2 September 2026

Privacy First response to the AMLA consultation on the monitoring guidelines

The EU must not become a financial surveillance state in which citizens' fundamental rights are ignored!

Foreword

On 2 September 2026 Privacy First has participated in the consultation by the *Authority for Countering Money Laundering and Financing of Terrorism* (AMLA) on draft-guidelines regarding the ongoing monitoring of customers by companies subject to anti-money laundering obligations ('OEs'), announced by the AMLA on 3 June 2026. [1]

The draft guidelines are set out in the consultation paper of 3 June 2026. [2] Feedback could only be provided via consultation questions, which could be found on a separate page under 'Public consultation questions". [3]

The following pages contain a formatted version of Privacy First's consultation response. We would like to point out that the headings have been added by us and do not form part of our consultation comments.

Notes:

[1] https://www.amla.europa.eu/amla-consults-draft-guidelines-ongoing-monitoring-business-relationships_en
[2] https://www.amla.europa.eu/document/download/46b50078-08ed-4ab1-aea0-28b1a6085755_en?filename=Consultation%20Paper%20-%20Article%2026%285%29%20AMLR.pdf
[3] https://ec.europa.eu/eusurvey/runner/eaddcaba-57d5-0f7d-d5e1-f33d815dee5b

Privacy First Foundation
John M. Keynesplein 10
1066 EP Amsterdam
https://privacyfirst.nl
info@privacyfirst.nl
+31 20 810 0279
KvK 34298157
ANBI accredited

PRIVACY FIRST

Contents

Introduction

This consultation concerns the performance of public tasks in the field of combating crime by, amongst others, banks and accountants, the obliged entities (OEs), based on European regulations against money laundering and terrorist financing (AML/CFT). The *Authority for Countering Money Laundering and Financing of Terrorism* (AMLA) is consulting on draft guidelines on how OEs should organise ongoing customer monitoring of their customers. The purpose of ongoing monitoring is to ascertain whether the customer is involved in criminal activity or holds criminal proceeds. If the OE suspects that this is the case, it must report this to the authorities (the FIUs).

Privacy First has the following fundamental concerns regarding the proposed guidelines.

First, compliance with these guidelines effectively results in **preemptive and continuous monitoring of citizens' behaviour**, with far-reaching consequences for their daily lives. Efforts to detect money laundering and crime in general now go so far that every law-abiding citizen is monitored by the public authorities—via private entities—at every step of his/her life. Privacy First is deeply concerned that the AMLA does not recognise that creating an infinite number of vague legal grounds that create exceptions to fundamental rights principles and circumvent privacy rules, turn these fundamental rights into an illusion. Applying these draft-guidelines leads to a European surveillance state, that does not adequately respect fundamental rights as enshrined in, amongst other things, European legislation such as the Charter and the GDPR. We observe that whilst compliance with these rights is professed in words, the reality on the ground is quite different. Furthermore, Privacy First notes that public tasks are being delegated to OEs, whilst the position of the various groups of OEs varies greatly and their knowledge and skills also differ. If government tasks are delegated to OEs, due consideration must be given to those OEs capacity to carry them out and to respect fundamental rights.

Secondly, Privacy First notes all legal texts dealing with anti-money laundering and crime are always replete with the concept of a **risk based approach** but as of yet there is no clarity of what this entails. The AMLA also does not explain in these draft-guidelines what a risk based approach is. The usual answer that risk based means "*focusing on the greatest risks*" is too vague to apply in real life. Privacy First calls upon the AMLA to give the concept real substance. Our suggestion: genuinely downsize monitoring requirements for low-risk customers and focus on high-risk groups. With such a system, the AMLA would only need to define what constitutes high-risk customers. Taking into consideration most citizens are law-abiding this group should not amount to a high percentage.

Our proposed approach would be proportionate and risk-based, and moreover in line with how government and public prosecutors themselves investigate and prosecute crime.

Thirdly, what is striking about the draft is that the AMLA pays no attention whatsoever to the position of the **data subjects and the customers** of OEs, who should also be informed about the monitoring activities and should be able to assess whether the OEs are complying with their obligation not to request more data than is necessary (data minimisation).

Privacy First PF points out that no attention is being paid to address prevention of the harmful effects of the AML/CFT-system and that the draft-guidelines contain incorrect perceptions of digital risk profiling and wrongly fail to include a ban on the use of automated means to detect crime, as further explained below.

Privacy First calls on the AMLA not only to focus on combating crime, but also to take responsibility for the **harmful social consequences** of the privatisation of crime-fighting. Privacy First urges the AMLA to help prevent abuses and the emergence of a society governed by financial surveillance. Privacy First draws the AMLA s attention to the serious abuses that have taken place in the Netherlands and which have led to fundamental criticism in the Netherlands from, amongst others, the Netherlands Institute for Human Rights, the Dutch Data Protection Authority, the Netherlands Court of Audit (Algemene Rekenkamer) and the Advisory Division of the Council of State (Raad van State).

Privacy First argues that the current landscape of **automated risk profiling**, whether carried out by public authorities or by OEs, is immature, and that the AMLA should specify in the draft-guidelines that the use of digital tools for risk assessment and monitoring is not permitted.

The AMLA places too much faith in the use of digital tools (such as AI) by financial institutions to determine whether a customer might be a criminal. We draw attention to the important reports that have been published on risk profiling, which show that digital systems are flawed and lead to discrimination and exclusion. These include, amongst others,

* the international report by Amnesty International '*Automating suspicion*' (https://www.amnesty.org/en/documents/POL40/1096/2026/en/), announced by Amnesty International in *Risk profiling systems used to identify potential offenders are in breach of international law and must be banned* (https://www.amnesty.org/en/latest/news/2026/06/risk-profiling-systems/);

* the advice from the Dutch State Commission against Discrimination and Racism, that is calling on the government to stop using data-driven profiling for the detection of fraud and crime, announcement (https://www.staatscommissietegendiscriminatieenracisme.nl/actueel/nieuws/2026/05/07/staatscommissie-stop-datagedreven-profilering-door-overheid-vanwege-discriminatie).

Privacy First notes – given the current immature digital landscape – that it be concluded that automated risk profiling to detect criminal funds and/or criminals cannot take place. Nowadays, it is becoming increasingly clear that public duties (AML/CFT) should not be carried out by amateurs (the OEs), but that they need to be carried out by public sector professionals, under strong independent supervision.

We advocate a complete ban on automated risk profiling in the fight against crime, not only for public authorities but also for private organisations, given that both the actors and the systems are still immature (and may never achieve maturity).

Privacy First has a large number of other comments on the draft-guidelines, which are set out later in this consultation response.

