To	The European Banking Authority
Date	6 June 2025, Amsterdam
Our reference	SPF20250606
Subject	Public consultation on four draft Regulatory Technical Standards (RTS) that will be part of the EBA's response to the European Commission's Call for Advice, announced on https://www.eba.europa.eu/publications-and-media/press-releases/eba-consults-new-rules-related-anti-money-laundering-and-countering-financing-terrorism-package and on https://www.eba.europa.eu/publications-and-media/events/consultation-proposed-rts-context-ebas-response-european-commissions-call-advice-new-amla-mandates

Dear Board of the European Banking Authority (EBA),

The Privacy First Foundation (hereinafter: Privacy First) welcomes the opportunity to comment on the consultation document on "*proposed RTS in the context of the EBA's response to the European Commission's Call for advice on new AMLA mandates*".

This response may be published on your website and on the website of the Anti-Money Laundering Authority (AMLA).

Our response focuses on the *Draft RTS under Article 28(1) of the AMLR on Customer Due Diligence* (paragraph 4.3) and the explanation on that paragraph in paragraph 5.3.

Our focus here is on respecting the fundamental rights of European citizens and on compliance with data protection rules in relation to the vast amounts of personal data collected by a very large number of private companies (obliged entities) for the purpose of combatting money laundering and terrorist financing (anti-money laundering, 'AML' and countering financing of terrorism, 'CFT'). Those obliged entities not only consist of large companies such as banks, but also include a large group of SMEs that hardly understand the AML/CFT rules.

Privacy First Foundation
Nieuwe Herengracht 49
1011 RN Amsterdam

https://privacyfirst.nl
info@privacyfirst.nl
+31 20 810 0279

KvK 34298157
ANBI accredited

PRIVACY FIRST

Contents

1. About Privacy First

Privacy First is a foundation (*stichting*) established under Dutch law that has financial privacy as one of its focus areas.[1] We have found that in recent years, citizens' financial privacy is slowly but surely being eroded and the risks of identity fraud, misuse of financial personal data and discrimination are increasing as a result of the violation of basic data protection principles. The European legislator has good intentions to tackle crime and combat criminal financial flows, but deploys methods that are disproportionate and that expose compliant citizens to unnecessary risks for their data, as well as their safety. This is an area where Privacy First has been very active.

For instance, we sent a letter to the Dutch Parliament drawing attention to the risks associated with European open finance plans[2], we commented on credit registration proposals by the Dutch government[3] and we warned that compliance with targeted financial sanctions should not lead to violation of civil rights.[4] In September 2024 we asked the Dutch central bank and the Ministry of Finance to adjust identification practices of financial institutions and in May 2025 we had a meeting with representatives of the central bank and the Ministry of Finance on the subject.[5]

The beneficial owner ('UBO') phenomenon and the registration of beneficial owners (UBO register) is a topic that Privacy First has been working on for a long time. An important issue is that we consider it undesirable that the general public should have access to UBO data. In 2020 we started the preparations of a lawsuit against the Dutch government regarding the Dutch UBO register. The summons was issued on 5 January 2021 and resulted in a court judgment of 18 March 2021[6] and a judgment in appeal of 16 November 2021.[7] The Dutch

[1] https://privacyfirst.nl/en/theme-2/financial/

[2] https://privacyfirst.nl/en/articles/privacy-first-advocates-restraint-in-dissemination-of-financial-personal-data/

[3] https://privacyfirst.nl/en/articles/credit-registration-in-netherlands-bkr-in-current-form-must-disappear/

[4] https://privacyfirst.nl/en/articles/compliance-with-financial-sanctions-must-not-lead-to-violation-of-civil-rights/

[5] https://privacyfirst.nl/en/articles/privacy-first-calls-for-adjustment-of-identification-practices-of-financial-institutions/

[6] https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2021:2457, article Privacy First: https://privacyfirst.nl/en/articles/court-doubt-on-ubo-register-is-justified/

