR)

The most direct provision on AI appears where the stakes are highest: decisions that affect a customer relationship or a customer transaction. The AMLR explicitly states that obliged entities may establish decisions via processes that use AI systems as defined in the AI Act, but only if three cumulative safeguards are met:

1. data limitation built into the tooling;
2. meaningful human intervention for customer-impacting decisions;
3. explainability and contestability, with a carve-out for suspicious transaction reporting (STR).

The AMLR permits AI to support AML operations, but it does not permit "autonomous" customer decisions without guardrails. If an AI-enabled process can lead to onboarding refusal, exit, transaction refusal, or materially stricter/lighter CDD measures, the bank must (i) keep the model's inputs within AMLR CDD data, (ii) organise meaningful human intervention, and (iii) provide explainability and a contest route, while protecting STR confidentiality where applicable.

AMLR as a fundamental-rights framework for AML data

The AMLR leaves no doubt: AML/CFT processing is not a carve-out from privacy rules. GDPR applies in full, and institutions must meet EU data-protection and fundamental-rights standards (EU Charter of Fundamental Rights) alongside AML obligations.[19]

Two practical implications stand out for AI in AML:

1. Necessity, purpose limitation, and prohibition of commercial repurposing. The AMLR stresses that collection and processing by obliged entities must remain limited to what is necessary for AML/CFT compliance, and that further processing for commercial purposes must be strictly prohibited.
2. Data subject rights remain the default, but the AMLR recognises justified limits where disclosure would undermine AML effectiveness. In particular, access to information linked to a suspicious transaction report may be restricted under GDPR Article 23,[20] especially when AI-generated signals feed suspicion assessment or reporting.

Importantly, the chapter also notes an operational reality: to respond to data subject requests (e.g., access requests), banks need a clear picture of what an AI system does and the logic behind it. It explicitly links this to the need for adequate system documentation, logs/records, and data governance, capabilities that are also core to the AI Act's compliance architecture for high-risk systems.

19. Charter of Fundamental Rights of the European Union, 2012/C 326/02.

20. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 96/46/EC (General Data Protection Regulation) (PbEU R 0679).

AMLR vs the AI Act

The analysis suggests that AMLR and AI Act take different routes, but converge on the same outcome: comparable protection of fundamental rights, through AMLR controls layered with GDPR duties and supervision. It makes this case on three points:

1. Stricter context controls: AI-assisted decisioning is constrained to AMLR Chapter III CDD data, a hard input perimeter not mirrored in the AI Act.
2. Stronger human control: the AMLR requires "meaningful human intervention" for sensitive customer decisions, going beyond the AI Act's broader "human oversight" framing.
3. Transparency with AML confidentiality: explainability must be balanced against STR confidentiality, which the analysis suggests the AI Act may not fully reflect if applied mechanically.

If you want to use AI in AML decisioning, you must design it as a controlled, audit-ready decision workflow ring-fenced to AMLR CDD data, subject to meaningful human intervention, and explainable without breaching STR confidentiality.

AI in AML: what banks should implement

Taken together, the analysis points to a practical operating model: AI can support TM/KYC/CDD, but customer-impacting decisioning must be engineered so the bank can evidence data-perimeter controls, meaningful human intervention and contestability, without compromising AML confidentiality. It also reinforces standard governance disciplines around new technology use, including DPIAs, robust data governance, and bias/discrimination controls aligned with GDPR fairness and supervisory expectations.

A practical, audit-ready approach would include:

- Data perimeter controls: clearly separating AMLR Chapter III CDD inputs from any external or commercial datasets used in customer-impacting decisions.
- Human intervention by design: defined decision workflows that specify reviewers, the evidence and rationale provided, and clear mechanisms to override or reverse outcomes when necessary.
- Explainability and recourse: customer-facing explanations and challenge routes, with a tightly governed exception where disclosure would undermine STR effectiveness.
- Documentation and DPIA discipline: robust technical/functional documentation, logging, and data governance, supported by DPIAs where required, to answer GDPR rights requests and supervisory questions.
- Bias and discrimination controls: ongoing measures to detect and mitigate bias, reflecting GDPR's fairness expectations and the recognised discrimination risk in AI-enabled compliance.

Conclusion

The AMLR permits innovation, including AI-enabled decisioning, but not at the expense of privacy and fundamental rights. It reinforces that the GDPR and EU Charter apply in full to AML processing, necessity, purpose limitation, and controlled limits on disclosure included. For banks, the challenge is evidencing an operating model that ring-fences AI to the AMLR CDD data perimeter, embeds meaningful human intervention, and delivers explainability and recourse without compromising STR confidentiality.

