

Insights and Analysis

AI in AML compliance: Navigating human intervention under the AML regulation

31 August 2026

AI is rapidly moving from experimentation to operational use in anti-money laundering and counter-terrorism financing (AML/CTF) compliance. Financial institutions are increasingly exploring AI-driven tools for customer onboarding, transaction monitoring and investigative workflows.

EU law permits AI in AML/CTF, but only within a complex framework shaped by the AI Act, the GDPR and the new AML Regulation, among other. The key question is not whether AI can be used, but what level of human involvement is required before AI-generated AML/CTF outputs may influence onboarding, transaction execution, customer due diligence decisions or suspicious activities reporting.

A permissive framework – but with significant strings attached

EU law does not prohibit the use of AI in AML/CTF compliance. The more difficult point is that AI-enabled AML/CTF tools sit at the intersection of several regulatory regimes that do not always use the same concepts, thresholds or terminology.

AI Act

The AI Act is an important starting point. Its risk-based approach creates particular complexity for financial institutions

AI systems used to assess creditworthiness are classified as high-risk under Annex III, whereas AI systems used to detect financial fraud are expressly carved out from that category. Many AML/CTF tools will not fit neatly on one side of these lines. In practice, the same system may support risk assessment, fraud detection, money laundering monitoring and customer due diligence workflows. That classification question matters. If a system is wrongly assumed to fall outside the high-risk category, it may not be designed to meet the AI Act's requirements on risk management, human oversight, technical documentation and fundamental rights impact assessment.

Certain AI systems that impose adverse consequences on individuals based on inferences about their behaviour, personality or profile are prohibited (Article 5(1) (c) and (d) of the AI Act). Such inference is very close to what AML/CTF applications of AI systems will be built for. Appropriate design will thus be key to their practical implementation.

As the Commission's Guidelines on prohibited AI practices indicate, compliance of these AI systems with the AML Regulation is necessary to ensure that they fall outside the scope of the prohibitions in Art. 5(1)(c) and (d) of the AI Act. The Commission's guidance seeks to draw a workable line between assessments grounded in legally prescribed data and processes and those based on more general individual profiling. However, that distinction may sit uneasily with the risk-based architecture of the AML/CTF framework. AML/CTF compliance is not purely rule-based. It requires obliged entities to assess risk contextually, drawing on multiple data points and patterns. AI-enabled AML/CTF tools should therefore be assessed carefully against Article 5(1) (c) and (d), rather than treated as automatically permissible merely because they are deployed for AML/CTF purposes.

The GDPR: a layer that is easy to underestimate

The GDPR adds a further layer that is sometimes underestimated in the AML context. Any AI-based AML process must comply with core data protection principles, regardless of whether the system produces automated decisions within the meaning of Article 22 GDPR. Legal basis, transparency, data minimisation, purpose limitation, accuracy and security each impose their own requirements.

Transparency obligations are a particular pressure point. Institutions frequently process data relating to natural persons — including beneficial owners, directors and signatories — even where the customer is a legal entity. Whether, and in what form, those individuals must be informed about AI-driven processing depends on the specific data flows, jurisdictions and institutional structures involved.

Article 22 GDPR raises further questions. It applies where a decision is made solely on the basis of automated processing, including profiling, and produces legal or similarly significant effects on a natural person. Both elements may be contested in the AML context.

Institutions sometimes assume that the presence of a compliance officer in the workflow is enough to take the process outside Article 22. That assumption is risky. Where human review amounts in practice to routine sign-off on AI-generated outputs rather than a genuine independent assessment, regulators and courts may view the decision as substantially automated.

The effects threshold also requires careful analysis. An AML decision may formally concern a corporate customer, but the underlying assessment may involve natural persons such as beneficial owners, directors or signatories. Where the AI output materially influences access to financial services or the level of scrutiny applied to those individuals, it cannot simply be assumed that Article 22 is irrelevant.

Where Article 22 applies, the required safeguards are substantive. The legal basis most likely to be relevant in AML — authorisation by Union or Member State law under Article 22(2)(b) — requires more than a general reference to AML legislation. Equally, satisfying the AML Regulation's meaningful human intervention requirement will not automatically satisfy the GDPR's safeguard obligations.

Article 76(5) AMLR: the central compliance challenge

The new AML Regulation provides the most operationally direct set of rules. Article 76(5) is likely to become the central provision for AI-enabled AML/CTF workflows because it addresses decisions resulting from automated processes or AI systems.

Article 76(5) sets out three cumulative conditions.

- First, the data processed must be limited to information obtained in the course of customer due diligence under Chapter III of the AML Regulation. On a strict reading, this may exclude information received from a financial intelligence unit and may also raise questions regarding information received through information-sharing partnerships under Article 75 and relevant information otherwise available to or obtainable by the financial institution. If interpreted narrowly, this could require institutions to operate AI systems on incomplete or decontextualised datasets, potentially affecting the accuracy of outputs.
- Second, decisions on entering into or refusing a business relationship, executing or refusing a transaction, or adjusting the level of customer due diligence must be subject to meaningful human intervention to ensure the accuracy and appropriateness of the decision.
- Third, customers must generally be able to obtain an explanation of the decision and challenge it.

