Docnr8

From: 5.1.2.e 5.1.2.e | Privacy First <5.1.2.e @privacyfirst.nl>
Date: Monday, September 21, 2026, 6:58 PM
To: "postbus@eerstekamer.nl" <postbus@eerstekamer.nl>
Subject: Privacy First nam deel aan de AMLA-consultatie over het format voor het melden van criminaliteitsvermoedens

---

Attachments:

2026-09-19 AMLA feedback format reporting suspicions Privacy First.pdf

---

U ontvangt niet vaak e-mail van 5.1.2.e @privacyfirst.nl. Ontdek waarom dit belangrijk is

DIT BERICHT IS BESTEMD VOOR:

de leden van de Commissie Digitalisering (DIGI)
de leden van de Commissie Justitie en Veiligheid (J&V)
de leden van de Commissie Financiën (FIN)
de leden van de Commissie voor Europese Zaken (EUZA)

Geachte leden van de commissies,

De stichting Privacy First heeft op 19 september jl. deel genomen aan de consultatie van de Europese antiwitwasautoriteit, de *Anti-Money Laundering Authority* (AMLA), over het voorstel voor regels inzake het format voor het melden van vermoedens van criminaliteit ('het voorstel') op grond van de nieuwe antiwitwasverordening (AMLR) zoals hier aangekondigd. Dergelijke vermoedens moeten worden gemeld door aangewezen bedrijven ('obliged entities', 'OEs'), onder meer banken en boekhouders.

Graag verzoeken wij uw commissies aandacht te besteden aan onze consultatiereactie.

Waarom wij aan de consultatie mee doen
Privacy First heeft financiële privacy als één van de focusgebieden en is bezorgd over de risico's van de bestrijding van witwassen en terrorismefinanciering en de naleving van de sanctieregels ('AML/CFT') voor burgers en voor de algemene maatschappelijke veiligheid. Wij roepen de AMLA op om verantwoordelijkheid te nemen voor de risico's die AML/CFT oproept. Misdaad bestrijden is op zich goed maar mag niet tot schending van grondrechten of onaanvaardbare risico's voor burgers leiden.

Hierna volgt een verkorte weergave van ons commentaar.

Algemene opmerkingen
Privacy First heeft een aantal algemene opmerkingen gemaakt over het voorstel, onder meer dat daarin allerlei keuzes door de AMLA worden gemaakt die niet worden toegelicht of onderbouwd, zoals de groepering van OEs, de indeling in groepen OEs in verband met het leveren van datapunten, het al dan niet verplicht stellen van datapunten en de onderbouwing per datapunt voor de misdaadbestrijding. Daar komt nog bij dat er in de datapunten niet uitgewerkte elementen zitten, zoals de *suspicion indicators* (DP0016). Privacy First adviseert de AMLA de consultatie in te trekken en opnieuw te houden nadat alle informatie beschikbaar is via het consultatiedocument.
Voorts constateert Privacy First dat de AMLA in het voorstel nieuwe regels toevoegt, terwijl die regelgevende bevoegdheid ontbreekt bij de AMLA (dan wel indien van toepassing de Commissie). Privacy First adviseert het voorstel te screenen op nieuwe regels en deze te verwijderen.
Voorts missen wij vermelding van de raadpleging door de AMLA van de EDPS dan wel EDPB als bepaald in artikel 42 van verordening (EU) 2018/17.

Te veel datapunten inzake natuurlijke personen
In het voorstel heeft de AMLA opgenomen dat er een exorbitant aantal persoonsgegevens (datapunten inzake natuurlijke personen) moeten worden opgegeven bij melding van een vermoeden, zonder aan te geven om welke personen het gaat. Hier is een nadere toelichting en onderbouwing nodig omdat niet bij iedere persoon die genoemd wordt in de melding van een vermoeden sprake hoeft te zijn van verdenking van criminaliteit. Verder is bij veel datapunten niet duidelijk welke relevantie ze hebben voor bestrijding van criminaliteit. Het lijkt er eerder op dat de AMLA bezig is met het organiseren van statistieken, echter dat is niet het doel van een melding van vermoedens. Voorkomen moet worden dat er onnodig datapunten (= persoonsgegevens) worden verwerkt en verspreid. Privacy First adviseert dit onderdeel nader toe te lichten en te onderbouwen.

