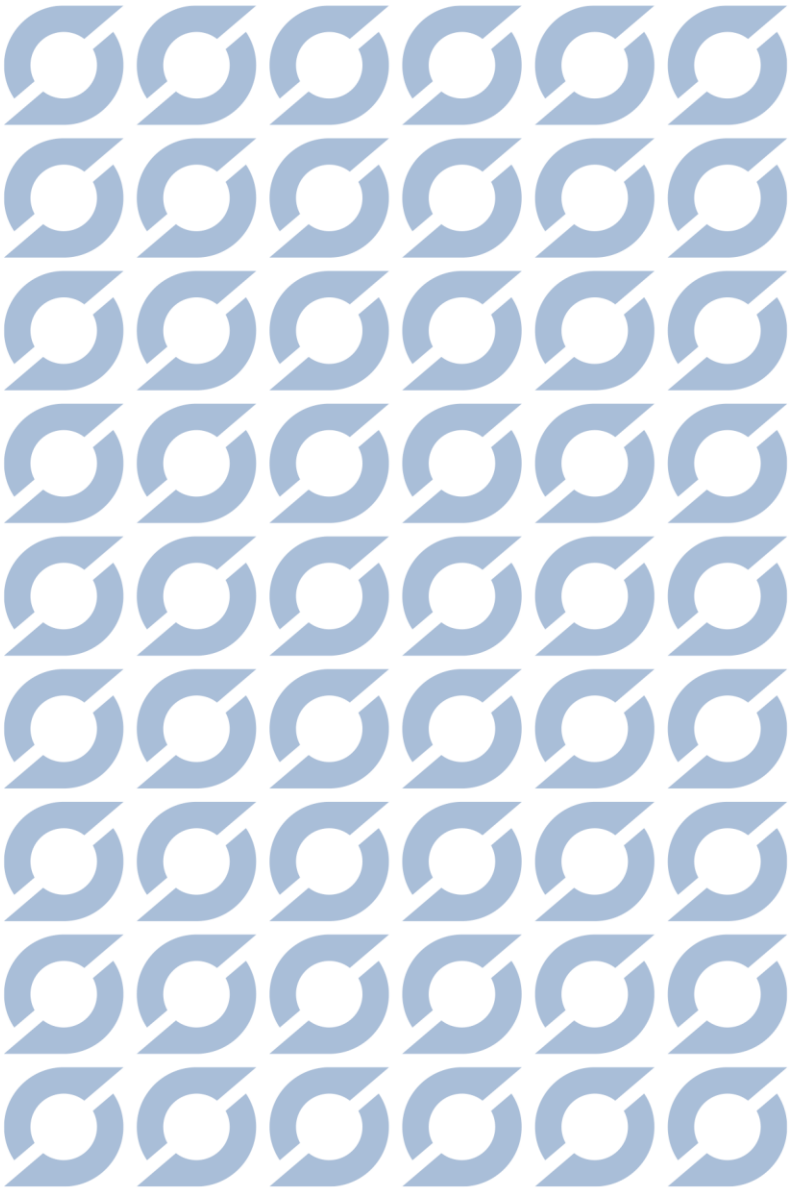
Ref. Ares(2026)8137938 - 25/08/2026

Consultation Paper

Draft Guidelines on ongoing monitoring of a business relationship under Article 26(5) of Regulation (EU) 2024/1624



AMLA
Anti-Money Laundering Authority

Frankfurt am Main – 3 June 2026

Contents

1 Responding to this consultation **2**

1.1 Submission of responses 2

1.2 Publication of responses 2

1.3 Data protection 2

1.4 Who should read this Consultation Paper? 2

2 Executive Summary **4**

2.1 Next steps 5

3 Background and rationale **6**

3.1 General considerations 6

3.2 AMLA's approach 7

3.3 Interaction with other L1/2/3 instruments 9

3.4 GUIDELINES STRUCTURE 10

4. Draft Guidelines **13**

5. Accompanying documents **42**

5.1 Impact assessment with cost-benefit analysis 42

5.2. Overview of questions for consultation 54

1 Responding to this consultation

The Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) invites comments on all proposals set out in this Consultation Paper and in particular on the specific questions summarised in Section 5.2.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices AMLA should consider.

1.1 Submission of responses

To submit your comments, click on the 'respond' button on the consultation page by 03.09.2026. Please note that comments submitted after this deadline or submitted via other means may not be processed.

1.2 Publication of responses

All contributions received will be published following the close of the consultation, unless you request otherwise. Please clearly indicate in the consultation form if you wish your comments to be treated as confidential. A confidential response may be requested from us in accordance with Regulation 1049/2021 regarding public access to European Parliament, Council and Commission documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the European Ombudsman.

1.3 Data protection

The protection of individuals with regard to the processing of personal data by AMLA is based on Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018. Further information on data protection can be found under the Legal Notice section of the AMLA website.

1.4 Who should read this Consultation Paper?

All interested stakeholders are invited to respond to this Consultation Paper. In particular, AMLA encourages obliged entities from the financial and the non-financial sectors to participate.

2 Executive Summary

These guidelines set out the Authority for Anti-Money Laundering and Countering the Financing of Terrorism's (AMLA) proposed approach to deliver on its mandate on the ongoing monitoring of business relationships under Article 26(5) of Regulation (EU) 2024/1624 (AMLR). These guidelines aim to ensure a proportionate, effective and risk-based application of ongoing monitoring obligations across all obliged entities.

Ongoing monitoring is an integral component of customer due diligence and is essential to maintaining an accurate understanding of the customer and identifying changes that may indicate money laundering or terrorist financing (ML/TF) risks including, where relevant, risks related to the non-implementation or evasion of targeted financial sanctions. The guidelines establish horizontal principles applicable to all obliged entities - both financial and non-financial sector - and clarify how ongoing monitoring, including the monitoring of transactions and activities, should be designed and implemented in practice. They aim to take into account the diversity of business models, data availability, and the need for proportionate and technologically neutral requirements.

The first part of these guidelines outlines expectations for keeping customer documents, data and information up to date, through both so called periodic and event-driven reviews, applied in line with a risk-based approach. It sets out the sources of information that may be used by obliged entities to update the CDD information and shares non exhaustive lists of information that obliged entities should consider and assess during periodic customer information reviews and event-trigger reviews.

The second part of these guidelines clarifies how obliged entities should design, implement and test monitoring frameworks to detect unusual or suspicious transactions and activities. It sets out proportionate approaches, including the use of manual, automated or semi-automated processes and controls and, where appropriate, advanced analytical tools. It also establishes expectations for the effective assessment and escalation of monitoring outputs and reinforces the importance of integration of monitoring with customer due diligence to support a holistic and up-to-date understanding of customer behaviour.

Across the guidelines, AMLA emphasises proportionality, cross-sectoral applicability, and the importance of a sound business-wide risk assessment as the basis for effective ongoing monitoring. The draft also reflects the need for clear governance, adequate documentation, appropriate staff training, and the responsible use of advanced analytical tools, supported by effective human oversight, where needed.

Taken together, the guidelines aim to promote supervisory convergence, strengthen the effectiveness and consistency of ongoing monitoring practices across the Union, and thereby contribute to the fight against money laundering and terrorist financing.

In preparing this consultation paper, AMLA sought and considered input from national supervisors across financial and non-financial sectors as well as from data protection experts. The draft guidelines are designed to ensure consistency with the broader AML Single Rulebook and other AMLA instruments currently under development.

AMLA invites stakeholders to provide feedback on the proposed approach to ensure that the final guidelines support a clear, practical and proportionate implementation of Article 26 of AMLR across all sectors. To further support obliged entities, in particular smaller ones, AMLA will consider developing tailored communication materials to accompany the guidelines, including factsheets and/or explainers.

2.1 Next steps

This Consultation Paper is published for a three-month period. AMLA will consider the feedback to this consultation when preparing the final guidelines, that will be issued in Q4 2026.

3 Background and rationale

3.1 General considerations

Regulation (EU) 2024/1624 (AMLR) aims for harmonisation of the measures to be put in place to prevent money laundering, its predicate offences and terrorist financing. To this end, Article 26(5) of AMLR mandates AMLA to issue guidelines specifying how obliged entities should perform ongoing monitoring of a business relationship, including the monitoring of the transactions and activities carried out in the context of such relationship.

Ongoing monitoring constitutes a core element of the customer due diligence requirements under AMLR. Article 26 of AMLR requires obliged entities to conduct customer due diligence reviews both periodically and on an ongoing basis to identify any relevant changes in customer information. Furthermore, obliged entities must perform transaction and activity monitoring as part of their ongoing monitoring obligations to ensure that transactions and activities undertaken throughout the course of the business relationship are consistent with the entity's knowledge of the customer, the customer's business activities, and risk profile, and, where appropriate, with information on the origin and destination of funds. This process should enable the detection of transactions and activities that warrant enhanced scrutiny, and potentially reporting, in accordance with Article 69(2) of AMLR.

These draft guidelines support a common, uniform and consistent understanding of the ongoing monitoring obligation across sectors and business models. They aim to ensure a consistent, efficient and effective application of these obligations.

Obliged entities are also required to consider risks related to the non-implementation or evasion of targeted financial sanctions as part of their overall AML/CFT framework. While these risks remain relevant in the context of ongoing monitoring, this guideline does not specify how such risks should be operationalised within monitoring frameworks. Ongoing monitoring should as part of the broader control framework, support the identification and escalation of unusual or suspicious transactions and activities, including patterns or behaviours that may indicate potential evasion of targeted financial sanctions, where they arise in the context of a business relationship.

Monitoring of transactions and activities

These guidelines aim to assist obliged entities in the practical implementation of their ongoing monitoring obligations, including the monitoring of transactions and activities. The reference to "monitoring of activities" has been introduced by AMLA to reflect the diversity of services and business models covered by AMLR, in which activity monitoring constitutes a central element for certain categories of obliged entities. The monitoring of 'transactions and activities' is used as the

standard wording in these guidelines to ensure that where obliged entities have the possibility to cover both transactions and activities, they should ensure that both are equally monitored.

These guidelines establish the core principles with which obliged entities should comply and which apply horizontally to all obliged entities.

Periodic customer information review

Obliged entities should periodically review customer information in accordance with Article 26(2) of AMLR. Feedback from several obliged entities indicates that a standard periodic review may not always be appropriate for certain business models, particularly where a business relationship exists but no new activity or services are provided over an extended period (e.g. in the context of a property sale that is completed after several years).

A core principle of these guidelines is that obliged entities may adjust the depth and intensity of periodic reviews, taking into account factors such as the absence of new activity or services, alongside the overall risk profile of the customer. There is no prescriptive definition of when such adjustments are appropriate nor how this review should be performed; rather, obliged entities are expected to assess each situation and determine the appropriate approach in line with the risk-based approach, with a view to effectively mitigating ML/TF risks.

3.2 AMLA's approach

AMLA was guided by the principles of legal certainty and proportionality while aiming for horizontal applicability, technological neutrality and a risk-based approach. This ensures that the draft Guidelines provide sufficient flexibility for obliged entities to apply the most effective and proportionate measures, while remaining applicable across both the financial and non-financial sectors.

Simplification principle

In drafting the Guidelines, due consideration was given to the objectives of the EU simplification agenda. Simplification has been incorporated, in particular, through the establishment of simple and horizontal principles applicable to all obliged entities. These include:

- the articulation of clear core principles relevant to both financial and non-financial sectors, allowing for flexible, effective and proportionate implementation; and
- the adoption of a risk-based approach to customer due diligence updates, including expired identity documents, passports or equivalent which are not required to be re-collected by default, but only where justified on the basis of a proper risk assessment.

These elements support a reduction of the compliance burden for obliged entities, in comparison to current practices, as the text focuses on effective outcomes rather than prescribing how they

should be achieved, allowing each entity to determine the appropriate approach based on its business-wide risk assessment. In addition, the text promotes a risk-based approach to the design and implementation of a sound transaction and activity monitoring framework, aligned with the nature, risks and complexity of their business, as well as the size of the obliged entity.