[7] https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHDHA:2021:2176, article Privacy First: https://privacyfirst.nl/en/articles/court-ubos-can-request-foreclosure-themselves/

court ruled that there were no grounds for provisions by the court in anticipation of the CJEU ruling, which was handed down on 22 November 2022.[8] In 2023, we participated in a legislative consultation on the new UBO register regulations and called for measures to protect citizens from misuse of personal data in the register.[9] On 20 September 2024 Privacy First wrote a letter[10] to the financial committee of the Dutch Parliament raising concerns about the new *de facto* public UBO register, based on the new Anti-Money Laundering Directive, AMLD6.[11] In that letter, Privacy First advised members of the House of Representatives to raise questions about the public accessibility of the UBO register and the lack of safeguards. Privacy First recognises the importance of fighting crime, but believes that the measures being taken should not result in criminals and other persons with bad intentions having free and indiscriminate access to people's personal data held in central UBO registers. An example of abuse can be found in the report on Turkey's use of anti-money laundering rules to silence opponents in the EU, as reported by the Institute for Diplomacy and Economy (instituDE): *Weaponizing Financial Systems - Erdoğan's Transnational Repression to Muzzle Dissidents Abroad.*[12]

[8] Press release: https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-11/cp220188en.pdf ; article Privacy First: https://privacyfirst.nl/en/articles/eu-court-strikes-down-public-ubo-register/

[9] https://privacyfirst.nl/en/articles/critical-comments-privacy-first-on-consultation-ubo-register/

[10] Letter in Dutch: https://privacyfirst.nl/wp-content/uploads/UBO_PrivacyFirst_TK_20september2024.pdf

[11] Article Privacy First: https://privacyfirst.nl/en/articles/privacy-first-asks-second-chamber-not-to-approve-public-ubo-register/

[12] See https://www.institude.org/report/weaponizing-financial-systems-erdogans-transnational-repression-to-muzzle-dissidents-abroad and the report: https://institude.ams3.digitaloceanspaces.com/Weaponizing_Financial_Systems_Version_1.2.pdf

2. Our reasons for commenting on the EBA proposal

2a. Introduction

Privacy First has observed that the current rules to combat money laundering and terrorist financing have very unpleasant effects for non-criminal citizens, SMEs and nonprofit organisations. We are concerned that all the problems that already exist in the Netherlands and which have been recognised by the Dutch government will worsen under the new European rules known as the AML Package. Examples of the problems are the dangerous practices of obliged entities involving identification of natural persons, insufficient data protection measures by obliged entities and discrimination and exclusion practices by obliged entities. For this reason, we decided to participate in this consultation.
Participation in this consultation does not mean that we consider the AML Package to be a correct solution for countering crime with assistance of private parties, the obliged entities. We will not provide an assessment on the new European rules here.

In this consultation response, we urge European authorities to ensure that, when setting rules on the collection of personal data in the AML/CFT domain, they provide measures that mitigate data protection risks and reduce the risk of violating fundamental rights of citizens, SMEs and nonprofit organisations.

2b. The downsides of privatisation of crime fighting as revealed in the Netherlands

It has been clear for a very long time that the AML/CFT system leads to violation of fundamental rights of citizens and poses a data protection risk to people. In the letter of 14 May last[13], the Dutch Minister of Finance acknowledged that the fight against money laundering and terrorist financing has led to discrimination and exclusion on a large scale. Earlier, he also admitted the same in the House of Representatives Finance Committee debate on 22 January 2025.[14] Denial of the issue was no longer possible after the release of the report commissioned by KPMG[15] for the Ministry of Finance and the scathing verdict of

---

13 https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2025D21156&did=2025D21156

14 https://www.tweedekamer.nl/debat_en_vergadering/commissievergaderingen/details?id=2024A04456

15 https://www.rijksoverheid.nl/documenten/publicaties/2024/04/19/rapport-kmpg-en-i-o-research-naar-ervaren-discriminatie

the Netherlands Institute for Human Rights (College voor de Rechten van de Mens).[16] Dutch media previously paid extensive attention to discriminatory practices by financial institutions.

The banks already saw the storm brewing, which is why the Dutch banking association (Nederlandse Vereniging van Banken, NVB) published the message Greater commitment by banks to exclude discrimination' in March 2024.[17]

The Dutch Public Prosecution Service (Openbaar Ministerie, 'OM') announced on 9 April this year that they will sue Rabobank for alleged structural non-compliance with the bank's obligations to detect crime. In the area of discrimination in complying with AML/CFT obligations however, nothing is heard from the OM.