Privacy First is counting on the AMLA to take responsibility for the impact of AML/CFT regulations on citizens fundamental rights and to adopt a critical and independent stance. This stems from the significant responsibilities assigned to the AMLA under the AML Package.

General comments

There are major flaws in this consultation and in the draft:

[1] The consultation form does not include an option to explain why an organisation (such as ours) is taking part in the consultation. We would like to draw your attention to the fact that **Privacy First** is a foundation established under Dutch law and has been working on privacy issues for a very long time. Financial privacy is one of our key areas of focus. We have observed that, in the fight against money laundering and terrorist financing and in compliance with sanctions regulations (AML/CFT), insufficient attention is paid to citizens fundamental rights. It is the AMLA s responsibility to also take fundamental rights into account and to prevent unnecessary data collection, discrimination and exclusion. We are calling on the AMLA to address this.

[2] The questions in this consultation are **limited to only pages 22 up to and including page 41 (guidelines 1 and 2, 'the draft-guidelines'**). That is incorrect, as the pages 16 to 21 and 42 to 53 also form part of the draft and are relevant to the meaning of the draft-guidelines. The questions only refer to obliged entities ('OEs'), not to their customers, that include many natural persons and SMEs. Privacy First is deeply concerned about **the implications of the AML Packages for natural persons** (customers, representatives, ultimate beneficial owners and other individuals subject to scrutiny by OEs). It is essential that the AMLA also takes their position into account and poses questions to them (or to the organisations representing them).

[3] Privacy First has noted that the draft contains texts and elements that are **not based on the AMLA s powers** under Article 26(5) of the AMLR. Example 1, section 1.1: "*These guidelines set out specific rules obliged entities should apply*", which is incorrect as the rules are set out in the AMLR; the purpose of the guidelines is to clarify the rules, not to create new ones. Example 2: the draft contains provisions relating to training (pages 5, 10, 54, especially page 20 nr. 7), which is not covered by Article 26. We also note that the AMLA has made its own adaptations of passages from the AMLR, which raises the question of whether the meaning intended is different. This could lead to ambiguity, which is highly undesirable. The AMLA must be strictly consistent with the text of the AMLR and the recitals to this regulation.

[4] We note that the **draft is based entirely on large OEs like banks**. This is undesirable, as these large OEs are already familiar with many of the issues and have capabilities that most other OEs do not have. Given the AMLA s responsibilities in EU society, these draft-guidelines should, in principle focus on OEs that are SMEs and on the customers of OEs and related persons, whilst the position of large enterprises could be addressed separately.

[5] The Netherlands served as a testing ground for AML/CFT. Experience in the Netherlands has shown that the system has led to widespread **discrimination and exclusion**, not only of foreign nationals or people with foreign-sounding names, but also of all manner of

organisations and sectors. There are several relevant reports on the downsides of AML/CFT, e.g. by the Dutch National Audit Office (Algemene Rekenkamer) and the Dutch Council of State (Raad van State). The AMLA is well aware of this. Yet we see no reflection of this in the draft-guidelines. It is precisely in the area of ongoing monitoring as referred to in Article 26 of the AMLR that problems arise.

Relevant documents are:

* The advice of the Dutch **Council of State**, which was made public in August 2026 (https://www.raadvanstate.nl/adviezen/@158150/w06-26-00123-iii/#toonsamenvatting). The Council makes comments that are also relevant to the draft-guidelines, e.g. (machine-translation): "*The Council points out that current legislation already prescribes a risk-based approach, but that this has not yet been sufficiently implemented in practice. It is not plausible that the new regulations will automatically lead to better implementation. (…) Research has shown that members of the public are sometimes discriminated against in their dealings with financial institutions. This can have far-reaching consequences: if a current account is refused, a person cannot participate fully in society. Although the new rules specifically state that discrimination is prohibited, it is currently unclear how this will be implemented in practice and who will be responsible for monitoring compliance. The Council advises the government to set out, in the explanatory notes to the bill, how the supervisory authorities will be enabled to effectively monitor compliance with these provisions by so-called obliged entities, such as banks and notaries.*".

* In June 2026 **Amnesty International** published an international report on risk profiling, titled '*Automating suspicion*', which states that risk profiling systems used to identify potential offenders are in breach of international law and must be banned (press release: https://www.amnesty.org/en/latest/news/2026/06/risk-profiling-systems/, report https://www.amnesty.org/en/documents/POL40/1096/2026/en/). The implication of this report is that automated risk profiling systems cannot be used in the AML/CFT context, certainly not by small OEs. It may be that large OEs need to use automated systems, but the significance of the output is highly questionable, given Amnesty's findings. Privacy First therefore advises that this be taken into account and that automated risk profiling is prohibited.

* In March 2026, the Dutch **National Audit Office** published the report '*Significant consequences, unknown benefits – A study into the anti-money laundering approach in the banking sector*' (https://www.rekenkamer.nl/documenten/2026/03/11/gevolgen-groot-opbrengsten-onbekend---onderzoek-naar-de-anti-witwasaanpak-in-de-bankensector), which had been announced in an article

(https://www.rekenkamer.nl/actueel/nieuws/2026/03/11/anti-witwascontroles-hebben-grote-gevolgen-voor-burgers-opbrengst-is-onbekend). The report shows that there is no evidence of the effectiveness of banks AML/CFT activities.

* In August 2025 **Privacy First** participated in a consultation on implementation of the AML Package in the Netherlands (https://privacyfirst.nl/wp-content/uploads/consultatie_Iwt_PrivacyFirst_29aug2025.pdf) and published an article on the threat of permanent surveillance under new AML/CFT-rules (https://privacyfirst.nl/en/articles/permanent-surveillance-threatened-under-new-anti-money-laundering-rules/). In Appendix 1 (in Dutch) of the consultation response you find information on the shadow side of the privatisation of crime-fighting, including many important sources of information, like the KPMG report (https://www.rijksoverheid.nl/documenten/2024/04/19/rapport-kmpg-en-i-o-research-naar-ervaren-discriminatie), the findings of the Netherlands Institute for Human Rights (https://www.mensenrechten.nl/actueel/nieuws/2025/01/29/discriminatiemonitor-2024-discriminatie-door-banken-in-beeld), and ING Bank s acknowledgement that it has been guilty of widespread discrimination (https://nieuws.ing.nl/nl-NL/250333-ing-luistert-leert-en-handelt-om-ervaren-discriminatie-te-voorkomen/).

Privacy First emphasizes the importance of the AMLA paying due regard to fundamental rights. The authority plays a key role not only in combating crime but also in protecting citizens from abuses arising from AML/CFT measures. We call on the AMLA to take this responsibility seriously.

[6] In the draft, the AMLA takes **automated monitoring** as its starting point and believes that such automated monitoring could yield relevant results.