Ongewenst dat FIUs mogen beslissen over extra datapunten en over de duur van het risico van voormalige PEPs
Bij diverse datapunten wordt genoemd dat de nationale FIU mag bepalen of deze aan OEs in het land mogen worden gevraagd. Privacy First acht het ongewenst dat een FIU deze bevoegdheid krijgt, aangezien een FIU geen begrip heeft voor de positie waarin OEs en hun klanten verkeren. Wij nemen het standpunt in dat bij een melding van een vermoeden een beperkte set van persoonsgegevens en andere datapunten mogen worden verschaft aan de FIU en dat vervolgens de FIU nadere gegevens kan opvragen. Daarmee wordt gewaarborgd dat persoonsgegevens niet onnodig worden verwerkt en verspreid.
Voorts is ongewenst dat de FIU beslist hoe lang een voormalige politiek geëxponeerde persoon (PEP) dat nog blijft. Deze bevoegdheid hoort evenmin bij een FIU thuis.

Het zijn van PEP is geen 'adverse information'
Privacy First stelt vast dat de AMLA alle mensen die politiek geëxponeerde persoon (PEP), bijvoorbeeld leden van de Tweede Kamer, hun ouders en hun kinderen, in het verdachtenbankje plaatst, door de datapunten inzake PEPs in de rubriek '*adverse information*' te plaatsen. Zoals de AMLA kan weten zijn de meeste PEPs geen criminelen, een medewerker van de Nederlandse Vereniging van Banken (NVB) heeft ons dit ook bevestigd. Privacy First is van mening dat de plaatsing van alle PEPs door de Europese wetgever in de categorie van een hoog risico op criminaliteit, in strijd is met de grondrechten. Nu dit onderdeel van de AMLR nog niet ongeldig is verklaard, hebben we te maken met het fenomeen PEP, maar doet de AMLA er goed aan de PEP-datapunten op te nemen in de categorie gegevens inzake natuurlijke personen.

Misdaadtypen
Privacy First acht de classificering van het vermoedelijke misdaadtype in de datapunten DP0017 (*Possible Criminal offence type*) en DP0018 (*Possible predicate offence type*) inadequaat en onwetenschappelijk. Daar komt nog bij dat de indeling niet praktisch bruikbaar is voor OEs en criminaliteit bevat die niets met witwassen of terrorismefinanciering te maken heeft.
De AMLA lijkt te denken dat de Amerikaanse sancties (OFAC) ook voor de OEs gelden, terwijl het de AMLA bekend behoort te zijn dat de VS de sancties ook richt op niet-criminele burgers en organisaties. Het was reden voor Privacy First om de brief aan Tweede Kamer, over bescherming van Europese organisaties tegen buitenlandse sanctiedruk, mede te ondertekenen. Privacy First adviseert dit element te schrappen.
Hoogst vreemd is dat de AMLA 'religious sects' als vorm van criminaliteit opvoert. Wat dit betekent wordt niet toegelicht en waarom dit strafbaar is vermeld men niet. Privacy First adviseert dit element te schrappen.
Privacy First adviseert de AMLA de classificatie volledig te herzien en te vereenvoudigen.

Slotopmerking
Bijgaand gaat de tekst van onze reactie.
Mochten er naar aanleiding van onze consultatiereactie vragen of opmerkingen zijn, dan altijd contact met ons worden opgenomen.