The problems caused by the AML/CFT system do not only affect people of foreign origin or of a different skin colour. Ordinary people and organisations also face inappropriate queries from obliged entities. From a January 2025 article[18] by the Dutch Home Owners Association (Vereniging Eigen Huis), it became clear that it is hardly possible for home owners' associations (verenigingen van eigenaars, VvE's) to get a bank account anymore, apparently because they are considered a high crime risk by banks. This is completely unjustified, as VvEs do not pose a high risk of crime.

Several other types of organisations, including many nonprofits, are experiencing major problems because of the AML/CFT rules and have asked the Dutch government many times to act and ensure that *bona fide* citizens and organisations are not harassed by

[16] Discrimination report 2024, announcement in https://www.mensenrechten.nl/actueel/nieuws/2025/01/29/discriminatiemonitor-2024-discriminatie-door-banken-in-beeld. Earlier the Institute reported on discrimination by ING Bank, https://www.mensenrechten.nl/actueel/nieuws/2024/07/25/ing-discrimineert-twee-klanten-door-betalingen-te-blokkeren-en-controleren-vanwege-niet-nederlands-klinkende-naam and by ASN Bank, https://www.mensenrechten.nl/actueel/nieuws/2024/09/02/asn-discrimineert-klant-door-geen-geld-over-te-maken-naar-palestina. The Institute also published an article on discrimination by financial institutions, https://www.mensenrechten.nl/actueel/toegelicht/toegelicht/2024/discriminatie-door-financiele-instellingen-veelvoorkomend-probleem-zonder-gerichte-maatregelen.

[17] https://www.nvb.nl/nieuws/grotere-inzet-banken-om-discriminatie-uit-te-sluiten/

[18] *Grote problemen bij bankrekeningen voor VvE's; soepeler toezicht noodzakelijk*, https://www.eigenhuis.nl/nieuws/grote-problemen-bij-bankrekeningen-vves

obliged entities.[19] The serious problems faced by people and organisations in the Netherlands and elsewhere in the EU are a consequence of the European AML-CFT system. Privacy First urges you, AMLA and the European Commission, through the implementing rules based on AMLR, to mitigate the problematic effects of the AML-CFT system and to counter new discriminatory practices. We will explain our calls below.

2c. Responsibility of the European financial legislator for data protection and respecting fundamental rights

Please note that with regard to the scope of data obliged entities are required to collect and retain for long periods, the basis lies in the new European AML-CFT rules. You and the AMLA/European Commission cannot refer to data protection authorities (national or European) for data protection aspects. The European AML/CFT rules, including the additional rules ('RTS') you are preparing, will have to ensure that citizens' fundamental rights are respected and that data protection safeguards are incorporated.

2d. European Accessibility Act

Also relevant in this context is the European Accessibility Act (EAA), which comes into force on 28 June 2025. This directive requires obliged entities to ensure that their services are accessible to every citizen. The Dutch EAA regulator, the Netherlands Authority for the Financial Markets (AFM), recently revealed[20] that a significant part of the Dutch population (5.5 million people, 32%) has disabilities and is insufficiently digitally literate (it cannot be expected that those digital skills will increase significantly through training and education). This group of people is at extra high risk of personal data misuse, which means they are also at extra risk if obliged entities demand personal data from them as part of an AML/CFT investigation. One of the most high-risk activities for this group is identity verification.

2e. Increasing cybersecurity risks related to financial services

On top of this, the Netherlands has for quite some time seen an increase in fraud around financial services, fraud for which financial institutions are not liable because the customer

[19] One example is the urgent letter that a large number of Dutch nonprofit organisations wrote to the Minister of Finance on 6 December 2021, reporting the serious problems these organisations have with banks and payment service providers, https://www.vrijwilligerswerk.nl/nieuws+en+blogs/2106433.aspx. The letter was signed by Vereniging NOV, CBF, CIO, FIN, Goede Doelen Nederland, HSC, Partin, Partos, SBF and WO=MEN. On 30 September 2022 a new letter was sent to the Minister of Finance, see https://www.vrijwilligerswerk.nl/nieuws+en+blogs/2313818.aspx and the letter https://www.vrijwilligerswerk.nl/PageByID.aspx?sectionID=172153&contentPageID=2313804.