Please note the following:

* In June 2026 Amnesty International published an international report on risk profiling, titled 'Automating suspicion' which states that risk profiling systems used to identify potential offenders are in breach of international law and must be banned (press release: https://www.amnesty.org/en/latest/news/2026/06/risk-profiling-systems/, report https://www.amnesty.org/en/documents/POL40/1096/2026/en/). The implication of this report is that automated risk profiling systems cannot be used in the AML/CFT context, certainly not by small OEs. It may be that large OEs need to use automated systems, but the significance of the output is highly questionable, given the Amnesty's findings.

* In May 2026 the Dutch State Commission against Discrimination and Racism has called on the government to stop using data-driven profiling for the detection of fraud and crime. This Commission, comprising academics and other experts, has

concluded that data-driven profiling does not lead to the desired results. The advice relates to the government and also applies to the performance of public tasks by businesses, as set out in the AML/CFT. More information you find in their announcement (https://www.staatscommissietegendiscriminatieenracisme.nl/actueel/nieuws/2026/05/07/staatscommissie-stop-datagedreven-profilering-door-overheid-vanwege-discriminatie) and their report (https://www.staatscommissietegendiscriminatieenracisme.nl/documenten/2026/05/07/principes-voor-profilering), there is a summary in English (https://www.staatscommissietegendiscriminatieenracisme.nl/site/binaries/site-content/collections/documents/2026/05/07/principes-voor-profilering/englisch-summary.pdf).

It can be inferred from these reports and other independent publications on risk profiling and predictive policing that the value of automated systems in monitoring customers is very limited, while their discriminatory impacts are well-documented. If large-scale systems are to be used at all, very robust safeguards are required, which, to the best of our knowledge, are not provided for in the AML/CFT regulations.

In Privacy First s view, providers of automated risk profiling systems are insufficiently capable of mitigating the human rights issues they cause. Policymakers and large OEs, too, repeatedly demonstrate that they are playing with fire by deploying AI and other digital applications without proof of their effectiveness and without adequate safeguards. Given that the landscape is so immature, Privacy First takes the view that all OEs should be prohibited from using digital tools to track down criminals and crime.

(Even if the above requirements were to be met at some point in the future, such systems should never be used by OEs that are SMEs, and other OEs should only be permitted to use such systems following rigorous assessment and subject to effective oversight. The use by should only be permitted subject to very robust safeguards. It must be possible for these safeguards to be independently assessed by experts who have no financial interests in advising OEs, their sector associations or the or investigative authorities.)

[7] The AML/CFT system has significant societal implications, as has become apparent both in the Netherlands and elsewhere in the EU. Nevertheless, the only **organisations from civil society** that currently are involved are those that represent OEs, and those that are engaged in the fight against crime and that show no interest in the violations of fundamental rights resulting from the AML/CFT system, such as Transparency International. This is a major shortcoming which can be rectified by the AMLA when developing its guidance.

[8] The AMLA may be aware that the new AML/CFT rules contain a large number of provisions that **infringe citizens fundamental rights**. One example of this is that all

members of parliament, as well as their parents and children, are by definition regarded as posing a high risk of criminal activity. As you know, this is an incorrect assumption on the part of the European legislator, which has not been substantiated by the facts, as can be confirmed, for example, by banks. It is part of the AMLA s role in society to ensure – until the rules that infringe fundamental rights have been amended or declared void – that no harm is caused in practice.

[8] Please **refrain from paraphrasing the text of the AMLR** in your own words, as this may lead to confusion and difficulties in understanding, and may raise the question of whether the AMLA is creating new rules without having the authority to do so.

[9] The subject matter of this draft is closely linked to, amongst other things, the risk variables and risk factors involved in entering into business relationships (Article 20(3), Article 42), the basis of KYC (Article 28(1)) and the reporting obligation under Article 69 (guidelines under Article 69(6)). **Separating all these elements results in an incoherent and unbalanced whole**.

[10] The AMLA will be aware of the enormous **security risks** posed by new technologies and the large number of cyber-attacks that have taken place recently. Examples of this include the breach of Liechtenstein s BO register (https://www.reuters.com/world/liechtenstein-says-hackers-access-information-31000-legal-entities-2026-08-03/), attempts to gain unauthorised access to the Luxembourg BO register via attorneys, breaches affecting the French government (including the French tax authorities and the register of bank details) and the large-scale breach at the Latvian state agency responsible for vehicle registration, driving licences and other services for drivers (https://bnn-news.com/data-of-1-2-million-people-leaked-in-csdd-cyberattack-in-latvia-including-personal-id-numbers-and-addresses-282949).

It has become clear in recent times that the security landscape has deteriorated significantly, as evidenced, amongst other things, by the AI attacks on financial institutions, as reported by, amongst others, The Guardian in the article 'AI firm claims it stopped Chinese state-sponsored cyber-attack campaign', https://www.theguardian.com/technology/2025/nov/14/ai-anthropic-chinese-state-sponsored-cyber-attack.

The article quotes an expert:

> "*Woźniak said Anthropic s release was a distraction from a bigger cybersecurity concern: businesses and governments integrating complex, poorly understood" AI tools into their operations without understanding them, exposing them to vulnerabilities. The real threat, he said, were cybercriminals themselves – and lax cybersecurity practices. (…) Woźniak said: Anthropic s valuation is at around $180bn, and they still can t figure out how not to have their tools subverted by a tactic a 13-*

year-old uses when they want to prank-call someone. Marius Hobbhahn, the founder of Apollo Research, a company that evaluates AI models for safety, said the attacks were a sign of what could come as capabilities grow. I think society is not well prepared for this kind of rapidly changing landscape in terms of AI and cyber capabilities. I would expect many more similar events to happen in the coming years, plausibly with larger consequences."

The AMLA will also be aware of **the warnings issued** by the European Systemic Risk Board (ESRB) (https://www.esrb.europa.eu/news/pr/date/2026/html/esrb.pr260707~4e1b68241a.en.html) and the call made by the ESAs to financial institutions (FIs) (https://www.eba.europa.eu/publications-and-media/press-releases/eba-eiopa-and-esma-call-enhanced-governance-and-consistent-supervision-mitigate-ict-risks-frontier). The risks for other organisations are even greater, as their cybersecurity is far less advanced than that of FIs. On 31 August 2026 the Financial Stability Board published the press release 'FSB Chair warns of risks arising from frontier Artificial Intelligence (AI) models', https://www.fsb.org/2026/08/fsb-chair-warns-of-risks-arising-from-frontier-artificial-intelligence-ai-models/, showing how urgent the problems with AI are.