Met vriendelijke groet,

5.1.2.e
Woordvoerder financiële privacy van Privacy First
PRIVACY FIRST
5.1.2.e @privacyfirst.nl

Contribution ID: 3cf5dacc-6324-46f3-8961-edee7b2c951f
Date: 19/09/2026 20:37:36

Feedback from Privacy First

Consultation on the draft ITS pursuant to Art. 69 (3) AMLR on the format to be used for the reporting of suspicions and for the provision of transaction records

General pages relating to this feedback have been removed

Compared to the current suspicion reporting process, what would be the expected level of monetary one-off investment costs for your institution (e.g. IT system changes, staff training, internal policy/procedure updates, etc.), based on the details provided in the draft ITS:

- ○ Nontangible one-off costs
- ○ Limited
- ○ Manageable
- ○ Disruptive (please provide further details and evidence)

In your view, how would the implementation of a new format for reporting suspicions affect your institution's ongoing (recurrent) suspicion reporting process costs (excluding one-off investments)?

- ○ Increase
- ○ Decrease
- ○ No impact

What are the main drivers of the expected change in costs?

- ☐ Changes in reporting format complexity
- ☐ Degree of harmonisation across jurisdictions
- ☐ IT system adaptation requirements
- ☐ Staff training and procedural changes
- ☐ Volume of required data fields
- ☐ Automation opportunities
- ☐ Other (please specify)

No answer to these questions

What would be the timeframe needed for you to adapt to the new framework?

- ○ Less than 1 year
- ○ 1 to 2 years
- ○ 2 to 3 years
- ○ More than 3 years

While the exact timeframe needed for technical implementation and full application of the ITS is not determined yet, it is envisaged to provide five years (three for FIUs and two for obliged entities integrating the reporting schemes into their internal systems, with a possible overlap). Is this timeframe:

No answer to this question

- ○ Adapted to the respective needs of FIUs and obliged entities
- ○ Too short (please provide explanation)
- ○ Too long (please provide explanation)

How would you rate the proposed approach, in particular Articles 3 and 4 of the draft ITS, regarding the necessary balance between harmonisation, quality and efficiency of reporting?

- ○ Fully agree
- ○ Agree to some extent (please provide explanation)
- ○ Disagree to some extent (please provide explanation)
- ◉ Fully disagree (please provide explanation)

* Explanation:

General | introduction
ABOUT PRIVACY FIRST: 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.
OUR COMMENTS: Privacy First would like to respond to the "Draft Implementing Technical Standards specifying the format to be used for the reporting of suspicions and for the provision of transaction records under Article 69(3) of Regulation (EU) 2024/1624" published by the AMLA on https://www.amla.europa.eu /policy/public-consultations/consultation-draft-its-format-reporting-suspicions-and-providing-transaction-records_en. The draft will hereinafter be referred to as 'the proposal'.
Our comments are provisional, and we reserve the right to raise objections regarding aspects not mentioned here as well.
We shall begin our comments with some general remarks on the proposal

General | Classification and Justification
Privacy First has many questions about the background to the proposal and is disappointed that the AMLA has limited itself in the proposal to a general introduction to the reporting obligations and does not address the specific choices it has made. Participants in the consultation are now forced to work their way through a confusing list of data points and speculate as to why the AMLA has chosen these classifications. It would be better if the AMLA were transparent about the choices made and provided justification for them, so that these can be assessed by those taking part in the consultation.

Some of our questions and comments:
[a] Why does the AMLA not provide an overview of the differences in data points between the groups of OEs and an explanation of how the OEs have been categorised?
[b] Why is there no overview of mandatory and non-mandatory data points, nor an explanation of the reasons behind the choices made?
[c] Why is there no justification, for each data point, regarding its relevance to the fight against crime?

Our general advice:

[d] Privacy First recommends withdrawing this consultation and launching a new one with complete information.

General | No new rules
Privacy First notes that the proposal introduces new, additional rules, even though the proposal is not intended for that purpose. This means that no new rules should be introduced.
[a] One example is the data quality guarantee set out in Article 9 ("When submitting to FIUs the data referred to in Articles 3 and 4 of this Regulation, obliged entities shall ensure that such data are complete and comply with the validation rules verifying their technical accuracy, data quality checks ensuring the consistency and completeness of the information reported, and plausibility checks put in place by FIUs."). Firstly, this text contains additional rules and, secondly, it is a text written for large organisations such as banks and is entirely unsuitable for small and medium-sized OEs. Privacy First advises to delete Article 9.
[b] Another example is the definition of 'reporting of suspicions' in Article 1 of the draft, which differs from that set out in Article 69 of the AMLR. Privacy First advises to delete this article.
[c] We recommend screening the draft for new rules and removing them all.