Finally, the guidelines have been aligned, with other relevant AMLA mandates covering related aspects, including on business-wide risk assessment, defining business relationships, occasional and linked transactions and the customer due diligence requirements.

Proportionality

In applying these guidelines, proportionality should be understood as relating to the design, calibration and operation of ongoing monitoring measures. Obliged entities can determine the tools, methods and processes that address and capture best the ML/TF risks associated with the nature, risks and complexity of their business, as well as the size of the obliged entity, enabling the timely identification and escalation of material ML/TF risks. Ongoing monitoring measures should be commensurate with the nature, risks and complexity of their business, as well as the size of the obliged entity and be capable of identifying transactions and activities that require more detailed assessment. Obliged entities, irrespective of their size, should ensure the effective application of the principles set out in these Guidelines. Proportionality should not be understood as implying lower or weaker standards for smaller obliged entities; rather, it requires obliged entities to assess a range of relevant factors when applying the principles of these guidelines, of which size is only one, alongside considerations such as the overall risk profile, the complexity and scale of activities and operations, the business model and the nature of the business. Obliged entities should ensure that the outcomes envisaged by these guidelines are effectively achieved.

Technological neutrality and use of technology

Technological neutrality is one of the key principles underpinning these Guidelines. The Guidelines do not prescribe the use of certain tools and do not mandate the use of automated systems. Obliged entities may determine the tools, processes and controls they use, whether manual, automated or semi-automated, provided that they ensure the effective identification and escalation of ML/TF risks in line with Article 26 of AMLR.

The Guidelines also clarify that automated and advanced analytical tools, including AI, should be considered where they enhance the identification and escalation of ML/TF risks. Their use is neither mandatory nor, in itself, an indicator of effectiveness, which should be assessed by reference to the timely detection and escalation of ML/TF risks. Where such tools are used, obliged entities should ensure proportionate safeguards and governance and be able to explain their role and outputs to competent authorities, including where third-party providers are relied upon.

Cross-sectoral applicability

A key objective of these guidelines is to underline that ongoing monitoring extends beyond transaction monitoring in a narrow sense. It also includes the monitoring of activities, behaviours, events and changes in circumstances that may indicate deviations from the customer's established risk profile or the emergence of unusual or potentially suspicious patterns, including at points in the business relationship where ML/TF risks are most likely to arise or change. This ensures that Article 26 of AMLR can be implemented effectively across both financial and non-financial sectors including in cases where ongoing monitoring relies primarily on periodic reviews, the monitoring of activities, relevant events, or changes that occurred during the business relationship rather than on continuous payment flows.

During the drafting process AMLA invited and considered stakeholder input from national supervisory authorities responsible for the financial and non-financial sector and AMLA's Expert Network. In addition, AMLA liaised closely with the European Commission.

3.3 Interaction with other L1/2/3 instruments

These guidelines interact with other level 1, level 2 and level 3 measures adopted or will be adopted under AMLR, AMLAR and AMLD, which provide complementary detail on related obligations, including:

Instrument / legal basis	What it covers	Relevance for ongoing monitoring
Guidelines – Article 10(4) AMLR	Business-wide risk assessment	A robust BWRA underpins the risk-based- approach and is essential for applying the core principles of ongoing monitoring.
Article 9 AMLR & future Guidelines (Art. 9(4))	Internal policies, procedures and controls	Ongoing and transaction monitoring must be embedded in internal frameworks and regularly reviewed or audited. In addition, obliged entities must consider risks of non-implementation or evasion of targeted financial sanctions and, although sanctions compliance falls outside these guidelines, ongoing monitoring should help identify and escalate such risks where they arise in a business relationship

RTS – Article 19(9) AMLR	Defines business relationships, occasional and linked transactions	Determines when ongoing monitoring applies. 'Linked transactions' differ: under Art. 19(9) they prevent CDD circumvention; in these Guidelines they support detection of unusual or suspicious activity.
RTS – Article 28(1) AMLR	Customer due diligence requirements	Initial CDD determines what must be reviewed or updated during ongoing monitoring.
Guidelines – Article 69(5) AMLR	Indicators of suspicious activity/behaviour	Supports detection of transactions and activities requiring further assessment and complements AMLA's mandate to issue indicators of suspicious behaviour.
Article 8 AMLAR and Article 40(3) AMLD	AML/CFT supervisory methodology and risk-based supervision guidelines	The implementation of the supervisory methodology and risk-based supervision should align with the content and principles of these guidelines. These guidelines should be considered by competent authorities when assessing the effectiveness of obliged entities ongoing monitoring framework.

3.4 GUIDELINES STRUCTURE

General Guidelines – Key principles and proportionality

This part lays out general principles which apply for both guidelines 1 and 2. It covers key principles for ongoing, risk-based monitoring, including periodic reviews, event triggers and transaction and activity monitoring. It highlights the importance of staff training, and it refers to the key principle of proportionality, requiring monitoring measures and data collection to be commensurate with the obliged entity's risk profile.

Guideline 1 - Keeping customer documents, data or information up to date

This guideline sets out how obliged entities should ensure that customer information remains accurate and up to date throughout the business relationship.

Updating customer information is an ongoing process and includes:

- periodic reviews, and
- updates triggered by specific events (e.g. changes in a customer's behaviour or circumstances).

The frequency and extent of updates should be risk-based, taking into account:

- the customer's risk level and overall risk profile, and
- the information already held

The guideline also refers to:

- which sources they can use to update the customer information; and
- a risk-based approach to decide whether to update an expired identification document or equivalent.

Overall, the aim is to help obliged entities maintain accurate customer information in a way that is proportionate, risk-focused, and practical for day-to-day operations.

Guideline 2 – Transaction and activity monitoring framework

This guideline sets out how obliged entities should design and operate an effective monitoring framework to detect unusual or suspicious transactions and activities.

Monitoring should be based on the nature, risks and complexity of their business, and the size of the obliged entity as well as on:

- the obliged entity's overall business-wide risk assessment; and
- its knowledge of its customers

Depending on the obliged entity's business model, products and services offered, it may include:

- pre-transaction checks
- real-time monitoring
- post-transaction reviews

In non-financial sectors, and more generally where obliged entities do not execute or control transactions or where business relationships are not continuous, pre-transaction or real-time monitoring may not be applicable. In such cases, monitoring is primarily achieved through customer due diligence measures, the assessment of instructions, mandates or assets prior to engagement, and through event-driven or post-activity reviews, in line with the obliged entity's role, and risk exposure.

The guideline also covers:

- the handling and escalation of monitoring outputs;
- the identification of linked or related activity across products, channels, or customers; and
- the integration of monitoring with customer due diligence.

Monitoring may be:

- manual
- automated
- semi-automated

as long as it is explainable, regularly tested, properly documented, and proportionate to the size, nature, complexity, transactions and activities volume, and risk exposure of the obliged entity.

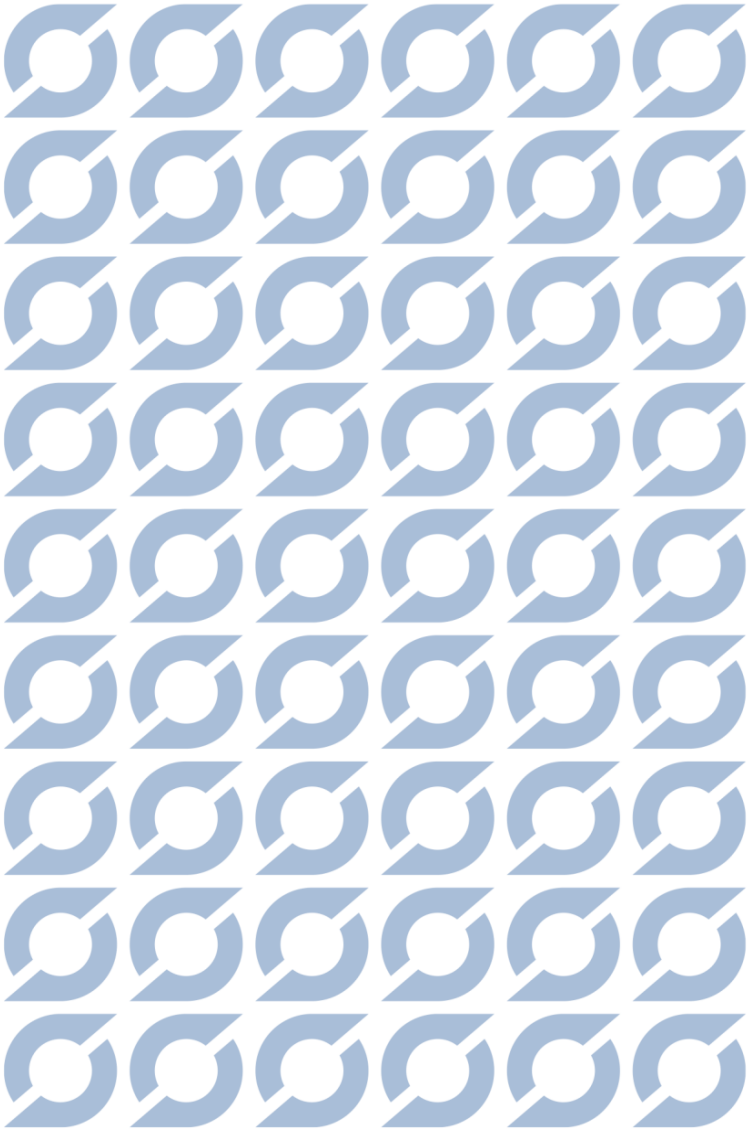
To ensure ongoing effectiveness, obliged entities should regularly:

- test and recalibrate their systems, and
- perform appropriate assurance checks

The overall aim is to ensure that monitoring frameworks remain effective, risk-based, and proportionate across different types of obliged entities.

4. Draft Guidelines

Draft Guidelines on ongoing monitoring of a business relationship under Article 26(5) of Regulation (EU) 2024/1624



Contents

1 Subject matter, scope and definitions 16

1.1 Subject matter and scope of application 16

1.2 Addressees 16

1.3 Legislatives references, abbreviations and definitions 16

LEGISLATIVE REFERENCES 16

Abbreviations 17

Definitions 17

2 DRAFT GUIDELINES 19

2.1 GENERAL GUIDELINES 19

Proportionality 20

GUIDELINE 1: KEEPING CUSTOMER DOCUMENTS, DATA OR INFORMATION UP TO DATE 22

2.2 UPDATE OF CUSTOMER DOCUMENTS, DATA OR INFORMATION AND ONGOING MONITORING 22

2.3 PERIODIC CUSTOMER INFORMATION REVIEWS 23

2.4 EVENT-DRIVEN REVIEWS 25

2.5 Use of suspension or restriction measures in the absence of updated customer information 27

GUIDELINE 2: TRANSACTION AND ACTIVITY MONITORING FRAMEWORK 29

2.6 GENERAL PRINCIPLES 29

2.7 MONITORING FRAMEWORK USING MANUAL, AUTOMATED, OR SEMI-AUTOMATED PROCESSES AND CONTROLS 31

2.8 LINK BETWEEN CUSTOMER DUE DILIGENCE AND THE ONGOING MONITORING FRAMEWORK 33

2.9 IMPLEMENTATION OF THE MONITORING FRAMEWORK 35

2.10 INTERNAL CONTROLS AND ONGOING REVIEW 38

2.11 USE OF TECHNOLOGY 40

5. Accompanying documents 42

5.1 Impact assessment with cost-benefit analysis 42

5.2. Overview of questions for consultation 54

1 Subject matter, scope and definitions

1.1 Subject matter and scope of application

1. These guidelines set out specific rules obliged entities should apply when fulfilling the obligations of conducting ongoing monitoring of a business relationship and the monitoring of transactions and other risk relevant activities carried out in the context of such relationship pursuant to Article 26(5) of Regulation (EU) 2024/1624.