A characteristic of the AML/CFT system is that OEs have to spend a great deal of time and money providing evidence that their AML/CFT due diligence has been carried out properly, without it having been established (particularly in the case of smaller OEs) that this contributes to the fight against crime. This is reflected in various passages in the AMLR that refer to to record, to document and similar terms. Out of fear of not doing things properly, OEs will request an **unnecessary amount of information** and will also ask for information that is not relevant to the fight against crime.

[11] The 'Executive Summary' and the 'Background and rationale' contain a number of shortcomings, including the suggestion that the draft guidelines would be suitable for all types of OEs and would meet the requirements of proportionality. As explained above, the draft does not meet these requirements.

Proposals of Privacy First related to the general comments

[1] Privacy First advises you to always include a question about the reason why an organisation is taking part in the consultation, leaving space for further explanation.

[2] Privacy First advises you to withdraw this consultation, to hold a new consultation on the full text of the draft directive and to include questions for the customers of OEs and related persons, and civil rights organisations that defend their interests.

[3] Privacy First advises you to screen the text of the draft in full and to remove anything that is not based on Article 26 of the AMLR. We also recommend that you do not rephrase

texts from the AMLR in your own words, but instead quote passages verbatim from the AMLR and provide clear explanations alongside them.

[4] Privacy First recommends that the draft be completely rewritten, taking our comments into account. We recommend aligning the text with that of the AMLR, keeping it as simple as possible and taking into account the different positions of the various types of OEs. The current text is written for the banks, which do not require this information. Move away from the approach whereby the AML/CFT working methods of banks are described, followed by the text that other OEs must achieve the same result using different means. This is incorrect and creates uncertainty for both SME OEs as the customers of all OEs, as well as for those associated with these customers.

[4] + [5] Privacy First advises the AMLA to completely revise the draft, taking into account amongst others the following recommendations and comments that we mentioned.

[6] Privacy First advises the AMLA to completely revise the draft, taking into account the recommendations of Amnesty International and the Dutch State Commission against Discrimination and Racism, and to propose that automated risk profiling is prohibited.

[7] Privacy First advises the AMLA to involve organisations that defend citizens fundamental rights closely in the preparation of further rules by the Commission and the guidelines for which the AMLA itself is responsible. Examples include organisations representing minority groups, such as people of Iranian or North African origin, and organisations representing SMEs. It is important to actively seek out customers who are being disadvantaged, as they themselves often do not realise why they are being disadvantaged and discriminated against.

It would be useful if the AMLA were to set up national reporting centres for clients of OEs, where complaints about the conduct of OEs could be reported, so that the AMLA is quickly made aware of the harm caused by OEs AML/CFT compliance.

Privacy First advises the AMLA to identify which elements of the new AML/CFT system infringe the fundamental rights of European citizens and, as part of this monitoring, to propose measures in guidelines and other documents drawn up by the AMLA to prevent harm caused by such elements. Take into account the experience already gained in this regard, including in the Netherlands (as evidenced by the report of the Netherlands Court of Audit (Algemene Rekenkamer) and other reports), and consult organisations representing affected customers.

[8] Privacy First advises the AMLA to reproduce the text of the AMLR verbatim, insofar as it is relevant to the draft-guidelines, and provide clarification where necessary, particularly for OEs that are SMEs. It will be even clearer if specific attention is paid to the position of the particular OE. Recognise that a one-size-fits-all approach does not work, given that there is a fundamental difference between the level of knowledge of a bookkeeper and that of a large bank.

[9] Privacy First recommends to present the topics relevant to customer due diligence, on which the AMLA draws up documents (Article 20(3), Article 28(1), Article 26(5), Article 42 and Article 69(5)) as a single, coherent whole to the OEs, in order to prevent fragmentation and to promote understanding amongst the OEs that are SMEs, all customers of OEs and the persons involved with those customers.

[10] Pay particular attention to **data minimisation**, given that the security risks posed by new technologies have increased so significantly. Privacy First advises the AMLA to limit the obligations to provide evidence to what is prescribed in the AMLR and not to impose any additional obligations of its own. It is also recommended that clarification be provided regarding what is expected in terms of providing evidence by OEs, taking into account the sector in which the OE operates and the data that the OE can reasonably be expected to have at its disposal. It is desirable that the AMLA also specifies that, in the case of long-term relationships, KYC data that is no longer relevant should be deleted, in order to reduce security risks to those concerned.

The large-scale collection of confidential data, including personal financial data, which is also retained for a long period (up to five years after the end of the business relationship), particularly in the case of long-term relationships with OEs that hold a great deal of information about the customer (like banks, bookkeepers), poses a significant risk to the security of citizens and organisations. The AMLA can help to mitigate the risks associated with large-scale data collections – which act as a honeypot for criminals – by limiting unnecessary burdens of proof, whilst also taking into account the sector in which the OE operates and the data the OE already requires for its own activities. To prevent security risks to OEs, their customers and security risks within the EU, it is important that measures are taken to limit the amount of confidential data processed. Privacy First calls on the AMLA to contribute to this.

[11] Privacy First recommends that the 'Executive Summary' and the 'Background and rationale' are amended to reflect an improved version of the draft-guidelines.

Comments on details of the draft-guidelines

Introductory comments

[12] In chapter 1 of the draft, '*Subject matter, scope and definitions*', section 1.1 states that the guidelines would contain **specific rules**. This is incorrect, as the AMLA cannot lay down rules.

[13] The general guidelines in section 2.1 are the AMLA s own interpretation of Article 26 of the AMLR and some other provisions from the AMLR. This adds no value and raises the question of whether **the AMLA is attempting to amend the relevant provisions** of the AMLR. This is undesirable and leads to ambiguity.

[14] The AMLR contains **vaguely worded terms**, which cause uncertainty amongst OEs and their clients. It is precisely the AMLA s role to provide clarification.

The text is replete with the concept of "risk-based approach" but does not clearly explain what is meant by it. We request AMLA provides a definition that gives real substance to the concept.

Examples of other texts that require clarification:

relevant documents, data or information (Article 26(2)) > when is something relevant?
change in the relevant circumstances (Article 26(3)) > which circumstances are relevant?
a relevant fact which pertains to the customer (Article 26(3)) > what is a relevant fact?
frequency… commensurate with the exposure (Article 26(4)) > when is the exposure low?
activities … are the proceeds of criminal activity or are related to terrorist financing or criminal activity (Article 69(1)(a)) > what is meant by activities ?
activities (Article 69(2)) > what is meant by activities ?
the characteristics of the customer and their counterparts (Article 69(2)) > what is meant by characteristics ?