7. Fighting Crime, Handling Data: The Hard Line to Walk

The EU's refreshed AML/CFT framework is set to materially raise effectiveness, consistency and resilience across the financial system, but it also sharpens a critical execution challenge: balancing stronger financial crime controls with strict EU data protection expectations. The AMLR and its Level 2 standards are deliberately steering obliged entities towards more standardised, evidence-led and data-intensive CDD, while GDPR principles such as data minimisation, purpose limitation and proportionality continue to act as hard design constraints.

For banks, this isn't an abstract legal debate, it's an operational balancing act that must be engineered into onboarding journeys, beneficial ownership verification, the use of public registers, and the deployment of advanced analytics and AI. Institutions that treat this as a strategic design problem, aligning policy, data architecture, governance and control frameworks, will be best placed to improve risk outcomes, withstand supervisory scrutiny, and scale compliance efficiently.

AMLR: Scaling Compliance within GDPR Guardrails

Obliged entities are feeling the privacy-AML trade-off most acutely in customer due diligence. To meet the AMLR's EU-wide identification and verification requirements, firms must capture and maintain a relatively broad "minimum dataset" for natural persons under Article 22 (including full names, place and full date of birth, nationality/status and, where applicable, national ID number, alongside address and contact details).

In low-risk, everyday relationships, that level of systematic data capture can appear disproportionate to customers and create avoidable friction in onboarding and servicing. At the same time, the AMLR is explicit that this data intensity must be tightly governed: processing under the AMLR is limited to AML/CFT purposes and use for commercial purposes is prohibited (Article 76), with additional sensitivity around criminal-offence data that must be "strictly necessary" and protected by safeguards.

Combined with the Level 2 emphasis on proportionality and the risk-based approach, the practical implication is clear: banks need to engineer CDD as a controlled, privacy-by-design capability. Aligning data collection, verification, retention and access to risk, so they can meet supervisory expectations while protecting customer trust and scaling compliance efficiently.

CDD Data: Standardised Collection, Risk-Based Application

AMLA's draft RTS on CDD is designed to make the risk-based approach executable and consistent across the EU, but it also creates a clear tension with GDPR, especially around data minimisation. By hard-coding a more prescriptive baseline for what must be collected, verified and evidenced, the RTS can pull institutions towards broader, more uniform data capture and a heavier "verification footprint": more granular data fields, stricter expectations for document equivalence, and a greater need to corroborate information via additional sources where ID documents do not contain the required details. The result is not just "more data", but more data flows, more documents processed, and more evidence retained; precisely where customers (and privacy stakeholders) expect restraint.

At the same time, the RTS offers practical levers to keep CDD defensible under GDPR if firms apply them with discipline. It repeatedly anchors CDD decisions in proportionality, scaling scope, intensity and frequency to the customer's ML/TF risk, and it introduces a pragmatic "use what you already have" principle to avoid re-collecting information that is already available within the institution or group, reducing duplication and customer friction. It also acknowledges financial inclusion risks by allowing alternative, credible evidence routes for customers who cannot provide standard documentation, aiming to prevent unwarranted de-risking while keeping core CDD outcomes intact. In practice, the "privacy win" will depend on whether banks operationalise these risk-sensitive valves end-to-end (policy, journeys, data governance, and evidence standards) and whether supervisors reinforce that tailoring in how they test compliance.

UBO Transparency, GDPR Risk

The EU AML framework materially elevates the role of UBO registers as a core control in CDD: obliged entities are expected to rely more heavily on centralised beneficial ownership data, validate register information as part of onboarding and review, and actively report discrepancies back to the relevant register. The AMLR also expands the access model beyond a purely domestic perimeter, enabling competent authorities and obliged entities in other Member States to obtain UBO information, strengthening cross-border transparency and consistency, but also amplifying GDPR sensitivities. In practice, this creates a direct tension between the policy objective of greater traceability (through mandatory registration and wider reuse of register data) and data protection constraints that demand strict purpose limitation, data minimisation and accuracy, as well as disciplined controls over who can access what data, for which AML/CFT use case, and with what evidential safeguards.

Personal Records Database (BRP)

Enabling bank access to selected datapoints in the Dutch government Personal Records Database (BRP) places two legitimate public interests in direct tension: strengthening AML/CFT effectiveness while safeguarding citizens' personal data. The policy rationale is pragmatic: mandatory CDD under EU AML rules is currently executed through largely manual, document-heavy journeys that force customers to resubmit the same evidence, driving avoidable friction, administrative burden and error rates. Direct BRP verification (limited to identification/verification datapoints for private customers) is positioned as a way to make checks faster, more reliable and less burdensome, while reducing unintended exclusion where customers cannot produce documents quickly enough.