1.2 Addressees

2. These guidelines are addressed to obliged entities as defined in Article 3 of Regulation (EU) 1624/2024 and supervisory authorities as defined in Article 2(1), point (46) of Regulation (EU) 1624/2024 responsible for supervising these obliged entities compliance with their anti-money laundering and counter-terrorist financing (AML/CFT) obligations.

1.3 Legislatives references, abbreviations and definitions

LEGISLATIVE REFERENCES

AMLR	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 (Text with EEA relevance)[1]
AMLAR	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[2]
PSR	Proposed Regulation (EU) on payment services in the internal market and amending Regulation (EU) No 1093/2010

[1] OJ L, 2024/1624, 19.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1624/oj

[2] OJ L, 2024/1620, 19.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1620/oj

GDPR	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 95/46/EC (General Data Protection Regulation)[3]
PAD	Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features[4]
TFR	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[5]

Abbreviations

AML/CFT	Anti-money laundering and countering the financing of terrorism
AMLA	Authority for Anti-Money Laundering and Countering the Financing of Terrorism
IP address	Internet protocol address
FIU	Financial Intelligence Unit
ML	Money laundering
TF	Terrorist financing
PEP	Politically Exposed Person
RTS	Regulatory Technical Standards
TFS	Targeted Financial Sanctions

Definitions

3. Unless otherwise specified, terms used and defined in AMLR have the same meaning in the guidelines. In addition, for the purposes of these guidelines, the following definitions apply:

[3] OJ L 119, 4.5.2016, ELI: http://data.europa.eu/eli/reg/2016/679/oj

[4] OJ L 257, 28.8.2014, ELI: http://data.europa.eu/eli/dir/2014/92/oj

[5] OJ L 150, 9.6.2023, ELI: http://data.europa.eu/eli/reg/2023/1113/oj

a) Event-driven review: means a review and, where relevant, an update of customer information and risk profiles that occurs when a trigger event or condition takes place as stipulated in Article 26(3) points (a), (b) and (c) of AMLR.
b) Triggering events: means an event or condition as stipulated in Article 26(3) points (a), (b) and (c) of AMLR or any other risk relevant event or condition.
c) Periodic review: means predefined periods that prompt customer information and, where relevant, risk profiles updates, depending on the risk level of the customer as stipulated in Article 26(2) of AMLR.
d) Pre-transaction/activity monitoring: assessing and, where relevant, investigating transactions and activities before execution, to determine whether the transaction/activity should proceed, be delayed or be escalated. Pre‑transaction/activity monitoring is preventive in nature and aims to identify ML/TF risks prior to execution.
e) Real-time monitoring: analysing transactions at the point of execution to enable immediate detection of unusual or suspicious activity and therefore act before or shortly after the transaction is completed.
f) Post-transaction/activity monitoring: assessing and, where relevant, investigating transactions and activities after they have been carried out, to identify unusual or suspicious activity based on patterns, behaviour and evolving risk indicators.

2 DRAFT GUIDELINES

2.1 GENERAL GUIDELINES

KEY PRINCIPLES

1. Obliged entities with business relationships should conduct ongoing monitoring including regular risk-based reviews and updates to the customer information as needed to ensure it remains accurate and consistent with their knowledge of the customer. Obliged entities should also monitor customer transactions and activities performed throughout the course of the business relationship to ensure they align with their knowledge of the customer and to identify any unusual or suspicious behaviour that requires further assessment.

2. Article 26(2) of AMLR sets the maximum periods of time for updating customer information for both higher-risk customers and all the other customers. However, obliged entities should decide whether more frequent updates are needed based on the customer's risk profile. If a review is carried out earlier than scheduled, this can reset the timeline for the next required update.

3. When conducting a periodic review or event-driven review in accordance with Article 26(2) and (3) of AMLR, obliged entities should assess which elements of the customer information, including the customer risk classification, require updating. In doing so, they should take into account the customer's risk profile and the information already available to them, including how up to date that information is. Where the customer's risk has increased, obliged entities should obtain any additional information necessary to apply appropriate risk-mitigating measures, including enhanced measures where the risk is higher.

4. Ongoing monitoring should not be limited to transaction monitoring but should also capture relevant activities, behaviours and events throughout the business relationship.

5. Obliged entities should ensure that their monitoring framework is effective, adaptable to changes in the customer's risk profile, and aligned with the risks identified in the business-wide risk assessment, including emerging risks related to products, services, customers, geographic exposure and distribution channels.

6. Obliged entities should ensure that the outputs of their monitoring framework are assessed and used to inform internal processes, including, where appropriate, the update of customer due diligence information and the customer's risk classification.

7. Obliged entities should ensure that staff involved in ongoing monitoring and in monitoring of transactions or activities are properly trained. Staff should have the necessary knowledge, skills and professional judgement to operate the monitoring framework effectively, understand and interpret its outputs, raise questions or challenge results where appropriate, and comply with AML/CFT requirements. Staff should be able to identify unusual or suspicious behaviour, and recognise, assess, report, and escalate to a more detailed level of review any changes in customer information that may affect customer due diligence. Staff members who interact directly with customers or oversee products and services should receive targeted training so they can quickly identify and communicate such changes through established escalation channels. Given their access to sensitive personal data, the training should also cover the handling of personal data.

8. Obliged entities should ensure that the governance of their ongoing monitoring framework, including the related decision-making processes, is documented in their internal policies, procedures and controls, in a manner that supports traceability, accountability and effective supervision. This should include documenting any limitations arising from the nature of their business, the mitigating measures applied to address those limitations, and the resulting monitoring outcomes. They should be able to understand what was assessed, what decisions are taken and the rationale behind. The form, level of detail and means of documentation should be proportionate to the ML/TF risk being mitigated and the nature, risks and complexity of their business, as well as the size of the obliged entity.

PROPORTIONALITY

9. Obliged entities should ensure that their ongoing monitoring framework is designed and implemented in a manner commensurate to the nature, risks and complexity of their business, as well as the size of the obliged entity. In applying the principle of proportionality, obliged entities should take into account their specific circumstances, including the overall ML/TF risk profile, the nature, complexity and scale of activities and operations, and the business model, with size being one of several relevant factors.

10. Proportionality should apply to the calibration and intensity of the monitoring measures applied, allowing obliged entities flexibility to determine the appropriate use of tools, methods and processes to achieve effective outcomes. It should also apply to the amount and type of personal data collected and processed for monitoring purposes, in line with the Regulation (EU) 2016/679 (GDPR) principles of necessity and data minimisation.

11. Where the obliged entity is a natural person or a legal person whose activities are performed by a single natural person only, that person should be responsible for complying with the requirements in these guidelines.

GUIDELINE 1: KEEPING CUSTOMER DOCUMENTS, DATA OR INFORMATION UP TO DATE

2.2 UPDATE OF CUSTOMER DOCUMENTS, DATA OR INFORMATION AND ONGOING MONITORING

12. Depending on the nature of the documents, data or information to be updated, and on the level and type of risk that needs to be mitigated, obliged entities should apply risk-sensitive measures in line with the RTS adopted pursuant to Article 28(1) of AMLR to assess the reliability and independence of the information source. Customer information should be updated by using:
    a) Reliable and independent sources of information which may include official registers or databases of government and competent authorities
    b) Information collected through reliable and reputable commercial organisations such as vendors and data service providers, and information from reliable and independent open sources;
    c) Information or confirmation provided directly by the customer, either in writing or through digital means, provided that this information is of sufficient quality to enable them to assess the authenticity and accuracy of the information;
    d) Information provided by other obliged entities;
    e) A combination of the sources above.

13. Obliged entities should take necessary steps to ensure that personal data obtained from public and commercial sources is accurate and up to date, and that only the information necessary to fulfil their ongoing monitoring obligations is collected and processed.

14. With regards to paragraph 12, point c, where a customer provides a written statement with new information or confirms previously collected information, documents, or data, obliged entities should, depending on the level and nature of the risk, consider whether the reliability of that statement needs to be verified using independent and reliable sources. In cases where a person representing the customer provides the confirmation on behalf of the customer, obliged entities should assess if they have the necessary knowledge and power of representation to confirm or provide such information.

15. In case of detection of unusual or suspicious transactions and activities, obliged entities should take the necessary action in accordance with Article 69 of AMLR.

RE-COLLECTION OF EXPIRED IDENTITY DOCUMENTS, PASSPORTS OR EQUIVALENT

16. During the process to update customer information to comply with Article 26 (2) of AMLR or during an event trigger review according to Article 26 (3) of AMLR, obliged entities should assess whether expired identity documents, passports or equivalent should be updated, including for natural persons or beneficial owners in respect of a legal entity. Where obliged entities conclude that an expired identity document, passport or equivalent should be re-collected or where a new or additional beneficial owner/s of a legal entity or a new person purporting to act on behalf of the customer that needs to be identified and verified, different methods of verification can be used such as electronic identification means as per Article 22(6), point (b) and for beneficial owners Article 22(7) of AMLR.

17. To assess whether or not to update an expired identity document, passport or equivalent, obliged entities should consider, amongst other elements, the following:
    a) The relevant risk associated with the customer and the business relationship that would call for an update of an expired identity document, passport or equivalent;
    b) The risk associated with the issuing country;
    c) The length of time that the identity document, passport or equivalent is expired;
    d) Whether it has all the necessary up-to-date security features since older identification documents might pose a heightened security risk of fraud and might be easier to counterfeit;
    e) Whether a newly issued document would provide updated or additional information relevant to verifying the updated customer's identity or customer's risk assessment; and
    f) Whether there are doubts as to continued accuracy of the customer's identification details, including doubts arising regarding the authenticity or adequacy of previously obtained identification data, or where such doubts may give rise to suspicions of ML/TF.

18. When the obliged entity deems it necessary to update an expired document, passport or equivalent, it should determine based on the level of risk whether the expired document:
    a) needs to be updated without delay; or
    b) the update takes place during the next scheduled customer information review or at the next occasion on which the customer interacts with the obliged entity, such as when requesting a new service or product.

2.3 PERIODIC CUSTOMER INFORMATION REVIEWS

19. Periodic reviews must always be conducted in accordance with Article 26(2) of AMLR. However, the depth and intensity of such reviews should follow a risk-based approach, whereby the obliged entity assesses, based on the customer's risk profile, which information, data, or documents require updating.

20. One of the considerations in adjusting the depth and intensity of a periodic review is when a business relationship exists but no new activity has occurred since the last customer information update, and no new services or products have been offered to the customer. Where, in a business relationship, the same activity continues without any change, obliged entities may adjust the depth and intensity of periodic reviews, for low-risk customers. For example, such review could mean checking business registries and other reliable and independent sources, conduct PEP and adverse media screening, and review internally whether anything has changed in the nature or purpose of the business relationship. Obliged entities should consider, amongst others, the following non exhaustive list of factors when deciding whether and how to adjust the depth and intensity of a periodic review:
    a) The customer's risk level
    b) Whether new activity or transaction has occurred or new services / products have been offered to the customer.
    c) The type and risk level of products or services provided to the customer and whether, despite the absence of new activity, the risk profile does not justify reducing the depth and intensity of monitoring.
    d) Whether a trigger event has occurred; where this is the case, a customer information review should be initiated without delay.
    e) Whether a new activity or transaction is initiated by the customer or by third parties; in such cases, a review should be carried out without delay.

21. When determining which documents, data, or information need to be updated as part of a periodic review, obliged entities should assess the information collected at customer onboarding and during the most recent customer review. Obliged entities should determine the appropriate scope of updates, taking into account the customer's overall risk profile. The list below sets out a non-exhaustive range of key customer information that needs to be assessed for the purpose of an update:
    a) The identification information on the customer, including the natural person or the beneficial owner in case of a legal entity;
    b) Beneficial ownership information, the legal status and valid statutory representation of legal entities;

c) An up-to-date understanding of the purpose and intended nature of the business relationship including, where applicable, a clear understanding of the source of funds; and
d) Whether the customer, beneficial owner of the customer and, where relevant, the person on whose behalf or for the benefit of whom a transaction or activity is being carried out has become a politically exposed person, a family member or person known to be a close associate.