The annexes contain many vague terms that are relevant to monitoring, including

reputation (Annex I, point (a)(ii)) > what is meant by this, and how can it be ascertained amongst the general public?
nature and behaviour (Annex I, point (a)(iii)): what do these terms mean, and how is an OE supposed to interpret them?

relevant personal links (Annex I, point (a)(vi)) > when does this apply?
purpose (Annex I(b)(i) > in many cases, the purpose is simple and clear; how should an OE deal with this aspect?
regularity or duration (Annex I(b)(ii) > what is meant by this, and how is it relevant to the risk of crime?
level, complexity, value (Annex I(b)(iii), (iv), (v), (vi))

[15] In section 2.2, the AMLA, points 12 to 14 inclusive, discusses relevant **sources of information**. This is not a subject covered by Article 26 of the AMLR; consequently, by including this provision, the AMLR exceeds the mandate set out in Article 26(5). For that reason alone, section 2.2 should be deleted.

Even if it were not outside the scope, the text would still be incorrect, as it imposes additional obligations on OEs beyond those set out in the AMLR, whilst failing to take into account that several of the sources mentioned in section 2.2 are neither accessible nor affordable for OEs that are SMEs. Furthermore, the text provides no clarity whatsoever and therefore fails to meet the expectations that OEs and their customers have of the guidelines.

Furthermore, point 12(b) wrongly cites data brokers as a source of information, even though this is an unregulated sector subject to no oversight regarding integrity or data protection. It is well known that in this sector, data – particularly consumer data – is frequently obtained illegally, that the data is unreliable, that data subjects are not informed, and that the GDPR is not complied with in other aspects either.

Point 15 of section 2.2 incorrectly states that unusual transactions or activities must be reported under Article 69 of the AMLR. Article 69 does not require this. There are many unusual things that have absolutely nothing to do with crime, so this term is of no use in the customer survey

Furthermore, there is no reason to include a provision on reporting, as this already follows from Article 69.

[16] Privacy First is very surprised by the wording of points 16 to 18 of section 2.2, given that a **natural person s identity** does not change. We fail to see how a copy of a valid identification document contributes to the fight against crime, whilst the large-scale storage of copies of identity documents does pose a huge security risk to all EU citizens. We refer to our earlier comments on the increased risks.

Privacy First supposes that the AMLA does not fully understand what is going on:

* The identity of a natural person who is a customer does not change; only if there is reasonable doubt as to their correct identity is there grounds for re-verification,

which does not, however, necessarily mean that a new copy of an identity document needs to be stored. It is safer not to do so.

* The situation of a customer who is not a natural person differs fundamentally from that of customers who are natural persons, as in the former case the relevant natural person (such as the representative or the ultimate beneficial owner) may change. If such a client is entered in the commercial register or another public register and the relevant persons are duly recorded in that register, there is no reason to verify their identity, as the registrar has already done so. There is more reason to check whether the status is correct; therefore, in the case of the ultimate beneficiary, it should be verified whether they have been registered with this status on valid grounds (for example, due to a shareholding). The same applies to a representative: has this person actually been appointed as such by the competent body?

Proposals of Privacy First

[12] Privacy First recommends that section 1.1 should make it clear that this document contains explanations and interpretations.

[13] Privacy First recommends that section 2.1 be deleted or replaced with quotations from the relevant provisions of the AMLR for the interpretation of Article 26 of the AMLR. Furthermore, if the AMLA deems it necessary, these quotations may be accompanied by clarifications and explanations. Passages that do not relate to Article 26 AMLR (such as the text in section 2.1 concerning training in point 7 and governance in point 8) should be deleted.

[14] Privacy First advises the AMLA to clarify the risk-based approach and to use the guidelines to clarify (other) vague terms in the AMLR, particularly for customers, data subjects and small OEs.

[15] Privacy First recommends that section 2.2, points 12 to 15 inclusive, be deleted in their entirety, as it falls outside the scope of Article 26(5) AMLR. Insofar as the AMLA wishes to include similar wording in another document, Privacy First advises against this, firstly because it adds nothing to what is already laid down in the AMLR and, secondly, because the private sources referred to in point 12(b) are not reliable.

[16] This means that the heading RE-COLLECTION OF EXPIRED IDENTITY DOCUMENTS, PASSPORTS OR EQUIVALENTS can be removed and points 16 to 18 should be completely rewritten. The key points could then be:

* A new verification of the identity of a natural person who is a customer is only necessary if there is reasonable doubt as to their identity.

* If, in the case of a customer who is not a natural person, new natural persons come to the fore to whom the identity verification obligations apply, the OE shall carry out such verification as soon as possible if there is no certainty that their identity has already been verified by other means (for example, via the commercial register).

Section 2.3 - reviews

[17] In the text of section 2.3 on periodic customer information reviews, the AMLA sets out the provisions of the AMLR, without adding any further clarification. It is not only the AMLA s responsibility to ensure that OEs carry out their anti-crime duties properly; the AMLA must also use the guidelines to ensure that OEs do not collect excessive amounts of data out of fear of fines and other enforcement measures.
The COE committee, '*Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*', amongst others, highlighted this risk in its 2023 guidelines ('*Guidelines on data protection for the processing of personal data for anti-money laundering/countering the financing of terrorism purposes*'):

> "*In practice, it appears that, in many instances, private-sector entities may lack clear and specific guidance needed on collecting customers personal data as part of AML/CFT obligations. For instance, regarding specific datasets to be collected as part of CDD obligations, OEs need to observe both data protection and AML/CFT legal obligations and may struggle to understand how to achieve both goals in a consistent and compatible way, notably with regard to the application of the data minimisation principle. As a result, by fear of exposing themselves to reputational and other risks caused by (i) the unintended processing of proceeds of crime, or (ii) the possibility of being subject to administrative fines or action by competent supervisors of both financial institutions and DNFBPs, private-sector entities may end up sharing larger volumes of data just in case". In that sense, the proper implementation of a risk-based approach from an AML/CFT perspective would also allow for alignment with the proportionality requirement envisaged under data protection requirements. An effective application of a risk-based approach requires clear and practical guidance and training by supervisory authorities, investment in resources and expertise by OEs, and a proportionate application and enforcement of national AML/CFT laws.*".

Section 2.3 contains a large number of general descriptions that add nothing to the text of the AMLR (including the preamble). For example, the *purpose and intended nature* of the business relationship is usually self-evident, and the real question is when attention should actually be paid to it. Point 22 is typically written for financial institutions; other organisations cannot make any use of it at all. Point 23 does not clarify in which cases the source of funds should be investigated.

The AMLA is aware that the unnecessary collection of excessive amounts of personal data and other confidential information poses a significant risk in the context of AML/CFT. It is the AMLA s responsibility to prevent this; however, the wording of section 2.3 does not contribute to this.

Proposals of Privacy First

[17] Privacy First suggests to replace section 2.3 completely with clear and proportionate guidance on the interpretation of the provisions of AMLR that are relevant for the obligations of OEs that are SMEs and understandable for customers and data subjects.