[20] https://www.afm.nl/nl-nl/sector/actueel/2025/apr/sb-eaa-update%201

himself made the mistake. Cybersecurity risks will grow exponentially as a result of the rise of artificial intelligence and threaten the security of customers of obliged entities. Those customers make those mistakes because of their limited digital skills. Privacy First believes that the limited skills of a large part of the Dutch population (as mentioned in the EAA passage above) should be taken into account when designing the AML/CFT rules. Those rules should ensure that people do not fall into the trap of criminals when asked for KYC information.

3. The draft for additional rules ('RTS') based on AMLR

3a. General comment

Paragraph 4.3 of the consultation document contains a proposal for additional rules to be adopted by the European Commission based on Regulation (EU) 2024/1624, the Anti-Money Laundering Regulation (AMLR), referred to as regulatory technical standards" (RTS), although there is nothing technical" about the additional rules. Hereinafter the draft in paragraph 4.3 of the consultation document will be referred to as the draft RTS .

The AMLR has a high level of abstraction and makes almost no distinction between types of obliged entities and types of products and relationships. Although the EBA purports to specify AMLR with this proposal, Privacy First does not see this in the text. The explanation in paragraph 5.3 says that the proposal is kept abstract so that obliged entities have more freedom.

Privacy First believes that it is precisely the abstract nature of the AML/CFT rules that has led to the harmful effects of the AML/CFT-system described in paragraph 2b and calls on the EBA to use the draft RTS to limit ambiguities in the interpretation of the CDD rules of the AMLR and prevent the draft RTS itself from also using abstract concepts whose meaning is unclear.

Example:

> According to article 2(33) AMLR, basic information in relation to a legal entity includes "a list of legal representatives". What is a 'legal representative'? Is that the official director who is responsible for the entity (in Dutch: 'statutair bestuurder'), or is it anyone with a power of attorney, including a lawyer who is representing the entity in a procedure?

As mentioned above, we urge you to delve into the harms caused by the AML/CFT system, to consider ways to reduce the harmful effects of the AML/CFT system and come up with a new proposal for the draft RTS that mitigates those harmful effects.

Privacy First believes that Article 28(1) offers a lot of scope to ensure clarification of AMLR requirements and improve the protection of customers from incorrect requests by the obliged entities.

Below we will address some of your questions regarding the draft RTS.

3b. Q1 - Section 1: Information to be collected for identification and verification purposes

> Question 1
> Do you agree with the proposals as set out in Section 1 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

Privacy First: no, we do not agree

Articles 1-4
In our opinion Articles 1, 2, 3 and 4 of the draft RTS have no additional value as this already follows from Articles 22 and 62 AMLR. It is only useful if clarification takes place, for example by stating that diacritic characters should also be able to be processed (see example in a decision of the Belgian DPA in a case against ING Bank[21]), as well as long names.

Please note that we do not understand the relevance of registering nationalities for countering crime (but it is in the AMLR so a court case might be necessary to dispute this).

Article 5
Article 5(1)(g) of the draft RTS requires biometric data 'where available'. Privacy First does not understand why this is relevant, as there is already the requirement of Article 5(1)(d). We suggest to delete Article 5(1)(g), because of the risks to citizens associated with biometric data.

The following texts in the draft RTS have no additional value in relation to AMLR and can be deleted: Article 5(3), Article 5(4), Article 7. An article about 'Reliable and independent sources of information' is only useful if it is made clear what the meaning is of:

- "reliable and independent"
- "risk-sensitive measures to assess the credibility of the source"
- "the reputation, official status and independence of the information source"
- "whether the information or data provided had to undergo certain checks before being provided"
- "the ease with which the identity information or data provided can be forged"

Article 6
See our comments in paragraph 3c on Q2.

Article 9

[21] https://www.gegevensbeschermingsautoriteit.be/publications/arrest-van-9-oktober-2019-van-het-marktenhof.pdf

This article of the draft RTS contains undesirable provisions that do not take into account the fact that a large proportion of obliged entities are unregulated and there is *de facto* no data protection or integrity oversight of them. What matters for verification of the beneficial owner (UBO) is primarily ***why*** he is a UBO (his economic or controlling interest) and his basic personal information. In our opinion:

- Article 9(a) of the draft RTS should be deleted to prevent criminal abuse of personal data and other confidential data. (If an exception were to be made, it could only apply to selected obliged entities that are strictly supervised and should have limited access to the registers mentioned in Article 9(a)).
- In Article 9(b) "*third-party sources such as utility bills in name of the customer or the beneficial owner*" should be deleted as it has no relevance for verification of the UBO.