General | consultation of EDPS/EDPB
Privacy First notes that the present proposal may also have far-reaching consequences for citizens, as it contains binding rules with a significant impact on citizens' fundamental rights. Privacy First assumes that, in accordance with Article 42 of Regulation (EU) 2018/1725 (hereinafter 'EUDPR'), the EDPS and, where appropriate, the EDPB, shall be formally
consulted before the proposed ITS are adopted by the Commission.

Our comment: You would do well to confirm that you shall submit this draft to the EDPS or the EDPB.

>>> to be continued below >>>

Do you agree with the grouping of obliged entities for the purpose of different templates for the reports of suspicion and for the transaction records?

- ○ Yes
- ◉ No (please provide explanation)

* Explanation

>>> continues from previous question >>>

DP0101-0136 "Natural person" category
Privacy First is concerned about the exorbitant amount of personal data that, according to the form, must be provided to the FIU, without it being clear what relevance the data has to the fight against crime.

Our comments:
[a] It is unclear WHICH individuals are referred to in the list of data points concerning natural persons. Does this only concern individuals suspected of being involved in criminal activity (as suggested by DP0123 'Role of natural person')? The suspected person may well not be a person in respect of whom the OE records data under the AMLR. This aspect is not clarified by the AMLA.
[b] If the report were also to include non-suspect individuals: why would all those data points concerning those individuals need to be provided? This does not comply with the data minimisation requirement, which also applies under the AML/CFT regulations.
[c] Can it be explained, for each data point, why the personal information is relevant to the fight against crime? We do not see the relevance of e.g. DP0117 residency status), DP0122 gender, DP0124 employment status,

DP0125 occupation, DP0121 nationality.

DP0117, DP0122, DP0134, DP0135 FIUs determining data points
Various data points, including those mentioned here, state that the FIUs may determine that these data points are mandatory. Privacy First considers it undesirable for the FIUs to determine the general obligations of OEs to provide personal data when making a report. We believe that, when making a report, only a limited set of personal data concerning suspects should be provided, and that the FIU may subsequently request additional information. This prevents the unnecessary dissemination of personal data and ensures data minimisation. Privacy First recommends removing all powers for FIUs to establish data points, except in short-term emergency situations.

DP0405, DP0406, DP0407, DP0408 "Adverse information" category | PEPs
[a] The AMLA incorrectly classifies PEP data as 'adverse information', whilst it is common knowledge that PEPs do not pose a high risk (this has also been confirmed to Privacy First by a representative of the Dutch Banking Association, NVB). Privacy First advises the AMLA to remove the PEP category from the 'adverse information' category and transfer it to the "Natural person" category. (Incidentally, we believe that the AMLR's blanket classification of PEPs as posing a high risk of criminality is contrary to human rights.)
[b] The text states that FIUs would be permitted to determine for how long a former PEP continues to pose a crime risk ("It concerns the PEP status at the date of the suspected facts, but also, if known, for former PEPs (during a period of time to be specified by FIUs)"). Such a power does not belong with the FIUs, as they view everything through the lens of criminal investigation and lack a proper understanding of fundamental rights. Privacy First recommends removing all powers of FIUs relating to data points from the proposal (with the exception of powers in short-term emergency situations).

DP0016 suspicion indicators
Privacy First notes that the AMLA expects OEs to make use of unknown indicators:
"A detailed enumeration will be provided by FIUs based on supranational and national risk indicators, among which the guidelines pursuant to Article 69(5) AMLR. Further categorisation will be provided. The possibility to select "unknown" value will be provided."
Why is a consultation being held on the duty to report when the 'suspicion indicators' are not known and cannot be tested? It is of the utmost importance that these suspicion indicators are well-designed and have been tested against the practical experience of organisational entities. It must not be the case that the indicators cause people to be unnecessarily suspected, thereby potentially causing harm.
Privacy First considers it undesirable that suspicion indicators cannot be tested in this consultation.
Privacy First reiterates its recommendation that the consultation be withdrawn and that a new consultation be held once all relevant information is available, including the indicators of suspicion.