Sector drafts frame this as a proportionality argument: BRP access does not expand what banks must know for CDD, but improves how they obtain and validate information they would otherwise still request and store, supporting burden reduction and better customer outcomes. To keep the model defensible, it is explicitly scoped around strict safeguards, purpose limitation (no commercial use), per-bank authorisation via the National Office for Identity Data (Rijksdienst voor Identiteitsgegevens), and controls such as logging and clear processes, so access remains structured, auditable, and tied to AMLR-driven verification moments.

At the same time, privacy stakeholders view BRP access as a qualitative step-change: it extends systematic access to a comprehensive government register into the private sector, raising classic GDPR questions around necessity, data minimisation and the risk of "function creep". Even within the policy debate, boundary-setting is treated as the core design lever: limiting the scope to specific banks and specific data fields to keep the measure proportionate and legally defensible.

Notably, in March 2026 the Dutch Data Protection Authority indicated it had no objections to the proposed legislation permitting Dutch banks to access BRP under the specified conditions, reinforcing that the acceptability of the approach hinges on tight scoping and enforceable safeguards.[21]

AMLR and AI

The AMLR addresses the key risks associated with advanced technologies such as AI systems and provides safeguards for data protection and fundamental rights, as laid down in the GDPR and the EU Charter of Fundamental Rights.

In addition, the Dutch Financial Supervision Act (Wft)[22] already imposes stringent requirements on risk management, including through the principles of sound and controlled business operations. Taken together, these frameworks provide safeguards that are comparable to those set out in the AI Act for high-risk AI systems.

For that reason, imposing the detailed high-risk requirements of the AI Act on banks again, specifically for AI systems used in the AMLR context, does not appear necessary. It may even be counterproductive, as the AI Act does not fully reflect the specific data processing features and constraints inherent in AMLR compliance.

Conclusion

AMLR and AMLA's Level 2 standards are clearly pushing CDD towards a more standardised, evidence-led and data-intensive model, while GDPR remains the counterweight, enforcing minimisation, purpose limitation and proportionality. The real question for banks is no longer whether to collect more data, but how to do so in a controlled, risk-sensitive way, using the RTS's proportionality levers and "avoid duplication" logic to keep processes efficient and customer-friendly.

Nowhere is this tension more visible than in the growing reliance on shared infrastructures such as UBO registers and BRP access. These can unlock real efficiency gains, but only if tightly governed: access must be scoped, purpose-limited, logged and auditable. The Dutch DPA's "no objections" stance underscores the point: success will be determined not by policy design, but by execution discipline.

21. Autoriteit Persoonsgegevens, 'Toets wijziging Besluit BRP', Toets wijziging Besluit BRP | Autoriteit Persoonsgegevens, 27 March 2026.
22. Wet op het financial toezicht 2006 (Wft).

8. Conclusion

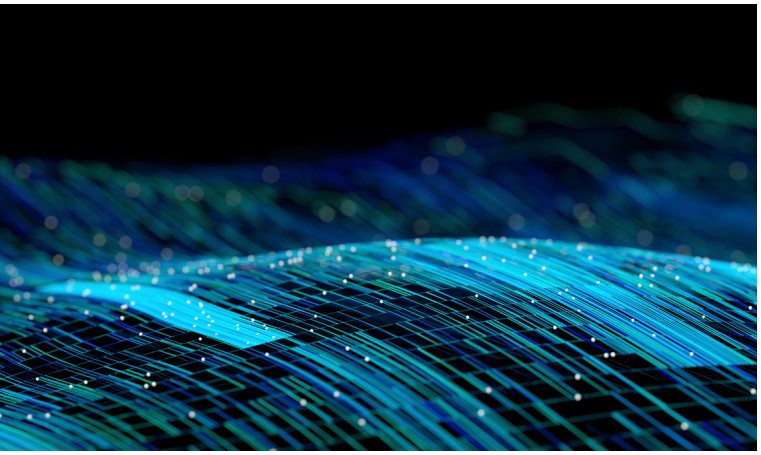
Taken together, the chapters make a single point: the AMLR is not a routine "policy refresh", but a structural change in how AML/CFT will be supervised, evidenced and delivered across the EU. The risk-based approach remains the organising principle, but it is being re-engineered from largely judgement-led practice into a more data-driven, standardised and testable discipline, backed by RTS, shared indicators and clearer expectations for how inherent risk, control quality and residual risk are assessed. Put simply, "risk-based" increasingly means "measurable and reproducible", with less tolerance for divergent national and institutional interpretations.