22. Obliged entities may use the transaction or activity history to determine whether the source of funds remains consistent with the customer's expected profile, especially in situations where the funds continue to originate from the same sources.

23. In situations where the information on source of funds needs to be updated and customer due diligence information held by the obliged entity does not sufficiently explain the customer's source of funds, obliged entities should obtain additional information in accordance with the RTS adopted pursuant to Article 28(1) of AMLR.

2.4 EVENT-DRIVEN REVIEWS

24. Obliged entities should have an effective and appropriate monitoring framework in place, including policies, procedures, processes and controls that define and detect trigger events. Such events may arise, amongst other factors, from changes in customer behaviour, from information obtained through monitoring or other controls, or from external information indicating a potential change in customer risk profile.

25. The monitoring framework should ensure that relevant changes related to the customer are detected, reviewed, and handled without undue delay, with actions prioritised based on risks. The type and level of sophistication of these processes and controls should be based on the obliged entities' business-wide risk assessment and should be proportionate to the nature, risks and complexity of their business, as well as the size of the obliged entity. Obliged entities should document in a clear and comprehensible way the processes and controls applied.

26. When a trigger event requires updates to customer information, obliged entities should update the customer information by collecting sufficient and relevant documents, data or information on the customer to assess and mitigate any changes in the ML/TF risk of the business relationship.

EVENTS AND CIRCUMSTANCES THAT MAY TRIGGER A CUSTOMER INFORMATION REVIEW

27. The following non-exhaustive list of events are provided as instances of what may trigger a review of customer information based on changes in the relevant circumstances of the customer or facts which pertain to the customer, pursuant to Article 26(3) AMLR. Obliged entities should update the customer information accordingly and, adopting a risk-based approach, assess whether any of the triggering events listed below constitute a relevant and material change to their customer's risk profile that would warrant a re-assessment and change of the customer's risk profile level. Such triggering events may include:
    a) Changes in identity, legal status or ownership: including updates to identity details, nationality or residency, changes in legal form, ownership structure, directors, authorised signatories or representatives.
    b) Behavioural, activity-based or transactional anomalies: unusual transaction patterns, inconsistent behaviour, frequent and unexplained changes of professional service providers, repeated or unusual changes in IP address or device location, where relevant, or any activity that deviates from the customer's profile or from the expected purpose and intended nature of the business relationship. Obliged entities should consider AMLA's guidelines pursuant to Article 69(5) AMLR on indicators of suspicious activity or behaviors.
    c) Risk-relevant information or adverse findings: new adverse media, new PEP status, legal proceedings related to potential ML/TF violations, regulatory notices, internal intelligence or warnings issued by competent authorities.
    d) Changes in financial situation, source of funds or wealth or business activity: significant variations in financial standing, financing structures, asset composition or control, new products or services used by the customer, or engagement with higher-risk jurisdictions or counterparties.

PROCESSES TO DETECT RELEVANT EVENTS OR CIRCUMSTANCES THAT MAY TRIGGER A CUSTOMER INFORMATION REVIEW

28. Having regard to the nature, risks and complexity of their business, as well as the size of the obliged entity and overall business-wide risk assessment, obliged entities should assess whether automated or semi-automated systems and processes, including the use of advanced analytical tools, are needed to capture relevant changes in the customer information. Where the nature of the business model is limited in scale, risk and complexity, manual or semi-automated processes and controls may be a proportionate option. The chosen systems and processes should be capable of identifying and escalating relevant ML/TF risks without undue delay and should be supported by appropriate documentation and controls.

29. To identify events or circumstances that trigger a review and, where relevant, an update to the existing customer information, obliged entities may refer to:

a) Risk indicators that have internally been developed, and escalation channels for relevant staff performing AML/CFT-related tasks to use and flag material changes they become aware of.
b) Alerts or outputs produced by the transaction and activity monitoring framework that indicate unusual or potentially suspicious customer behaviour or adverse media alerts.
c) Use of company registries and public databases to detect changes, such as changes in corporate ownership or status.
d) Use of information from external data sources such as FIU communication, regulatory updates, tax authority communications, or other governmental alerts.
e) Use of information through internal cross-functional collaboration such as, and where relevant, structured information sharing between front-office, risk, compliance, and AML teams to detect triggers.
f) Use of information shared among entities belonging to the same group.
g) Use of information obtained directly from the customer during the usual course of communication

2.5 Use of suspension or restriction measures where the obliged entity does not receive updated information from the customer

30. Pursuant to Articles 20, 21 and 26 of AMLR, where an obliged entity is unable to keep the relevant customer documents, data or information up to date, it shall refrain from carrying out transactions and shall terminate the business relationship. Where an obliged entity needs to obtain updated documents, data or information from the customer, or to seek customer confirmation, and no response is received, and this temporarily prevents compliance with Article 20(1), point (f), of the AMLR, the obliged entity may, before terminating the business relationship, temporarily suspend or restrict transactions, activities or services. Such measures should be applied only where they allow the ML/TF risks to be effectively managed. When assessing whether it is appropriate and possible to suspend or restrict transactions, activities or services, obliged entities should take into account the following factors:
    a) No trigger event within the meaning of Article 26(3) has occurred;
    b) Considering the risk level of the customer;
    c) The nature of the products or services provided to the customer, and whether the suspension or restriction of transactions, activities or services is sufficient to effectively mitigate the ML/TF risks of the business relationship, thereby justifying a longer interval between updates; and

d) The documents, data or information already available remain sufficient to manage the identified risks, taking into account the scope of the suspension or restriction applied.

31. Obliged entities should take into account that the absence of transactions or activities does not, in itself, eliminate ML/TF risks. Such risks may still arise, in particular where assets are held or safeguarded and changes occur in beneficial ownership or control.

32. Obliged entities should take all reasonable measures and make every effort to obtain and update such documents, data, or information as soon as possible. The suspension or restriction of transactions and activities should be understood as a temporary measure, to be applied only where an obliged entity has taken repeated and reasonable steps to request and obtain up-to-date customer documents, data or information, and only until the obliged entity obtains the necessary documents, data or information from the customer. Termination should follow where the obliged entity is ultimately unable to comply with its obligations.

33. The measures set out in this Section 2.5 should apply without prejudice to the requirements of Directive 2014/92/EU. When applying these measures, entities should also ensure compliance with Article 21(3) of the AMLR, which requires obliged entities to keep records of their efforts to fulfil their due diligence obligations, including any actions taken and decisions made that led to the termination of a business relationship.

GUIDELINE 2: TRANSACTION AND ACTIVITY MONITORING FRAMEWORK

2.6 GENERAL PRINCIPLES

34. Obliged entities should ensure that their monitoring framework, including transaction and activity monitoring processes and controls, is based on their business-wide risk assessment and:
    a) Leverages systems and processes required by other Union legislation, such as Regulation (EU) 2023/1113 or the proposal on payment services in the internal market (PSR), as well as other already existing systems intended to detect unusual customer behaviour.
    b) Relies on complete, accurate, and timely data, drawing on sources available internally, and, where relevant, reliable and independent sources, including group information exchanged pursuant to Article 16(3) of AMLR;
    c) Covers all products and services in order to enable a holistic understanding of the customer's behaviour and support the detection of unusual or suspicious transactions and activities.
    d) Is capable of identifying transactions and activities that materially deviate from expected behaviour and may be unusual or suspicious, requiring further assessment under Article 69(2) AMLR;
    e) Is capable of identifying patterns, behaviours or linkages that may indicate risks related to the non-implementation or evasion of targeted financial sanctions, insofar as such risks are identifiable through the ongoing monitoring framework, including through intermediaries, ownership or control structures, counterparties, assets or transaction patterns;
    f) Is designed to be effective, at the point of implementation, in addressing the risks identified in the obliged entity's business-wide risk assessment, and to remain effective and fit for purpose over time through ongoing testing and adaptation to emerging risks.

35. Obliged entities that structurally have limited or no access to transaction and activity data, or that do not process transactions should ensure their monitoring framework is adjusted accordingly. This should include applying proportionate and effective alternative measures that are aligned with the obliged entity's business-wide risk assessment to identify and mitigate ML/TF risks, while ensuring that the limitations described above do not result in gaps in their ability to identify, assess and mitigate those risks, including, where relevant:

a) A structured, risk-based assessment of the customer's behaviour, and relevant events throughout the business relationship;
b) Reviewing customer documentation, instructions, mandates, and assets involved, including, where relevant, source of funds information, as well as the counterparties involved, funding arrangements and client account controls;
c) Conducting event-driven reviews;
d) Carrying out monitoring at relevant stages of the business relationship;
e) Escalating unusual or inconsistent behaviour identified by staff, supported by appropriate documentation;
f) Where partial access to transaction information exists, ensuring that transaction and activity monitoring remains a central component of their monitoring framework.

36. In those specific circumstances described in paragraph 35, obliged entities should document these limitations and resulting constraints, including the reasons underlying those limitations. Such limitations should not, in themselves, be considered a deficiency, provided they are understood, documented and appropriately mitigated, and the monitoring framework remains capable of identifying and escalating relevant ML/TF risks.

37. Where obliged entities rely on agents, intermediaries, distribution networks, or other entities within the group, they remain responsible for the effectiveness and performance of their monitoring framework and for ensuring it remains commensurate with the risks to which the obliged entity is exposed. They should also be able to demonstrate an understanding of the rationale behind the monitoring activities carried out and how these activities effectively mitigate those risks. Activities carried out through such arrangements should be documented and traceable, including the identification of the entity performing relevant monitoring tasks. Obliged entities should take appropriate measures to prevent gaps, inconsistencies, or circumvention of monitoring obligations that could undermine the effectiveness of the monitoring framework and should ensure access to the data, information, and documents necessary to perform ongoing monitoring. Obliged entities should consider AMLA's guidelines adopted pursuant to Article 18(8) AMLR on outsourcing and Article 50 AMLR on reliance on other obliged entities.

38. Where a customer acts as an intermediary - whether as an obliged entity or as another entity processing transactions and activities on behalf of underlying customers - obliged entities should ensure that their monitoring framework takes into account the risks arising from that intermediary role. This includes considering the intermediary's business model, the characteristics of its client base, and the nature of the transaction or activity flows it processes.

39. Where obliged entities are exposed to more complex products, services or business models, including relationships with non-bank financial institutions, correspondent

banking, trade finance, or investment and wealth management activities, monitoring frameworks should take into account the specific ML/TF risks associated with these activities. In such cases, monitoring should not focus solely on individual transactions and activities, but may also involve the analysis of aggregated flows, activity patterns, documentary information or changes in the form or structure of value, as appropriate.

40. Obliged entities should design and maintain their monitoring framework to ensure that high-risk business relationships and transactions receive a level of monitoring commensurate with their risk and are subject to enhanced scrutiny. In applying enhanced scrutiny, obliged entities should ensure that increased monitoring intensity is targeted to areas of material risk and does not result in a disproportionate allocation of resources to lower-risk activities.

41. Enhanced scrutiny should be tailored to the customer's risk profile and to the risks identified in the business-wide risk assessment. This may include applying, where appropriate:
    a) more targeted or intensified monitoring parameters, scenarios, risk indicators or analytical approaches;
    b) more frequent or in-depth reviews, including reviews covering an extended look-back period where this is relevant to assess patterns, links or cumulative risk indicators;
    c) specific controls adapted to the customer's activity and risk profile.