Article 12

Privacy First does not understand why people who are already registered as statutory directors in the trade register (senior managing officials, SMOs) are designated as UBO. In our opinion this is a wrong decision of the European legislator. Having this system in AMLR, it is important that these senior managing officials are protected against disproportional requirements regarding their personal data, when these personal data are not relevant for the obliged entity's duty to assess the risk connected to the customer. We recommend reflecting in Article 12(a) that only information is collected from the SMO that is relevant to the customer's risk assessment.

Other Articles

We have no opinion on Articles 8, 11 and 13-14.

3c. Q2 - Article 6. Verification of the customer in a non-face-to-face context

> Question 2
> Do you have any comments regarding Article 6 on the verification of the customer in a non face-to-face context? Do you think that the remote solutions, as described under Article 6 paragraphs 2-6 would provide the same level of protection against identity fraud as the electronic identification means described under Article 6 paragraph 1 (i.e. e-IDAS compliant solutions)? Do you think that the use of such remote solutions should be considered only temporary, until such time when e-IDAS-compliant solutions are made available? Please explain your reasoning.

Privacy First: yes, we have comments

Our primary comment: the draft RTS do not adequately reflect the eIDAS principle of non-mandatory use of the electronic identity.

For verification of a customer in a non-face-to-face context, Article 6(1) of the draft RTS requires that obliged entities use electronic identification means. According to Article 6(2)

only in cases where no electronic identification means are available or they cannot reasonably be expected to be provided, obliged entities shall acquire the customer s identity document (or equivalent) using other remote solutions, mentioning that any alternative solution shall be commensurate to the size, nature and complexity of the obliged entity s business and its exposure to ML/TF risks. The customer of the obliged entity is not mentioned at all.

Article 6 is not in line with the explicit principle laid down in Regulation (EU) No 910/2014 (the eIDAS Regulation) that the use of eIDAS compliant solutions shall be voluntary and that access to public and private services, and freedom to conduct business shall not in any way be restricted or made disadvantageous to natural or legal persons that do not use these solutions.

The non-mandatory character of eIDAS compliant solutions means that it is always the voluntary choice of the relevant natural or legal person to (not) use the digital identity. The decision whether to use or not use the electronic identity is free and can consequently not be made mandatory by imposing an obligation on public or private service providers to require electronic identification as a standard in non-face-to-face contexts. Imposing such an obligation would effectively render the use of electronic identification mandatory and make this principle of the eIDAS regulation illusory.

Privacy First advises that the current version of Article 6 is deleted from the draft RTS. Any approach that makes the use of digital identity dependent on public or private entities assessment or willingness to accept a digital identity, as supposed in Article 6(3) of the draft RTS, is not voluntary. A customer s decision to use or not use an electronic identity can only depend on the customer s own choice.

Also relevant in this context is the EAA (see paragraph 2d) and the large number of people in the EU who have limited digital skills. As financial institutions have evolved into digital enterprises without offices accessible to customers, major problems arise for all the people with limited digital skills.

Privacy First proposes that the EBA creates a new draft of Article 6 expressing:

- the use of an eIDAS solution and remote solutions shall only take place on a completely voluntary basis and if such a solution is used, it is the responsibility of the obliged entity to verify that the person that is going to use this solution understands the risks of the digital mode of operation;
- a physical alternative shall always be offered at a trusted party, with the customer being enabled to verify the reliability of that party and the reliability of the equipment used.

<u>The risks of remote solutions, described under Article 6 paragraphs 2-6 of the draft RTS are high</u>

Privacy First is of the opinion that the level of protection of remote solutions, described under Article 6 paragraphs 2-6 of the draft RTS is insufficient, as it is based on biometric

information of the customer that can easily be harvested by criminal parties and misused. Incidentally, it is not sure that eIDAS solutions are secure and there is a lot of criticism on the system.[22] Also playing a role here is that a significant proportion of the population has inadequate digital abilities and the EAA requires that this is taken into account.