This direction is reinforced by AMLA's supervisory architecture and data strategy. AMLA combines direct supervision for a limited set of high-impact financial institutions with EU-level convergence mechanisms across the wider financial sector, alongside oversight tools that pull non-financial supervision towards greater consistency. For banks, the implication is practical: outcomes will increasingly hinge on structured, comparable data and on the ability to show that decisions can be explained and repeated across entities and jurisdictions.

The Dutch policy direction is the right one: restore genuinely risk-based gatekeeping and reduce unnecessary friction for bona fide customers under the new EU framework. But delivering on that promise is execution dependent. The Iwt needs to provide earlier operational clarity and demonstrably stay within the "European lanes"; otherwise, national additions and delayed detail will push firms back into the very rule-based behaviour the government is trying to prevent.

Operationally, AMLA's draft RTS on CDD is positioned as the blueprint for a single EU-wide CDD execution standard. It translates Level 1 obligations into concrete requirements across SDD, standard CDD and EDD; sets expectations for verification methods (including non-face-to-face onboarding); tightens UBO and PEP controls; and defines a risk-sensitive uplift path for existing customers through Article 33 RTS on CDD and the reference timelines in Article 26(2) AMLR. This improves target-state clarity and convergence, but it also raises the bar for operating model discipline: process, data, controls and documentation must function as one integrated system.

Finally, the privacy chapter brings the strategic tension into sharp focus. The framework drives more data and shared checks, while GDPR principles (data minimisation, proportionality and accuracy) operate as hard design constraints. The upside isn't automatic: benefits only with tightly scoped, purpose-limited, logged and auditable access, and proportionality applied in day-to-day execution.



Bottom line: AMLR readiness is a transformation programme: not a compliance checklist. It requires banks to deliver one EU-consistent way of working, supervisory-grade, data-driven evidence, and GDPR-compliant restraint in parallel.

Capgemini's FCC practice helps banks move from interpretation to execution: translating AMLR into clear operational requirements and a delivery roadmap, then implementing the change across the Target Operating Model, CDD processes, data foundations and evidence frameworks. It typically starts with an AML Quick Scan and AMLR gap analysis, followed by prioritised remediation and hands-on transformation, optionally supported by AI-enabled KYC and scalable delivery capacity so compliance becomes repeatable, auditable and sustainable.

Glossary

Abbreviation

AI	Artificial Intelligence
AML	Anti-Money Laundering
AMLA	Anti-Money Laundering Authority
AMLD6	The sixth Anti-Money Laundering Directive
AMLR	Anti-Money Laundering Regulation
BO	Beneficial Ownership
BRP	Dutch government Personal Records Database (Basisregistratie personen)
CDD	Customer due diligence
CFT	Countering the Financing of Terrorism
EBA	European Banking Authority
EDD	Enhanced Due Diligence
EU	European Union
FIU	Financial Intelligence Unit
GL	Guideline
ITS	Implementing Technical Standard
Iwt	Implementing act (Implementatiewet ter voorkoming van witwassen en terrorismefinanciering)
KYC	Know Your Customer
ML	Money Laundering
NCA	National competent authority
PEP	Politically exposed person
RTS	Regulatory Technical Standard
SDD	Simplified due diligence
TF	Terrorism financing
UBO	Ultimate beneficial owner
Wwft	Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme)

Editor or contact

Capgemini The Netherlands | Amsterdam

Authors

David Zwarts LL.M.

Global Head of Financial Crime Compliance Academy | Director

Maylin Schouten LL.M., MSc.

Senior Consultant Financial Services Financial Crime Compliance

Fabienne Bos, MSc.

Consultant Financial Services Financial Crime Compliance

Publication year

June 2026

About Capgemini

Capgemini is an AI-powered global business and technology transformation partner, delivering tangible business value. We imagine the future of organizations and make it real with AI, technology and people. With our strong heritage of nearly 60 years, we are a responsible and diverse group of over 420,000 team members in more than 50 countries. We deliver end-to-end services and solutions with our deep industry expertise and strong partner ecosystem, leveraging our capabilities across strategy, technology, design, engineering and business operations. The Group reported 2025 global revenues of €22.5 billion.

Make it real. | www.capgemini.com

Capgemini

08-004.26