2.7 MONITORING FRAMEWORK USING MANUAL, AUTOMATED, OR SEMI-AUTOMATED PROCESSES AND CONTROLS

42. Obliged entities should determine whether their monitoring framework uses manual, automated or semi-automated processes and controls, taking into account their size, nature of business, transactions and activities volumes and frequency as well as complexity and overall ML/TF risk exposure. The design and intensity of the monitoring framework should be risk-based and mitigate the risks identified in the business-wide risk assessment. Obliged entities should document the rationale for the chosen monitoring framework, its design, and, where needed, the adjustments and be able to demonstrate its functionality, rationale and effectiveness to the competent authorities upon request.

43. Obliged entities should ensure that their monitoring framework is capable of identifying and assessing, without undue delay new ML/TF methods, trends and typologies including those related to the non-implementation or evasion of targeted financial sanctions, identified by, amongst others, supervisory authorities, FIUs and other reliable public sources, as well as relevant risk indicators and red flags. They should assess and

document whether there is a need to amend or supplement their monitoring framework. Obliged entities should revisit earlier decisions regarding their framework where needed, including as part of the review of their business-wide risk assessment and in response to internal cases, supervisory feedback or other credible external information and insights. They should be able to demonstrate to competent authorities the steps taken, the rationale for their decisions and the timing of their actions.

44. Obliged entities should ensure that their monitoring framework is capable of detecting ML/TF risks that only emerge when transactions and activities are considered together over time, rather than in isolation. This includes, but is not limited to:
    a) Identifying linked, repeated or aggregated behaviour across and within accounts, customers, devices, wallets or other identifiers;
    b) Analysing risk-relevant behavioural patterns based on an assessment of customer's behaviour, relationships, and transaction patterns over time;
    c) Recognising network relationships or behavioural patterns that may indicate attempts to conceal ownership, control or the economic purpose of an activity;
    d) Recognising situations where individual transactions and activities may appear low-risk on their own but form concerning patterns or behaviours over time, including cases where value is accumulated, split, or transferred across multiple transactions and activities.

45. Obliged entities should ensure that their monitoring framework operates in a controlled and sufficiently transparent manner, underpinned by clear governance arrangements and proportionate documentation, including dedicated policies and procedures, and, where applicable, defined escalation arrangements. This should enable monitoring outcomes to be assessed, escalated and acted upon in a consistent and timely manner. Obliged entities should be able to explain, on request, material changes in monitoring behaviour or outcomes, including those resulting from updates to rules, thresholds, models or analytical methods. They should also ensure periodic internal and/or external reviews to maintain the effectiveness of the framework.

MANUAL PROCESSES AND CONTROLS

46. Obliged entities should ensure effective monitoring systems, taking into account the nature of the business, including its risks and complexity, and the size of the obliged entity. On the basis of their business-wide risk assessment, they should assess whether manual processes and controls are sufficient to achieve effective monitoring outcomes or whether their monitoring framework should, as a general rule, be supported by automated or semi-automated systems and processes where justified.

47. Obliged entities that structurally have limited or no access to transaction and activity data, do not process transactions due to the nature of their business model, or whose

transaction volumes, speed, scale and complexity do not justify the use of automated or semi-automated monitoring systems and processes may rely on manual monitoring processes and controls. These systems and processes should be commensurate with the obliged entity's risks, and may include periodic and event-driven reviews, documentation-based checks, and, where relevant pre-transaction checks. Such measures should be proportionate to the nature, risks and complexity of their business, as well as the size of the obliged entity and be capable of detecting unusual or suspicious transactions and activities.

AUTOMATED OR SEMI-AUTOMATED MONITORING SYSTEMS AND PROCESSES

48. Obliged entities that use automated or semi-automated monitoring processes and controls should ensure that their rules, scenarios, thresholds and, where relevant, models or behavioural baselines are clearly defined and capable of detecting the relevant ML/FT risks, taking into account relevant typologies and the general principles in paragraph 34 of these Guidelines.

49. Obliged entities should maintain, and where needed, calibrate their monitoring framework to ensure it remains effective and produces valid and meaningful output. When designing and adjusting their monitoring framework, obliged entities should consider the potential impact of their choices on both detection capability and the risk of undetected activity. Obliged entities should document, test and record any updates to their detection logic, underlying configuration and, where relevant, models or behavioural baselines, and ensure that these updates are communicated to the relevant staff directly involved in the design, operation or assessment of the monitoring framework.

50. Where obliged entities rely on pre-configured or externally developed monitoring tools, they need to ensure they understand the appropriate use of such tools. They should also review and assess the suitability of the default settings considering the nature, risks and complexity of their business, as well as the size of the obliged entity and calibrate these settings. Default settings should not be used without a documented assessment of their appropriateness.

2.8 LINK BETWEEN CUSTOMER DUE DILIGENCE AND THE ONGOING MONITORING FRAMEWORK

51. Obliged entities should ensure that their customer due diligence processes including, sanctions screening processes, and their monitoring framework operate in an integrated and coordinated manner and are supported by adequate data and information quality.

This includes ensuring that the relevant documents, data or information are complete, accurate and up to date in accordance with the requirements set out in guideline 1.

52. Obliged entities should ensure that relevant outputs from their monitoring framework are assessed and used to inform internal processes and, where appropriate, update the customer due diligence information and risk classification. Where monitoring outputs indicate increased risk, obliged entities should apply appropriate risk-mitigating measures, which may include enhanced due diligence. Where such outputs indicate emerging or evolving ML/TF risks, obliged entities should consider, where appropriate, whether these have implications for their business-wide risk assessment. Obliged entities should document the analysis performed and the rationale for decisions taken.

53. Obliged entities should use customer profiles for their monitoring framework and ensure these profiles are based on verified customer due diligence information held by them. This should include the customer's purpose and intended nature of the business relationship and, where relevant, the expected transactions and envisaged activities, and the resulting expected behavioural profile of the customer. Where the obliged entity has structurally limited or no access to transaction and activity data, the customer profile should instead draw on other risk-relevant information, such as those arising from the business relationship. Monitoring should be calibrated to this baseline so that deviations from the customer's known or expected transaction, activity, behaviour or risk profile can be identified in a reliable manner and without undue delay.

54. Where appropriate, considering the customer's risk profile and the nature, risks and complexity of their business, as well as the size of the obliged entity, obliged entities may decide to make use of reference or peer groups with an aggregated expected transaction or activity profile. Obliged entities using such groups, should ensure that transactions and activities that deviate from the group pattern are assessed in the context of the individual customer's profile and not only at the level of the customer's account. The absence of a deviation at peer-group level should not, on its own, be used to dismiss risk indicators identified at individual customer level.

55. Obliged entities using reference or peer groups should ensure it supports, and not replace, their understanding of the individual customer and the purpose of the business relationship. These groups should not be relied upon where customer behaviour is inherently heterogeneous.

56. Obliged entities should have mechanisms in place to ensure that customer or customer-group profiles, including expected transaction and activity profiles and the composition of any reference or peer groups, are kept up to date. This should include reviewing, and where necessary, updating these profiles where monitoring outputs or

other information indicate a material change in risk, behaviour or use of the service, regardless of whether a periodic customer review is due.

57. Where obliged entities identify deviations or inconsistencies, they should reassess the customer's information and risk profile and determine, based on the analysis performed, whether a suspicious activity report should be submitted in accordance with Article 69 AMLR.

2.9 IMPLEMENTATION OF THE MONITORING FRAMEWORK

58. Obliged entities should, as a general rule, ensure that ongoing monitoring is performed on a continuous basis throughout the business relationship.

59. Where continuous monitoring cannot be applied due to the nature of the business model or objective legal or technical constraints beyond the control of the obliged entity, obliged entities may perform monitoring at defined stages in the lifecycle of the business relationship, where ML/TF risks may arise or materially change. In such cases, obliged entities should:
    a) justify the use of this approach;
    b) document the limitations and the mitigating measures applied;
    c) demonstrate that the chosen approach ensures an effective level of risk identification and mitigation, commensurate with the limitations identified.

PRE-TRANSACTION AND PRE-ACTIVITY MONITORING

60. Pre-transaction and pre-activity monitoring enable obliged entities to assess and, where necessary, investigate transactions and activities before they are carried out or completed, in order to identify any unusual or suspicious transactions and activities.

61. Where obliged entities, taking into account their role, business model and access to relevant information, have the ability to assess or intervene prior to a transaction or activity being carried out or completed, they should apply pre-transaction and pre-activity monitoring to detect unusual or suspicious transactions and activities.

62. Where, within their role, business model and access to relevant information, obliged entities have the ability to assess or intervene at the point of execution, immediately before a transaction or activity is carried out or completed, they should, where relevant, ensure that real-time monitoring forms part of pre-transaction and pre-activity monitoring to detect unusual or suspicious transactions and activities prior to execution.

63. Obliged entities should ensure that appropriate measures are taken without undue delay, including the ability, within their role, business model and access to relevant information, to intervene by preventing, delaying or further assessing transactions and activities presenting heightened ML/TF risk

64. Where obliged entities do not directly execute or control transactions, pre-transaction and pre-activity monitoring should be designed to include controls applied prior to the provision of a service or product or the carrying out of an activity, such as the review of mandates, instructions, contractual arrangements or assets involved.

65. Where this is not possible, in particular in sectors where business relationships are not continuous or where obliged entities do not control or execute transactions, pre-transaction and pre-activity monitoring may be limited in scope. In such cases, where obliged entities are not, within their role, business model and access to relevant information, able to assess or intervene prior to a transaction or activity being carried out or completed, such monitoring may be limited to the application of customer due diligence measures and the assessment of relevant information prior to entering into a transaction or providing a service.

66. Where, due to the nature of the business model or objective legal or technical constraints beyond the obliged entity's control, effective pre-transaction, pre-activity or real-time monitoring cannot be applied in line with the principles set out above, obliged entities should ensure that such limitations do not create gaps in their ability to identify, assess and escalate ML/TF risks. Such limitations should not arise from, or be reinforced by, the design of products, services or business practices, which should support the effective application of monitoring measures and should not unduly restrict it. Legal or technical constraints should not be used to justify the absence of pre-transaction or pre-activity monitoring where the obliged entity is in a position to assess or intervene prior to a transaction or activity being carried out or completed.

67. Obliged entities should define their monitoring approach and should not treat different monitoring approaches as interchangeable. They should document the basis for their approach, including any limitations and the mitigating measures applied. They should demonstrate that the chosen approach ensures an effective level of ML/TF risk identification and mitigation, commensurate with those limitations and mitigating measures.

POST-TRANSACTION AND POST-ACTIVITY MONITORING

68. Post-transaction and post-activity monitoring enable obliged entities to assess and, where relevant, investigate transactions and activities after they have been carried out, in order to identify any unusual or suspicious transactions and activities.

69. Where obliged entities have the ability, within their role, business model and access to relevant information, to assess transactions and activities after they have been carried out, they should apply post-transaction and post-activity monitoring to detect unusual or suspicious transactions and activities.

70. Where obliged entities have the ability, within their role, business model and access to relevant information, to analyse transactions and activities after they have been carried out, including, where relevant, on an aggregated or behavioural basis, they should ensure that such analysis also forms part of post-transaction and post-activity monitoring to identify unusual patterns, linkages or cumulative risk indicators.

71. Obliged entities should ensure that appropriate measures are taken without undue delay, including the identification and escalation of unusual or suspicious transactions and activities, including patterns, linkages or cumulative risk indicators identified through monitoring, for further assessment and, where necessary, escalation.

72. Where, due to the nature of the service or objective technical or legal constraints beyond the control of the obliged entity, relevant transaction data becomes available only after they have been carried out, obliged entities should ensure that appropriate post-transaction monitoring measures are applied without undue delay, taking into account the nature, timing and completeness of the information available.

73. Where, due to the nature of the service or objective technical or legal constraints beyond the control of the obliged entity, post-transaction and post-activity monitoring may be limited in scope or duration, obliged entities should ensure that such limitations do not create gaps in their ability to identify, analyse and escalate ML/TF risks. Such limitations should not arise from, or be reinforced by, the design of products, services or business practices, which should support the effective application of monitoring measures and should not unduly restrict it. Legal or technical constraints should not be used to justify the absence or limitation of post-transaction or post-activity monitoring where the obliged entity is able to identify and analyse transactions and activities after their execution.