>>> to be continued below >>>

Does the ITS need further clarification on definitions, processes or legal aspects?

- (●) Yes (please provide explanation)
- ( ) No

* Explanation

>>> continues from previous question >>>

DP0017 Possible Criminal offence type
Privacy First does not understand the point of the OEs classifying the suspected criminal offence or act into two categories, DP0017 and DP0018, both of which contain incomprehensible and unscientific classifications.

It appears that the AMLA is attempting to force facts into highly dubious categories, as sub-categories of ML, TF and PF. There is no justification for this approach.
[a] Privacy First recommends merging DP0017 and DP0018 and simplifying them.
[b] Privacy First recommends removing the values 'Other (+ free text)' and 'Unknown', as there is no reason to report a suspicion if there is no fact that gives rise to a suspicion of ML, TF or PF.

DP0018 Possible predicate offence type
Privacy First notes that, in DP0018, the AMLA includes an incomprehensible and unscientific-looking list of 'predicate offences', without substantiating the purpose of this categorisation.
[a] The category 'Religious sects' is not substantiated. Is being a religious organisation a criminal offence? Who does this term cover – anyone who is not Christian? Is it a crime to be a Buddhist or Muslim? Privacy First recommends that this category be removed.
[b] Privacy First notes that the AMLA considers non-compliance with OFAC sanctions to be relevant, whilst the US uses OFAC sanctions as a political weapon to disadvantage legitimate individuals and organisations in the EU, such as officials of the International Criminal Court (ICC) at the Hague, the internet company A/I in Italy and the non-profit organisation HateAid (https://netzpolitik.org/2026/hateaid-nach-us-einreiseverbot-wir-sollten-nicht-fuerchten-muessen-vor-den-bus-geschubst-zu-werden/). Privacy First has signed the letter to the Dutch government, 'Letter to the House of Representatives: protect European organisations from foreign sanctions pressure' ('Brief aan de Tweede Kamer: bescherm Europese organisaties tegen buitenlandse sanctiedruk'), https://publicspaces.net/2026/09/17/brief-aan-de-tweede-kamer-bescherm-europese-organisaties-tegen-buitenlandse-sanctiedruk/. The EU must not legitimise violations of fundamental rights by countries outside the EU. Privacy First recommends removing the reference to OFAC.
[c] The list includes criminal offences that may have nothing to do with ML, TF or PF, such as murder. Privacy First recommends removing references to all such criminal offences.
[c] The classification of DP0018 is also unscientific and not evidence-based for other reasons. Privacy First recommends significantly simplifying the classification.

DP0411 Media information
Why is there no question here about the reliability of the allegations? It is common knowledge that both the mainstream media and social media contain inaccurate and unreliable information.
Our comment: Add a section on demonstrating the reliability of the source mentioned.

FINAL REMARK
This consultation is inadequately structured, which makes it very difficult to submit comments. Privacy First strongly advises you to make significant changes to the consultation system.

Several data points will be country-specific and not required by all FIUs, depending on their national legal frameworks.

How would you rate the addition of country-specific data points?

- ○ The country-specific data points are acceptable
- ○ The country-specific data points have no impact
- ◉ The country-specific data points pose challenges (please provide explanation)

* Explanation

It is undesirable for FIUs to make decisions on data points

AMLA developed templates adapted to various types of obliged entities (see Annexes I and II of the Draft ITS and Interpretative Note).

No comments on the questions that follow,

[1] "How would you rate the established list of data points for the various sector categories, as established in Annexes I and II, in terms of comprehensiveness and clarity?"
[2] Please comment on the individual data points of your selection.
Select the data point on which you would like to comment, then select which aspect of the data point you would like to comment (name, definition, treatment, attributes, etc.), and provide the content of your comment.
Note: you can submit comments on up to 20 questions in one questionnaire. Should you wish to comment on more than the indicated number, please submit another questionnaire again.

(pages not included)