Section 2.2 / 2.3 - verification of the identity

[18] In our previous comments, we have already explained that the AMLA is mistaken when it comes to **identity verification**. The approach taken by the AMLA in points 16–18 of section 2.2 and also in point 21(a) of section 2.3 is incorrect, as a distinction must be made between the customer who is a natural person, and other relevant natural persons. This distinction is not made in point 21(a). The identity of a natural person does not change (unless the person dies). In the case of individuals who have a relationship with a customer, the key consideration is whether they still have a relevant relationship with that customer, such as acting as a representative or authorised signatory. For these individuals, it is the relationship that matters, not their identity, if this has already been verified.

Proposals of Privacy First

[18] Privacy First emphasises that the incorrect interpretation of the term identification should not be included in section 2.3.

Section 2.4 - event-driven reviews

[19] Section 2.4 on **event-driven reviews** suffers from the same shortcomings as Section 2.3. The text merely paraphrases the AMLR and fails to provide the clarification that customers

and OEs that are SMEs need. It fails to take into account that these OEs do not have a monitoring framework comparable to that of financial institutions. Examples of serious shortcomings include: point 25 does not explain what relevant changes are and this point presupposes knowledge and skills that OEs do not possess. Point 25 stipulates in its final sentence that the OE must prove the measures taken, which places an additional bureaucratic burden on OEs that are SMEs. As noted above, it is undesirable to impose obligations to provide evidence on OEs unless it has been demonstrated that such obligations contribute to the OE s role in combating crime, especially when the OE is an SME. To the best of our knowledge, it has not been proven that such obligations are of any use to these OEs.

Privacy First is calling on the AMLA to come down from its ivory tower and provide practical guidance to all OEs, ensuring that data collection is necessary and proportionate. This information is also very important for data subjects (natural persons that are customer, representative of a customer, BO of the customer or otherwise involved).

The type of terminology that requires clarification is e.g.:

* 'relevant changes', 'changes in the relevant circumstances' (point 25, 27);

* 'proportionate to the nature, risks and complexity of their business' (point 25);

* 'sufficient and relevant documents, data or information' (point 26).

Point 27 lists many triggering events for which it is unclear why they are relevant to the fight against crime. Furthermore, there are unclear concepts and facts, the meaning of which is not clear. Privacy First wonders why the facts mentioned in point 27 should, by definition, lead to a re-investigation and why this cannot be left to the discretion of the OE. We do not understand what is meant by '*Changes in identity*' and by '*identity details*' (point 27(a)), nor do we understand what nationality has to do with the likelihood of a customer being a criminal. Trigger events must be limited to facts that indicate criminal activity.

Point 27(b) is even more baffling: what does the AMLA mean by *behaviour* and by *activity-based or transactional anomalies* , '*unusual transaction patterns, inconsistent behaviour, frequent and unexplained changes of professional service providers*', and how does the AMLA arrive at the conclusion that OEs could (be able to) detect these? Can a bank infer behaviour from financial transactions if the bank never meets the customer in person? Why does the AMLA think that '*the expected purpose and intended nature of the business relationship*' have anything to do with the possibility that the customer is involved in crime? Why is the AMLA referring to Article 69(5) AMLR guidelines that are not yet published?

This point largely covers what is already set out in the AMLR, perhaps with the exception of the rather odd focus on IP addresses and device location, that is discussed hereinafter.

Proposals of Privacy First

[19] Privacy First suggests to replace section 2.4 completely with clear and proportionate guidance on the interpretation of the provisions of AMLR that are relevant for the obligations of OEs that are SMEs and for their customers and the data subjects. We recommend refraining from including provisions imposing additional obligations to provide evidence and not including elements that only are relevant only to financial institutions, as these would be of no use to the other OEs.

Section 2.4 - IP address and device location

[20] Section 2.4, point 27(a), **IP address and device location**: naturally, the AMLA is aware that most organisations do not hold information about their customers IP addresses or device locations. It is therefore incomprehensible that the AMLA should include this element in the draft.

If an organisation did hold such information – for example, a bank in the context of online banking – the question is what relevance this would have. Firstly, people can access the internet from all sorts of locations, such as their workplace, a café or restaurant, their neighbour s Wi-Fi connection, and so on. A particularly cunning criminal might use the IP address of a home user who isn t using a VPN, forcing that person to prove their innocence. Secondly, advertising companies such as Google and Meta have a keen interest in IP addresses and device locations so that they can illegally track and profile every citizen on the planet; citizens can only protect themselves against this by hiding their location and using a VPN. Citizens further need to protect themselves against criminals, hostile states and other unsavoury characters online; this is another reason why the use of a VPN, location masking and other protective measures are necessary.

In general IP address and device location are irrelevant, so there is no reason to include them in guidelines for all OEs.

Proposals of Privacy First

[20] Privacy First recommends not including any references to IP addresses or device location in the guidelines of the AMLA for all OEs. This data should only be included in guidelines for specific law enforcement agencies if it has been demonstrated that such data is relevant to the fight against crime by those OEs.

Section 2.4 - automated or semi-automated systems and processes, including the use of advanced analytical tools

[21] In point 28. of section 2.4, the AMLA imposes an **obligation on OEs to use automated or semi-automated systems and processes, including the use of advanced analytical tools**, unless this is not possible. As already explained in earlier comments, the AMLA is taking an incorrect starting point here, as these systems are unsuitable for all OEs, given that OEs cannot guarantee that the use of these systems will not result in violations of fundamental rights. Furthermore, it is undesirable for the AMLA to reverse the burden of proof for all OEs, in the sense that all OEs are expected to do what banks do (which banks themselves do not manage to do properly) and that, subsequently, those OEs who cannot prove that they have taken alternative measures to achieve the same results as banks are held to account. This is an inappropriate approach, which is not befitting of an independent European body such as the AMLA with significant responsibilities.

[22] In point 29. of section 2.4 **trigger events** are listed, that are just as inadequate as the events listed in point 27. This point, too, is based on what is expected of banks and is not feasible for all OEs, for example because they do not have access to the information sources referred to in points 29(c) and (d) (other than at disproportionately high cost). Trigger events must be limited to facts that indicate criminal activity.

Proposals of Privacy First

[21] Privacy First advises to completely delete point 28. from section 2.4 (and other general guidelines), given that automated risk profiling currently is prohibited.

[22] Privacy First recommends that point 29 be deleted and advises that the AMLA confine itself to providing an explanation of the relevant passages in the AMLR in which trigger events are discussed, whilst taking into account the capabilities of SMEs and the importance of providing customers with accurate information about the monitoring activities of OEs.