74. Where a business relationship is determined to be established after a series of occasional transactions that have been carried out, pursuant to Article 19 of AMLR and in line with

the RTS adopted pursuant to Article 19(9) of AMLR, obliged entities should assess these transactions to identify any unusual or suspicious transactions and activities requiring further action.

HANDLING OF MONITORING OUTPUTS

75. Obliged entities should ensure that monitoring outputs, whether generated through automated systems or arising from manual processes within the monitoring framework, are assessed without undue delay, prioritised based on risk, and escalated, where further analysis is required, to staff with appropriate knowledge of the customer and expertise. Obliged entities should be able to explain, on request, how monitoring outputs were assessed, escalated and acted upon, including the documented rationale for decisions taken.

76. Obliged entities should define and maintain appropriate internal arrangements to ensure that monitoring outputs are assessed and resolved without undue delay, including mechanisms to identify, monitor and address any accumulation of pending monitoring outputs that may affect the effectiveness of the monitoring framework.

77. The assessment of monitoring outputs should be carried out in a manner that ensures objectivity and avoids conflicts of interest. Where tasks are distributed across different functions or lines of defence, obliged entities should clearly define, in their policies and procedures, roles and responsibilities and implement appropriate safeguards to ensure the independence and integrity of the assessment process.

78. Obliged entities that use automated mechanisms to close monitoring outputs should ensure that these mechanisms are only applied to cases which, following automated analysis, do not indicate suspicious or unusual transactions and activities or other material ML/TF risk indicators. Such mechanisms should not be applied where there are indicators of heightened risk, including in relation to higher-risk customers or situations requiring enhanced scrutiny.

79. Obliged entities should ensure that the underlying decision logic can be understood and documented. They should also ensure that the effectiveness of automated mechanisms is subject to effective human oversight, including periodic validation through sampling, the review of potential cases where suspicious transactions or activities were not identified, or other appropriate checks.

2.10 INTERNAL CONTROLS AND ONGOING REVIEW

80. The provisions in this section focus on ensuring the effectiveness of the monitoring framework and should be read in conjunction with, and without prejudice to, broader requirements on internal controls, policies and procedures.

81. Obliged entities should periodically review and test their monitoring framework to ensure that it remains effective and aligned with the risks identified in the business-wide risk assessment. Such review should support the ongoing improvement of the monitoring at a framework level, taking into account monitoring performance, the outcomes of escalations and suspicious activity reports, emerging ML/TF risks and other relevant feedback, including, where relevant, the performance and limitations of analytical tools used within the monitoring framework.

82. Obliged entities should also implement robust data quality controls, data validation processes, and regular data cleansing. Testing or validation of automated or semi-automated monitoring systems should, where appropriate, rely on synthetic or anonymised data, in particular for functional validation. Where the use of real personal data is necessary for such testing or validation to assess whether the monitoring framework operates effectively, including through the review of monitoring outputs or case samples, obliged entities should ensure that such use is limited to what is strictly necessary, in line with data minimisation principles, and subject to appropriate safeguards.

83. Obliged entities should define the outcomes of their monitoring framework and periodically reassess whether those outcomes remain appropriate in light of their business-wide risk assessment and, where relevant, publicly available national or Union-level priorities.

84. Obliged entities should consider, in assessing effectiveness, the extent to which their monitoring framework produces outcomes that are relevant, risk-based and capable of supporting the identification and reporting of ML/TF risks. Effectiveness should not be assessed solely by reference to alert, reporting volumes or to the breadth of typology coverage where this does not result in meaningful detection or escalation outcomes. Instead, where relevant, obliged entities should consider the timeliness of escalation, the appropriateness of outcomes, recurring deficiencies, and whether the framework remains capable of addressing the ML/TF risks.

85. Where obliged entities materially change their monitoring logic, analytical methods or monitoring approach, they should apply a documented transition and validation framework to assess whether the revised approach remains effective and consistent with

the defined effective outcomes and their business risk assessment. Validation should include testing that goes beyond comparison with legacy outputs. Comparative analysis with prior approaches may be used where it provides meaningful insight into potential gaps or ML/TF risks.

86. Obliged entities should ensure that the responsibility for overseeing the effectiveness of the monitoring framework is clearly assigned and that identified deficiencies are addressed without undue delay. Governance arrangements, including policies and procedures, should enable relevant staff to effectively understand and challenge monitoring tools and their outputs.

2.11 USE OF TECHNOLOGY

87. Obliged entities should assess whether the use of automated or advanced analytical tools, including algorithms, machine learning, artificial intelligence and other innovative technologies, would enhance the effective identification and escalation of ML/TF risks within their monitoring framework. This assessment should take into account whether manual processes are sufficient to achieve effective monitoring outcomes, having regard to the obliged entity's risk exposure, complexity, size and operational scale, including the volume and speed of activity. The deployment of such tools should not, in itself, be considered an indicator of effectiveness. Effectiveness should instead be assessed by reference to whether the tools enable the obliged entity to detect and escalate relevant ML/TF risks without undue delay.

88. Obliged entities should ensure appropriate safeguards, proportionate to their size, nature, complexity and risk, and to the impact of the tool on monitoring outcomes or decisions. They should ensure that the outputs of such tools can be reviewed and, where necessary, challenged, and that responsibility for monitoring decisions remains clearly assigned.

89. The level of safeguards applied, including oversight, challenge and explainability, should be commensurate with the role of the tool within the monitoring framework and the associated ML/TF risk. In applying these safeguards, obliged entities should take into account model risk, including risks arising from inaccuracies, biases, lack of robustness or limited transparency of analytical tools that may affect monitoring outcomes. They should also consider the risk of delaying or limiting improvements in detection capabilities and avoid introducing unnecessary constraints that do not materially enhance those outcomes.

90. Obliged entities should be able to demonstrate and explain, upon request, the role, functioning and outputs of such tools to competent authorities in a manner that enables

effective understanding, assessment and challenge of those outputs, without requiring full technical interpretability of the underlying model.

91. Where obliged entities rely on third-party providers, they should ensure that sufficient information is available to meet the requirements set out above. Where this is not the case, obliged entities should not rely on such tools for monitoring functions that materially influence monitoring outcomes or decisions.

92. Obliged entities should ensure that data used within their monitoring framework is of sufficient quality and integrity to support the effective identification and escalation of ML/TF risks. They should understand and, where relevant, document material limitations in the data or its use that may affect monitoring outcomes, including how data is attributed to customers, counterparties, assets or activities.

93. Where deficiencies in data quality, accuracy, attribution or completeness may materially affect monitoring outcomes, obliged entities should document the deficiencies identified, the basis for their assessment and the mitigating measures applied.

94. Outputs generated by analytical tools, including artificial intelligence, should support monitoring decisions and should be subject to appropriate governance, oversight, challenge and control, in a manner that avoids discriminatory outcomes, in line with the relevant legislation.

95. Obliged entities should ensure, in a manner commensurate with the role of the tool within the monitoring framework and the associated ML/TF risk, that such tools maintain the expected performance over time, including through appropriate monitoring and, where relevant, the identification of material performance degradation or drift. Obliged entities remain responsible for monitoring decisions and should ensure that these can be reviewed and, where necessary, adjusted, including, where appropriate, through effective human oversight.

5. Accompanying documents

5.1 Impact assessment with cost-benefit analysis

Introduction

As per Article 54(2) of Regulation (EU) 2024/1620 (AMLAR), AMLA may issue guidelines and shall, where appropriate, conduct open public consultations and analyse the related potential costs and benefits arising from such guidelines.

This analysis presents the Impact assessment with cost-benefit analysis (IA/CBA) of the main policy options included in the Consultation Paper (CP) on the guidelines under Article 26(5) of AMLR (guidelines).

This IA/CBA is qualitative in nature and the policy choices have been taken in accordance with qualitative considerations, taking into account the experience and professional judgment of competent authorities from the financial and the non-financial sectors, the European Commission, and AMLA. Moreover, quantitative figures in relation to this mandate are currently unavailable and performing a targeted collection would impose a disproportionate burden on obliged entities. Where quantitative evidence is lacking, the analysis is supported by structured qualitative reasoning and professional judgement informed by supervisory experience and wider stakeholders' input.

A. Problem identification

The obligation to conduct ongoing monitoring of business relationships, including scrutiny of transactions undertaken throughout the course of such relationship has formed part of the Union's AML framework since the adoption of the third AML Directive (Directive (EU) 2005/60/EC). Directive (EU) 2005/60/EC established that customer due diligence (CDD) obligations do not end with onboarding but rather continue throughout the lifecycle of the business relationship, reflecting the fact that customers' circumstances, activities, and transactional patterns may evolve over time. However, the previous AML framework relied heavily on national implementation by Member States, which resulted in divergent practices with regard to the frequency and scope of updates of the relevant customer's documents, data and information. These divergencies created opportunities for regulatory arbitrage as criminals could exploit jurisdictions with less stringent approach.

AMLR addresses these shortcomings by introducing directly applicable, more granular rules, including a maximum five-year interval for updating relevant customer documents, data, and information. This harmonisation ensures consistent application across the internal market. The Regulation further emphasises that obliged entities must maintain a comprehensive and up-to-

date understanding of each customer's risk profile and shall review customer information regularly in line with the risk-based approach. Such reviews are required not only on a periodic basis but also when triggered by material change in the relevant customer's circumstances, whether related to their risk profile or their identification details.

AMLR also broadens the range of obliged entities, bringing additional sectors within the scope of customer due diligence and ongoing monitoring requirements. Newly covered entities include crowdfunding service providers and crowdfunding intermediaries, investment migration operators, football clubs and agents, credit intermediaries for mortgage and consumer credit, non-financial mixed-activity holding companies, certain crypto-asset service providers, and traders in high-value goods, some of which were previously subject to AML obligations only in limited circumstances.

By expanding the list of obliged entities, the Regulation aims to address emerging ML/TF risks across both the financial and non-financial sectors and to ensure that all vulnerable areas of the internal market are adequately protected. However, complying with AML/CFT requirements to conduct ongoing monitoring of business relationships may prove challenging for obliged entities with limited or no prior experience in applying such rules, particularly where their business models differ substantially from those of traditional financial institutions.

To date, additional guidance on ongoing monitoring for the financial sector has been provided in the EBA Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849 (EBA/GL/2021/02)[6]. By contrast, guidance at the EU level for the non-financial sector has been limited to date. It is therefore important to provide further clarification to support also obliged entities in the non-financial sector in applying a consistent, effective, and risk-based approach to ongoing monitoring of business relationships.

The monitoring of the transactions and activities carried out in the context of such relationships constitutes an integral component of the requirement to conduct ongoing monitoring. As stated in Article 26 of AMLR, obliged entities must ensure that transactions carried out during the business relationship are consistent with their knowledge of the customer, the customer's business activities and risk profile, and where necessary the origin and destination of funds. The monitoring framework must therefore be designed to detect transactions and activities that may give rise to suspicions of ML or TF. This is particularly important in the non-financial sector, where business models often differ substantially in nature, size and complexity from those of the financial sector.

[6] EBA/GL/2021/02, as amended.

B. Policy objectives

The draft Guidelines aim to ensure that obliged entities in the financial and non-financial sector adopt a consistent approach to ongoing monitoring of a business relationship and on the monitoring of the transactions and activities carried out in the context of such relationship. These draft Guidelines provide further information and assist in effectively implementing these obligations in a uniform and consistent manner across the Union, while promoting a risk-based approach and the efficient use of resources.

Leveraging technology is a key recommendation for improving the efficiency and effectiveness of transaction and activity monitoring, especially when dealing with higher volumes of transactions. At the same time, the draft Guidelines recognise that not all obliged entities, particularly those with limited or smaller scale operations, will have a business model that justifies the deployment of automated monitoring solutions. In such cases, the Guidelines provide direction on how to establish appropriate systems and controls using manual or simpler tools, aligned with the risk-based approach and proportionality principle.