These requirements raise difficult questions. What makes human intervention meaningful? Is the list of decisions in Article 76(5)(b) exhaustive? At what stage is a “decision” reached? Is the list of relevant decisions exhaustive (note that decisions in the context of suspicious activities reporting are not included in this list)? What standard of explanation is required where the underlying AI model is complex or opaque? And how should institutions reconcile Article 76(5) with Article 75(4)(g), which uses the related but different language of adequate human oversight for AI-generated outputs shared within information-sharing partnerships?

Meaningful human intervention

The core interpretative question is open to further calibration. One reading of Article 76(5)(b) is that it requires active human validation before a relevant AI-generated decision takes effect. On that view, the AML Regulation imposes a demanding human-in-the-loop model for key AML/CTF decisions.

Another reading is that Recital 150 AMLR, by cross-referring to Article 22 GDPR, points towards a more calibrated approach. On this interpretation, automated AI-based decision-making is not excluded in principle, provided that it is accompanied by appropriate safeguards, governance structures, escalation routes and targeted human review.

With a view to the AI Act, the difficulty is that the AML Regulation uses the language of “intervention”, while the AI Act more commonly speaks of “oversight”. The two concepts are related but not necessarily identical. Intervention may suggest a human ability to affect the individual decision before it takes effect. Oversight may, depending on context, involve monitoring, escalation and the ability to intervene where needed. For de-risking decisions and decisions about the level of customer due diligence, Article 76(5) may or may not therefore set a more demanding standard than the AI Act's general high-risk system oversight requirements.

The AMLA's draft Guidelines on ongoing monitoring of a business relationship permit automated (including AI-based) closure of monitoring outputs unless in the presence of high-risk indicators and subject to effective human “oversight”. However, there is currently no definitive supervisory guidance that resolves this ambiguity, particularly in light of the continuously increasing capabilities of AI systems. .

Human oversight in practice: where the legal risks crystallise

The legal risk is not simply whether a human appears somewhere in the workflow. The more important question is whether the human review is capable of ensuring the accuracy and appropriateness of the decision.

That assessment depends on practical factors: the seniority and expertise of the reviewer, the number and frequency of outputs reviewed, the information available to the reviewer, the extent to which the reviewer understands the system's logic, and whether the review process is genuinely capable of changing outcomes. A high-volume process in which reviewers routinely approve AI-generated outputs is in a very different legal position from a process that is substantive, documented and capable of identifying errors.

Supervisors are unlikely to stop at asking whether a person was involved. They are more likely to ask whether the institution can demonstrate that human involvement was meaningful in practice. That requires evidence, not just policy.

The AMLR and GDPR: calibration, not contradiction – but whose calibration?

The reference to Article 22 GDPR in Recital 150 AMLR supports a reading in which automated decision-making can, in principle, be compatible with AML/CTF compliance where appropriate safeguards are in place. In that sense, the AML Regulation and the GDPR may be understood as requiring calibration rather than imposing a direct contradiction.

That calibration is not, however, predetermined. The AI Act and the AML Regulation were adopted in the same broad legislative period, but they do not always align neatly with the GDPR or with each other. Conceptual and practical inconsistencies remain, particularly around classification, automated decision-making, human involvement and explainability.

How supervisors and courts will resolve those ambiguities remains to be seen. Institutions that wait for complete clarity before reviewing their compliance frameworks may find that they have already made design choices that are difficult and costly to reverse.

Practical takeaways for financial institutions

- Map where AI is or can be used across AML/CTF workflows, including onboarding, screening, transaction monitoring, alert prioritisation and investigations.

- Classify each AI system under the AI Act and document the rationale.
- Assess whether Article 5(1)(c) or (d) of the AI Act could be engaged, particularly where natural persons are profiled or assessed for financial crime risk.
- Analyse whether Article 22 GDPR is relevant, including where decisions formally concern corporate customers but materially affect natural persons.
- Define what meaningful human intervention means for each relevant decision point and ensure that, where necessary, reviewers have sufficient information, authority and time to challenge AI outputs.
- Document explanation and challenge mechanisms so that they are operational, not merely theoretical.

Conclusion: uncertainty is not a reason to wait

The EU framework does not prohibit the automation of AML/CTF processes. But the conditions under which automation is legally permissible are complex, layered and, in important respects, not fully resolved.

The question of what Article 76(5) AMLR requires in practice sits at the heart of that uncertainty. For de-risking decisions and decisions about customer due diligence, the AML Regulation may require a level of human involvement that goes beyond general AI Act oversight concepts.

For financial institutions investing in AI-based AML/CTF infrastructure, the compliance risks are real. Decisions made now about system design, data governance, human review and explainability will shape both regulatory compliance and legal exposure. Until supervisory practice and case law provide greater clarity, those decisions should be made deliberately, documented carefully and tested against all three regimes.

Authored by David Bamberg and Max von Cube.

Contacts



Dr. Martin Pflueger

Partner

 Munich

 [Email me](#)



Dr. Richard Reimer

Partner

 Frankfurt

 [Email me](#)



David Bamberg

Counsel

 Munich

 [Email me](#)



Max von Cube

Senior Associate

 Frankfurt

 [Email me](#)