Section 2.5 - suspension and restriction measures

[23] In regard of section 2.5 on the use of **suspension or restriction measures**, it is important to pay attention to the following. In the Netherlands, there is a great deal of frustration amongst customers regarding the conduct of banks, which sometimes request all sorts of information that is not relevant to the fight against crime, whilst threatening customers at the slightest pretext with the blocking or closure of their bank accounts and the termination of their banking relationship. More information you find in previous comments, e.g. comment 4. The problems with OEs are not limited to banks. There have also been incidents

involving other OEs in which fundamental rights were violated. The risk posed by the AML Package and the actions of the AMLA is that the harm caused by the actions of OEs will increase.

It is not without reason that the Dutch Council of State (Raad van State) notes in a recent advisory opinion (https://www.raadvanstate.nl/adviezen/@158150/w06-26-00123-iii/#toonsamenvatting), machine translation: "*It is unlikely that the new regulations will automatically lead to better execution*" and *The Council emphasises that the government must, in particular, keep a close eye on the implementation of the risk-based approach, the prevention of discrimination and exclusion, and the protection of personal data, as these aspects have proved to be vulnerable in current practice*".

It is therefore of the utmost importance that OEs exercise due care when using their means of pressure, such as closing a bank account or suspending operations. The draft text for section 2.5 fails to address the customer s position, even though the AMLA may be aware of the Dutch experience. For instance, the text omits: [a] that the OE communicated with the customer in a careful and comprehensible manner; [b] that the OE has only requested information relevant to the fight against crime and that the OE has correctly explained to the customer why the requested information is required; [c] that the OE has given the customer sufficient time to respond; [d] that the OE contacts the customer by telephone if the response is not satisfactory; [e] that the member of staff dealing with the customer has adequate knowledge of the type of customer and the sector in which they operate; [d] that the customer is able to provide the requested information; [e] that there are adequate remedies for the customer who doesn t understand what the OE is doing.

Further we do not understand why the trigger events proposed by the AMLA are relevant for the assessment of the measures to be taken (point 30(a)), given that various trigger events are defined which are not related to crime. Trigger events must be limited to facts that indicate criminal activity.

Proposals of Privacy First

[23] Privacy First recommends that point 30 should make it clear that **the OE deals with the customer correctly** and should include, amongst other things, the following: [a] that the OE communicated with the customer in a careful and comprehensible manner; [b] that the OE has only requested information relevant to the fight against crime and that the OE has correctly explained to the customer why the requested information is required; [c] that the OE has given the customer sufficient time to respond; [d] that the OE contacts the customer by telephone if the response is not satisfactory; [e] that the member of staff dealing with the customer has adequate knowledge of the type of customer and the sector in which they operate; [d] that the customer is able to provide the requested information; [e] that there are adequate remedies for the customer who doesn t understand what the OE is doing.

Section 2.5 - termination and record keeping

[24] According to point 32 of section 2.5 **termination** should follow "*where the obliged entity is ultimately unable to comply with its obligations*". The penultimate sentence fails to mention that the customer is actually able to provide that information but refuses to do so.

[25] **Point 33** of section 2.5 of the draft on record keeping is not an element of Article 26 AMLR, the AMLA is not permitted to include any such provision in the draft, so it should be deleted.

Proposals of Privacy First

[24] In the penultimate sentence of point 32 of section 2.5 add: "*, that the customer is actually able to provide that information but refuses to do so*".

[25] Delete point 33. of section 2.5.

Section 2.6 general surveillance principles

[26] Privacy First notes that, in section 2.6 of the draft on the **general surveillance principles**, the AMLA sets out completely unrealistic expectations of the large group of OEs. Not even the banks can meet these expectations. It appears that the AMLA is imposing additional requirements that go even further than the excessive and unworkable requirements that the AMLR already imposes on OEs. Privacy First points out that the staff of OEs working in the field of AML/CFT are not all university professors, and that even university professors lack sufficiently broad knowledge. The AMLA should be aware that there is no evidence to suggest that the business-wide risk assessment (BWRA) contributes in any way to the fight against crime, certainly not when carried out by OEs that are SMEs. Like the rest of the draft, this section is written for banks (which are already struggling with this) under the illusion that other OEs are capable of doing so. Furthermore, the text appears to impose additional obligations compared with the text of the AMLR.

Examples of unrealistic and unexplained passages:

* "*as other already existing systems intended to detect unusual customer behaviour*", point 34(a) > what is meant by the AMLA and has this relevance for OEs that are SMEs?

* OEs are supposed to be able to do a "*structured, risk-based assessment of the customer s behaviour, and relevant events*", point 35(a) > this is completely unrealistic, and what is meant by 'behaviour'?

* OEs are supposed to have "*a holistic understanding of the customer s behaviour*" point 34(c) and even when an OE has limited access to information, the OE is supposed to ensure "*that transaction and activity monitoring remains a central component of their monitoring framework*" > the AMLA is undoubtedly aware that this is inhumane and impossible, so why does it include this in point 34(c)?

* OEs are supposed the identify '*expected behaviour*', point 34(d), though they mostly have limited knowledge of their customer (for example, because they provide digital services exclusively, or because their service has a very limited scope) > This is an unrealistic expectation that should be removed from the draft.

* It is unrealistic to expect all OEs to be aware of "*intermediaries, ownership or control structures, counterparties, assets or transaction patterns*" that are relevant to compliance with the sanctions rules, point 34(e).

* The government already lacks insight into the effectiveness of the AML/CFT system, so how can financial institutions be expected to assess whether their own systems are effective? (point 34(f)

Another new feature is that the AMLA reintroduces unusual transactions and behaviour into the draft, e.g. in point 34(d) and 35(e). In the AMLR being 'unusual' is not relevant. By using the word unusual in the text, the AMLA is adding to the AMLR rules, even though it has no authority to do so.

It is not sufficient for the AMLA to state in point 35 that there are OEs which are not in the same position as banks. It is highly unsatisfactory that all these other OEs are required to prove that they comply with their surveillance obligations in a different way to banks.

Proposals of Privacy First

[26] Delete points 34-35 and replace them by a realistic explanation of the obligations of Article 26 AMLR, without adding extra duties. Draft the text with OEs that are SMEs in mind, and refrain from including topics that are only relevant to large OEs with a specific information status in the guidelines, as the guidelines are intended to apply to all OEs.

Section 2.5 unusual transactions and behaviour, obligations to provide evidence, unnecessary provisions

[27] Whilst it is perfectly clear why most OEs have limited information about their customers and have limited possibilities to assess whether a customer is a criminal, OEs that do not do what banks are expected to do must provide evidence of their efforts to achieve the same result as banks, according to point 36. This is an incorrect approach on the part of

the AMLA, whilst it also imposes unnecessary obligations to provide evidence that are not prescribed by the AMLR.