The Guidelines therefore set out horizontal core principles for all obliged entities, ensuring that requirements remain broad enough to be widely applicable while still supporting effective and efficient implementation of their ongoing monitoring obligations.

By doing so, they enhance legal certainty for obliged entities and strengthen the overall effectiveness and efficiency of supervisory oversight. Clear, common guidance also facilitates smoother cooperation among supervisors, increases transparency, and reduces regulatory burdens arising from divergent national expectations.

C. Baseline scenario

Under the baseline scenario, obliged entities would conduct ongoing monitoring of business relationships, including transactions undertaken by the customer solely in accordance with Article 26 of AMLR, without further guidance on how to ensure compliance in practice. The absence of more detailed direction may result in divergent interpretations, particularly within certain non-financial sectors that were not previously considered as obliged entities under the former framework. Many of these sectors are now required to apply CDD measures for the first time and may not yet have benefited from guidance issued by competent authorities before.

Such variation in approaches and interpretations risks undermining the consistent application of ongoing monitoring requirements and may create opportunities for regulatory arbitrage. This could disproportionately affect obliged entities operating across multiple jurisdictions, as well as enable criminals to exploit countries that adopt more permissive interpretations.

To address these risks, Article 26(5) of AMLR mandates that AMLA issues guidelines on the ongoing monitoring of business relationships and on the monitoring of the transactions carried out in the context of such relationships. In developing these guidelines, AMLA has given due consideration to the principle of proportionality and to the diverse range of stakeholders concerned.

D. Options considered, cost-benefit analysis, and preferred option

Section D presents the main policy options discussed and the decisions taken by AMLA during the development of the draft Guidelines. It begins by outlining the overarching principles that guided the policy choices. It then presents the policy options considered for the main policy issues identified during the preparation of the draft Guidelines, followed by a qualitative assessment of the potential costs and benefits associated with each option. The section concludes by identifying the preferred option resulting from this analysis.

Overarching principles

The policy choices reflected in the draft Guidelines are guided by four overarching principles: risk-based approach, proportionality, horizontal applicability across financial and non-financial sectors, and technological neutrality. These principles respond directly to the problem identified in the baseline scenario, namely the risk of divergent national practices and uneven supervisory expectations in the absence of detailed guidance.

At the core of the draft Guidelines lies the **risk-based approach**, which underpins the EU AML/CFT framework. Ongoing monitoring, including the monitoring of transactions and activities, is designed to ensure that obliged entities maintain an accurate and up-to-date understanding of their customers and are capable of identifying material deviations that may indicate ML/TF risks, where relevant. AMLA therefore sought to promote effective and risk-based outcomes, rather than encouraging formalistic, purely procedural or "tick-the-box" compliance. The draft Guidelines focus on ensuring that monitoring frameworks are capable of detecting material risks without undue delay and are calibrated to the actual exposure of the obliged entity.

Closely linked to the risk-based approach is the **principle of proportionality**. AMLA aimed to ensure that the requirements set out in the draft Guidelines are appropriate and necessary to achieve their objectives and do not impose unnecessary or excessive compliance costs, particularly on obliged entities with lower risk exposure, smaller scale operations or less complex business models, including newly obliged entities with limited prior experience in AML/CFT compliance. This principle is reflected in the recognition that monitoring frameworks may be manual, automated or semi-automated, and that their design, calibration and intensity should be commensurate with the complexity of the obliged entity's activities. It is also reflected in the approach to periodic and event-driven reviews, including the updating of expired identification documents, which is framed in risk-based rather than automatic terms.

AMLA pursued a high degree of regulatory consistency and harmonisation across Member States and sectors by adopting a fully horizontal structure applicable to all obliged entities. This **horizontal applicability** avoids fragmentation across sectors and promotes consistent interpretation throughout the Union. The draft Guidelines therefore establish common minimum expectations and core elements for keeping customer information up to date and for designing and operating monitoring frameworks, thereby supporting supervisory convergence, ensuring neutral conditions of competition, and reducing the risk of divergent national or sectoral approaches that could give rise to regulatory arbitrage.

At the same time, the Guidelines are grounded in the principle of **technological neutrality**, ensuring flexibility and future-proofs the framework. Rather than mandating specific systems or methodologies, AMLA defines the minimum requirements and intended outcomes of ongoing monitoring, leaving obliged entities free to determine how best to achieve them. This approach acknowledges the diversity of business models and risk profiles across financial and non-financial sectors, including newly in-scope entities. Obliged entities may therefore design a monitoring framework suited to their operations, provided that it is well-justified, properly documented, and effective in managing ML and TF risks.

Against this background, three main policy issues were identified.

Policy Issue 1: Horizontal structure versus sector-specific Guidelines

A key policy issue concerned the overall structure of the draft Guidelines, namely whether AMLA should adopt a fully horizontal approach applicable to all obliged entities or combine horizontal provisions with dedicated sector-specific sections. This issue was closely linked to the broader objectives of ensuring harmonised implementation of article 26 of Regulation of AMLR, avoiding regulatory arbitrage, and accommodating the diversity of business models across financial and non-financial sectors.

In this context, AMLA considered the following options.

1. Adopting **fully horizontal structure** of draft Guidelines.
2. Adopting **horizontal parts with including dedicated sector- specific** guidelines.

Option A

Under Option A, the draft Guidelines would adopt a fully horizontal structure, setting out core principles and expectations applicable to all obliged entities, regardless of sector, while allowing for proportionate implementation depending on the nature, risks and complexity of their business, as well as the size of the obliged entity. This approach reflects the framework established in Article 26 of AMLR, which requires obliged entities to conduct ongoing monitoring of business relationships and transactions performed by customers, without distinguishing between sectors or establishing sector-specific requirements. The policy choice to structure the

draft Guidelines horizontally therefore mirrors the structure of the Regulation itself, ensuring that the core principles and expectations follow the uniform legal obligations laid down at Union level.

The principal benefit of this option is regulatory consistency. By articulating core expectations for keeping customer information up to date and for designing and operating monitoring frameworks, the draft Guidelines support supervisory convergence and reduce the risk of divergent national or sectoral interpretations. This directly addresses the problem identified in the baseline scenario, namely fragmentation and uneven supervisory expectations.

Option A also promotes inclusiveness and future-proofing. AMLR expanded the scope of obliged entities, including sectors that were previously subject to limited or no AML/CFT obligations. A horizontal framework ensures that all obliged entities, including newly in-scope sectors, are subject to the same core expectations while retaining flexibility to implement them proportionately. It avoids creating rigid sector-specific principles that may quickly become outdated as business models evolve or as new categories of obliged entities are brought within the scope. Furthermore, for obliged entities operating across multiple sectors or providing diversified services, a single horizontal framework reduces complexity and compliance costs by eliminating the need to navigate multiple sector-specific guidelines.

From a supervisory perspective, Option A facilitates more coherent oversight. Supervisory authorities can rely on a common set of principles and expectations when assessing compliance, which enhances comparability and contributes to neutral conditions of competition across the Union. It also limits the risk that sector-specific differences could unintentionally create different expectations or perceptions of unequal treatment.

The main cost associated with Option A is that sector-specific nuances are not addressed through tailored, prescriptive provisions. Certain sectors, particularly in the non-financial domain or those with non-continuous business relationships, may face interpretative challenges when applying horizontal principles to their specific operational contexts. This could require additional clarification through examples, supervisory dialogue or future guidance. However, these costs are mitigated by the risk-based and proportional nature of the Guidelines, which allow obliged entities to adapt implementation to their specific characteristics without being constrained by heterogeneity of sectors concerned.

Option B

Under Option B, AMLA would adopt a hybrid structure consisting of horizontal provisions complemented by dedicated sector-specific sections for selected categories of obliged entities, such as financial institutions, legal professionals, real estate agents or crypto-asset service providers. The benefit of this approach would be increased sectoral clarity and potentially easier implementation for specific industries. Tailored sections could address particular risk patterns, data availability constraints or transaction monitoring frameworks specific to certain industries,

potentially facilitating implementation and reducing initial uncertainty, especially for newly obliged entities.

However, Option B may entail certain structural implications. In particular, it could increase the risk of fragmentation within the regulatory framework, as differences in sector-specific drafting may give rise to varying interpretations and supervisory practices. Over time, this could complicate the objective of harmonisation under the AMLR and, in some cases, create uneven application across sectors or Member States.

Second, a sector-specific structure would be resource-intensive to develop, maintain and update. As new typologies emerge or as the scope of obliged entities or services evolves, AMLA would need to continuously amend multiple sections to ensure consistency. This could delay updates and create transitional inconsistencies. It would also increase complexity for cross-sectoral entities and supervisors overseeing diversified business models.

Third, introducing sector-specific sections for only some sectors could create perceptions of asymmetry or preferential treatment. Deciding which sectors merit dedicated guidelines and which do not would itself raise policy and governance challenges. Over time, the structure could become increasingly complex, reducing transparency and accessibility of the Guidelines.

Preferred option

On balance, AMLA concluded that Option A better achieves the objectives of harmonisation, proportionality and legal certainty while remaining sufficiently flexible to accommodate sectoral diversity. A fully horizontal structure establishes a clear and coherent baseline applicable to all obliged entities, supports supervisory convergence, and reduces long-term regulatory complexity.

It also promotes a proportionate implementation approach that reflects the nature, complexity, size, and overall risk profile of the obliged entity, while emphasising that obliged entities should first have a clear understanding of their business-wide risk assessment before establishing their ongoing monitoring framework. This may entail additional initial costs, especially, for smaller obliged entities to obtain a sufficiently comprehensive understanding of their business's related risks. However, such an assessment ultimately forms the necessary basis for complying with Article 26 of AMLR and applying the core principles of these draft Guidelines in a manner that appropriately addresses their specific risk profile, thereby preventing a purely formalistic or "tick-the-box" approach that could otherwise lead to disproportionate or unnecessary controls and policies.

While it requires some reliance on interpretation and proportional implementation, these features are consistent with the risk-based approach embedded in Article 26 of AMLR and are preferable to the structural fragmentation and maintenance burdens associated with a sector-specific model. For these reasons, Option A was selected as the preferred option.

Policy Issue 2: Prescriptive versus principle-based Guidelines

Closely linked to the structural decision was the question of how detailed the draft Guidelines should be, particularly in relation to updating customer information and designing ongoing monitoring frameworks.

During the development of the draft Guidelines, AMLA considered the following options.

A. **Prescriptive** approach.

B. **Principle-based** approach.

Option A

Under a prescriptive model, the draft Guidelines would specify in detail which documents, sources, review frequencies, monitoring parameters or technical features obliged entities should use. This could include consultation of specific registers, defining obligatory re-collection of documents or defining system functionalities for ongoing monitoring.

The benefit of this approach would be increased legal certainty and ease of benchmarking. Detailed provisions could limit interpretative divergence and facilitate implementation, particularly for smaller or less experienced obliged entities. From a supervisory perspective, such an approach could also support more consistent and structured supervisory assessment criteria, as compliance could be evaluated against clearly defined procedural and operational expectations.

However, these advantages would come at cost. Prescriptive rules tend to encourage formalistic, “tick-the-box” compliance, where adherence to enumerated steps substitutes for substantive risk assessment. These could undermine the core objective of Article 26, which embeds a risk-based approach to ongoing monitoring of the business relationship and monitoring of transactions performed by customers.

Moreover, prescriptive requirements may impose disproportionate burdens, particularly on smaller or lower-risk entities and in non-financial sector with non-continuous business relationships. Uniform obligations, such as automatic re-collection of expired documents irrespective of risk, could generate unnecessary operational and financial costs.

Detailed prescriptions also risk rapid obsolescence. Monitoring technologies, typologies and data sources evolve quickly. Embedding specific tools or technical parameters in Level 3 guidelines could hinder innovation and conflict with the principle of technological neutrality. In addition, selective prescriptiveness in certain areas could create uneven expectations across sectors, contradicting the logic of the horizontal structure and potentially incentivising compliance based on form rather than effectiveness.

Option B

Under Option B, the draft Guidelines would set out core outcomes and expectations, such as maintaining accurate and up-to-date customer information, implementing effective event-driven and periodic reviews, and operating monitoring frameworks capable of detecting unusual or suspicious activity, while leaving the choice of tools, methodologies and documentation to obliged entities, subject to proportionality.

The key benefit of this option would be flexibility anchored in clearly defined outcomes. It would align with the risk-based approach of Article 26 of AMLR and support effective integration between customer due diligence and ongoing monitoring. Obliged entities could design systems proportionate to their risk exposure and operational model, while remaining accountable for results.

This option would also reduce the risk of regulatory arbitrage based on formal compliance with detailed rules and support innovation, including the responsible use of advanced analytical tools. In addition, it would help to ensure that compliance costs are commensurate with risk rather than driven by uniform procedural requirements.

The main cost of this option would be that obliged entities might face higher initial interpretative and implementation effort. Some obliged entities, particularly those newly brought within scope of AMLR, may need to undertake additional internal effort to translate principle-based expectations into operational processes. AMLA may consider sharing additional material in the form of explainers along with the guidelines final text to help obliged entities better understand how to apply them. Ensuring supervisory convergence may also require continued supervisory dialogue and the sharing of good practices to promote a consistent understanding of the Guidelines.

Preferred option

Based on the considerations above, Option B was preferred. A principles-based approach best supports proportionality, effectiveness and technological neutrality. While a prescriptive model might offer short-term clarity, it would increase structural rigidity, risk formalistic compliance and generate disproportionate burdens. The chosen approach ensures that effectiveness is assessed by reference to outcomes and risk coverage rather than to mechanical adherence to specified inputs.

Policy Issue 3: Re-collection of expired identity documents, passports or equivalent

In the context of ongoing monitoring, Article 26(2) of AMLR requires obliged entities to ensure that the relevant customer's documents, data or information are kept up to date. As part of this obligation, a policy issue arose as to whether expired identity documents, passports or equivalent should always be re-collected once they expire.

Identity documents are collected during the customer identification and verification process. However, during the lifecycle of a business relationship such documents may expire while the relationship remains ongoing. The question therefore arises whether expiry alone should trigger the automatic re-collection of updated documentation, or whether obliged entities should assess the need for re-collection based on the risk profile of the customer and other relevant factors.

In this respect, AMLA considered the following options:

A. Automatic update of all expired identity documents.

B. Risk-based approach to updating expired identity documents.

Option A

Under Option A, the draft Guidelines would automatically require the update of all expired identification documents as part of ongoing monitoring. The benefit of this option would be uniformity and clarity, as expiration would automatically trigger action. However, the cost could be substantial. Automatic updates could create high administrative burdens, particularly for large customer bases, without necessarily improving risk mitigation. Expiry alone does not automatically imply higher ML/TF risk, since the identity has already been verified.

Under Option A, the draft Guidelines would require obliged entities to obtain updated identity documents whenever a previously collected identification document expires. Expiry of the document would therefore trigger a requirement to obtain a new document as part of the ad hoc or periodic customer information review.

The principal benefit of this option would be clarity and consistency. A uniform rule requiring the re-collection of all expired documents would provide a clear and easily enforceable standard for both obliged entities and supervisors. Expiration would constitute an objective trigger, removing the need for case-by-case assessments or internal policies to determine whether an update is required.

This option could also ensure that customer information review would reflect currently valid documents. In some jurisdictions, newly issued identity documents may contain enhanced security elements that help reduce the risk of document fraud or impersonation. In addition, automatic re-collection would contribute to greater supervisory comparability, as all obliged entities would follow the same rule regardless of customer risk profiles.

However, Option A would impose significant operational and administrative costs on obliged entities. Many obliged entities maintain large customer bases, including long-standing relationships with customers who present a low risk of money laundering or terrorist financing. Requiring the automatic re-collection of identity documents upon expiry would therefore necessitate contacting a large number of customers and processing large volumes of documentation, regardless of the underlying risk.

This could also negatively affect customer relationships, as repeated requests for updated documentation may create friction and inconvenience, particularly as customers have already been subject to identification and verification procedures and their risk profile remains low. In addition, such requirements could affect the allocation of internal resources. Compliance obligations related to document re-collection would need to be carried out primarily within the first line of defence, requiring employees to process large number of routine document updates that may not contribute meaningfully to risk mitigation.

Furthermore, the expiry of an identity document does not, in itself, necessarily indicate an increased risk of ML or TF. The customer's identity has already been verified at the onboarding stage, and the expiration of a document does not automatically invalidate the previously verified identity. As a result, requiring the automatic re-collection of all expired documents could risk becoming a largely formalistic exercise, generating significant operational effort while providing limited additional benefit in terms of preventing or detecting ML or TF.

Option B

Under Option B, the draft Guidelines would adopt a risk-based approach to determining whether expired identity documents should be re-collected. Instead of requiring automatic updates, obliged entities would assess whether re-collection takes place during next scheduled customer information review or earlier.

In line with the draft Guidelines, obliged entities would consider several factors when determining whether to update an expired document. Where re-collection would be assessed as necessary, obliged entities could use different verification methods, including electronic verification means. The timing of re-collection would also depend on the risk level. For example, re-collection may occur during the next scheduled customer review or next customer interaction for lower-risk situations, while it should occur as soon as possible where specific risks or doubts arise regarding the accuracy or adequacy of the existing identification data.

The main benefit of Option B is proportionality and efficient allocation of resources. By linking document re-collection to risk factors, obliged entities can prioritise situations where updated documentation provides genuine risk-mitigation value. For example, re-collection may be appropriate where the document has been expired for a significant period, where the issuing jurisdiction presents higher risks, or where the updated document would provide additional identifying information.

This approach also reflects the risk-based framework underlying in AMLR. It avoids unnecessary operational burdens while still ensuring that customers' identity documents remain reliable and up to date. In addition, the risk-based approach supports more effective monitoring, as resources can be directed towards customers and situations where there are doubts about the continued accuracy or adequacy of identification data or where ML/TF suspicions may arise.

The principal cost of this option is that it requires obliged entities to perform case-by-case assessments and maintain internal procedures to determine when re-collection is necessary. This requires developing internal policies, training staff and documenting the rationale behind decisions not to re-collect expired documents.

There may also be differences in implementation across obliged entities, as risk assessments and internal policies may vary. This could potentially reduce uniformity compared with an automatic collection and may require supervisory authorities to assess the adequacy of entities' risk-based approaches.

Preferred option

Option B is the preferred option. It better reflects the risk-based approach embedded in Article 26 of AMLR, which requires obliged entities to keep customer information up to date while taking into account the risks associated with the business relationship.

By allowing obliged entities to assess factors such as specific risks associated with the customer, issuing country's risk, the length of document expiry and the relevance of updated information, this approach ensures that identity documents are re-collected where this meaningfully contributes to risk mitigation, rather than imposing a blanket requirement that could create disproportionate burdens for low-risk customer relationships.

At the same time, the approach ensures that updated documentation is obtained as soon as possible in higher-risk situations or where doubts arise regarding the accuracy or adequacy of existing identification data, including where such doubts may give rise to suspicions of ML or TF.

Methodology

For all three policy issues, the analysis drew primarily on targeted exchanges with national competent authorities responsible for supervising obliged entities in both the financial and non-financial sectors, as well as on comparative legal analysis.

Across all three policy issues, the assessment focused on identifying the relative costs and benefits of the different options, taking into account the diversity of obliged entities. The analysis also considered consistency with existing EU-level guidance, in particular the EBA Guidelines EBA/GL/2021/02, as amended, and assessed the extent to which the options would support the effective, proportionate and risk-based implementation of AMLR.

Limitations

The analysis is primarily based on qualitative supervisory input and comparative legal assessment. While the exchanges with supervisors provided valuable insights into practical supervisory experience, they may not capture all sector-specific particularities, especially given the high degree of heterogeneity within the financial and non-financial sectors. In addition,

supervisory practices and market structures continue to evolve, particularly in relation to newly designated obliged entities. These limitations are mitigated by the principle-based design of the draft Guidelines, which allows for proportional application across sectors, and by the possibility to address emerging issues through interpretative tools, where necessary.

Further assessments

During the public consultation, respondents will have the opportunity to provide supporting data, evidence, or concrete examples to substantiate any proposals or suggested amendments to the draft Guidelines. In particular, stakeholders will be invited to submit quantitative data and information illustrating sector-specific risks, operational constraints, compliance costs, or supervisory impacts, where relevant.

This evidence-based input will support AMLA in re-assessing, where justified, whether proposed changes are proportionate, justified, and consistent with the risk-based approach underpinning the draft Guidelines, and in determining whether any further clarification or targeted adjustments are warranted.

5.2. Overview of questions for consultation

Question 1:

Do you consider that Guideline 1 supports a risk-based approach and clearly sets out the core principles that obliged entities should apply to keep customer information up to date?

If you see scope for further clarification, please:

(i) specify the paragraph concerned;
(ii) explain your rationale; and
(iii) consider submitting an amendment proposal

Question 2:

Do you foresee any challenges in applying Guideline 1, taking into consideration the differences in obliged entities' nature, risks and complexity of their business, as well as their size?

If you see scope for further clarification, please:

(i) specify the paragraph concerned;
(ii) explain your rationale; and
(iii) consider submitting an amendment proposal

Question 3:

Compared to your current ongoing monitoring process, what impact would *Guideline 1: Keeping customer documents, data or information up to date* have on your compliance costs and operational processes? Please provide:

a. the estimated percentage increase or reduction in annual compliance costs (increase/reduction/no effect by: below 25%; 25% to 50%; 50% to 75%; more than 75%). Please explain the basis for your assessment, including the methodology used and any supporting evidence.

b. Please rate the expected impact (very positive; positive; neutral; negative; very negative) on the following operational processes:

- periodic customer information review including document re-collection;
- event-driven reviews;
- implications for staff;
- other (please specify).

c. If you selected "negative" or "very negative" for any of the above under (b), please explain the basis for your assessment, including the methodology used and any supporting evidence, and indicate the distinction between one-off investment costs and recurring costs.

Question 4:

Do you foresee any challenges in applying Guideline 2? In your view, does the guideline provide sufficient clarity and is applicable across your products and services to support effective, risk-based monitoring of unusual or suspicious transactions and activities?

If you see scope for further clarification, please:

(i) specify the paragraph concerned;
(ii) explain your rationale; and
(iii) consider submitting an amendment proposal

Question 5:

Do you consider that the provisions on the use of automated or advanced analytical tools are sufficiently flexible and do not favour specific technologies?

If you see scope for further clarification, please:

(i) specify the paragraph concerned;
(ii) explain your rationale; and
(iii) consider submitting an amendment proposal

Question 6:

What impact would the design and implementation of the transaction and activity monitoring framework described in Guideline 2 have on your compliance costs? Please explain the basis for your assessment, including the methodology used and any supporting evidence.

(a) The estimated percentage increase or reduction in annual compliance costs (increase/reduction/no effect by: below 25%; 25% to 50%; 50% to 75%; more than 75%). Please explain the basis for your assessment, including the methodology used and any supporting evidence

(b) Please rate the expected changes in the following operational processes (very positive; positive; neutral; negative; very negative):
    - implications on staff;
    - processes and controls;
    - other (please specify).

(c) If you selected "negative" or "very negative" for any of the above under (b), please explain the basis for your assessment, including the methodology used and any supporting evidence, and indicate the distinction between one-off investment costs and recurring costs.

Question 7:

Do you identify any further opportunities for simplification or measures that could further support proportionality across the guidelines?

- If so, please provide concrete drafting proposals and explain why the specific measures you propose would be more appropriate.