[28] The additional obligations to provide evidence set out in point 37 will not only affect large OEs. It is therefore undesirable for this point to be worded in this way. The AMLA should confine itself to the obligations to provide evidence already set out in the AMLR and should provide a realistic and workable interpretation of them, in order to avoid unnecessary bureaucracy and costs.

[29] Points 39–41 follow directly from the AMLR and do not provide any further clarification; they are therefore superfluous and may be deleted.

Proposals of Privacy First

[27] Remove all additional requirements for evidence and documentation. Limit the text to an explanation of the meaning of the AMLR obligations and take OEs that are SMEs into account.

[28] Remove all additional requirements for evidence and documentation. Limit the text to an explanation of the meaning of the AMLR obligations and take OEs that are SMEs into account.

[29] Delete points 39-41.

Section 2.7 automated or semi-automated processes and controls

[30] As we explained in the introduction, automated systems are unsuitable for assessing the risk of individuals and organisations being involved in criminal activity. We are familiar with the appealing marketing claims made by the providers of this software; however, these are contradicted by independent investigations, such as those carried out by Amnesty International and the Dutch State Commission. The use of automated systems should therefore be limited to document management and other simple applications.

We note that users of such systems, such as banks, are unaware of the importance of robust safeguards. One example of this is the English-language publication by the Dutch Banking Association (Nederlandse Vereniging van Banken, 'NVB') on transaction monitoring, "*AI Machine learning in transaction monitoring*", https://www.nvb.nl/media/egyfld5c/ai-machine-learning-in-tm-1.pdf. It is clear from the text that the NVB believes it does not need to explain anything at all to its customers (individuals and organisations).

In the draft of the AMLA, we see no indication that the AMLA realises the enormous risks to fundamental rights associated with the automated systems referred to in section 2.7. Privacy First takes the view that it has not been proven that the current systems are suitable for assessing individuals and organisations for potential criminal activity; moreover, the safeguards against misuse are wholly inadequate. Examples of missing safeguards include the fact that there is no mention anywhere of the need for human intervention to be meaningful. Privacy First believes that, particularly in the fight against crime, a human being is simply incapable of assessing the outputs of automated systems when it comes to determining whether a person, an action or an event is criminal. There are examples everywhere of people who blindly believe the results produced by the computer, especially if they tie in with their own preconceptions. Another significant shortcoming of the AML/CFT system is the lack of independent scrutiny of the activities carried out by the various involved parties (government bodies, software providers, financial institutions and other stakeholders). This is because everything is subject to investigative secrecy. As a result, there is a lack of genuine debate.

Proposals of Privacy First

[30] Privacy First recommends that section 2.7 be completely rewritten to make it clear that the use of automated systems for the detection of crime in the context of AML/CFT is currently prohibited. The reasons are that their effectiveness has not been demonstrated and that the actors dealing with the systems and the systems are immature.

If that level of maturity were to be achieved in the future, there would be all sorts of requirements, such as robust safeguards, including:

1. a fully-fledged right to challenge and organised countervailing systems (including involvement of independent civil society organisations),

2. intensive monitoring of the systems and the parties (OEs and authorities) using them,

3. ongoing assessment of the parties creating and using such systems,

4. an independent body (such as an ombudsman) to which individuals and organisations can turn with reports and complaints, and which also has access to confidential information and has the power to intervene.

Sections 2.8-2.11

[31] Our previous comments also apply to sections 2.8-2.11. Once again, the text has been drafted with the banks in mind rather than the wider group of OEs. Once again, no account has been taken of the customers of OEs and the data subjects, and of small OEs, and unnecessary additional obligations have been imposed, even though the AMLA has no regulatory authority and the purpose of the guidelines is to clarify the AMLR.

[32] It is necessary for the guidelines to be reviewed periodically and for checks to be carried out to ensure that the AMLA acts appropriately in relation to these guidelines, given that the AMLA has a societal role in this regard that affects all OEs, their customers and data subjects.

Proposals of Privacy First

[31] Privacy First recommends that section 2.8 be completely rewritten, taking into consideration the previous comments.

[32] Privacy First recommends that the guidelines will be reviewed within three years and that the effectiveness and adequacy of AMLA s actions and the effectiveness of the of the guidelines is part of the review. The effectiveness should be assessed by an independent party such as the EU Court of Auditors.

Sections 2.6-2.11 - guideline 2 - transaction and activity monitoring framework

We have set out the shortcomings of Guideline 2 in detail in the comments on Question 2, to which we refer.

Proposals of Privacy First

In the amendments to question 2, we have put forward proposals to improve the draft, to which we refer. We recommend amending guideline 2 in a similar manner and omitting any incorrect passages.

Answer to the question on the use of automated or advanced analytical tools

We have set out the shortcomings of the use of automated or advanced analytical tools in detail in the previous comments, to which we refer. T**he use of automated systems for the detection of crime in the context of AML/CFT is prohibited** as the current landscape is immature and the effectiveness had not been proven.

If that level of maturity were to be achieved in the future, tools of this kind should only be made available to parties who have been assessed for their ability to use them in a responsible manner, and provided that **robust safeguards** are in place, including:
1. a fully-fledged right to challenge and organised countervailing systems involving independent civil society organisations (not those that engage in anti-crime marketing, such as Transparency International),
2. intensive monitoring of the AML/CFT systems and the parties using them (OEs and authorities),
3. ongoing assessment of the parties using such systems (OEs and authorities),
4. an independent body (such as an ombudsman) to which individuals and organisations can turn with reports and complaints, and which also has access to confidential information and has the power to intervene.

Proposals of Privacy First

In the amendments to questions 1 and 2, we have put forward proposals to improve the draft, to which we refer.

Privacy First recommends that the texts on the use of automated or advanced analytical tools be completely rewritten to make it clear that **the use of automated systems for the detection of crime in the context of AML/CFT is prohibited** as the current landscape is immature and the effectiveness had not been proven.

Final remark: the EU must not become a financial surveillance state

In its previous comments, Privacy First has already set out in detail that the draft-guidelines by AMLA contain a great many shortcomings and must be completely rewritten, firstly to ensure it is comprehensible to customers and OEs that are SMEs, and secondly to do justice to the safeguards required in a financial surveillance system such as that provided by the European AML/CFT rules, which means that automated systems for detecting criminals and crime are not an option due to a lack of maturity.

Privacy First calls on the AMLA to step out of its ivory tower and pay attention to the fundamental rights safeguards needed to counter the excesses that may arise from the AML/CFT rules, and which have already become apparent in the Netherlands as a testing ground.

We are prepared to discuss this with you and hope to involve other civil liberties organisations in the process.

The EU must not become a financial surveillance state in which citizens' fundamental rights are ignored!