3d. Q4 - Section 2: Purpose and intended nature of the business relationship or the occasional transactions

> Question 4
> Do you agree with the proposals as set out in Section 2 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

Privacy First does not agree with section 2 of the draft RTS, as it has no additional value since it does not add any value compared to AMLR and does not clarify for individuals, SMEs and nonprofit organisations facing requests by obliged entities and having to assess whether the obliged entity unnecessarily asks for information and documentary evidence. What the 'risk-sensitive measures' encompass is not explained. In the majority of cases the answer to Article 16(a) is clear. We do not understand why small customers will have the prophetic powers that are required for answering questions based on Article 15(b), Article 16(b) and Article 16(d).

It is a major invasion of privacy (with cybersecurity aspects) when an obliged entity asks for:

> *employment income, including salary, wages, bonusses and other compensation from employment, pension or retirement funds and government benefits including social benefits and grants, business revenue, savings, loans and investments income, inheritance and gifts, sales of assets and legal settlements.*

The same applies to the private information in Article 16(e) ("*information on their employment status whether employed, unemployed, self-employed or retired*").

---

[22] Read the article by the Verbraucherzentrale Bundesverband (vzbv), https://www.vzbv.de/pressemitteilungen/digitale-identitaet-verbraucherinnen-muessen-digitalen-brieftaschen-vertrauen and the position and report. Expert Jaap-Henk Hoepman published: *Feedback on the consultation on the eID implementing regulations*, https://blog.xot.nl/2024/09/05/feedback-on-the-consultation-on-the-eid-implementing-regulations/index.html. Dutch newspaper NRC published an interview with expert Denis Roio: *Europese digitale identiteit is straks niet veilig genoeg, waarschuwen experts*, https://www.nrc.nl/nieuws/2024/12/22/europese-digitale-identiteit-is-straks-niet-veilig-genoeg-waarschuwen-experts-a4877532.

For SMEs and nonprofit organisations it is relevant that the questions asked are appropriate and that obliged entities are not looking for personal data of the customer's clients, members, relations and other people involved, something currently happening often without good reasons.

Article 16 may cause obliged entities to start asking for all this information to cover themselves and fill the file. This is already happening under the current AML/CFT legislation and Article 16 may encourage these practices.

Privacy First therefore suggests to delete Article 16.

3e. Q5 - Section 3: Politically Exposed Persons

> Question 5
> Do you agree with the proposals as set out in Section 3 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

Privacy First does not agree with section 3, as it has no added value in respect of the AMLR. (We oppose the current concept of the PEP, as most PEPs are not high risk and it is contrary to European legal principles to consider in all cases family members and 'close associates' a high risk of crime or terrorist financing.)

3f. Q8 - Section 5: Enhanced Due Diligence measures

> Question 8
> Do you agree with the proposals as set out in Section 5 of the draft RTS? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

Privacy First does not agree with section 5 for several reasons. Firstly, it does not take into account the different types of high risk. For instance: most PEPs are not a high AML/CFT risk, though they are qualified (unjustly) as a group as high risk. There are many different types of high risk. In many cases it is disproportionate to demand what is stated in Article 24(b) and Article 24(c).

Article 24(d) is even worse, as in a situation that an obliged entity has reasonable grounds to suspect criminal activity of a (future) customer, this provision makes it possible to violate fundamental rights of people that have (when they are not criminals) the misfortune to be "*family members, persons known to be a close associate or any other close business partners or associates of the customer or the beneficial owner*". Apparently, the idea is that family and relations of a criminal are allowed to suffer an invasion of their privacy. Privacy First is of the opinion that it is against European legal principles to treat these people in this

way. The threshold for illegally entering into the lives of innocent people is unacceptably lowered by Article 24(d). It should be taken into account that legal protection against the action of obliged entities is not adequate, not in the Netherlands but probably not in the rest of the EU either. The same applies to Article 27(d).

The mandatory requirements of Article 25, Article 26 and Article 27 also go too far, as they do not take into account the nature of the high risk and all the facts and circumstances, where invasive requirements provide detailed requirements that are not placed into context, such as (Article 25(c)):

> *information on the customer's key customers, contracts and business partners or associates*

and all the examples in Article 26. Article 27 is invasive as well and in many situations inappropriate.

The entire section 5 should be deleted.

3g. Q11 - Section 8: Electronic identification means and relevant qualified trust services

> Question 11
> Do you agree with the proposals as set out in Section 8 of the draft RTS (and in Annex I linked to it)? If you do not agree, please explain your rationale and provide evidence of the impact this section would have, including the cost of compliance, if adopted as such?

Privacy First does not agree with section 8 of the draft RTS
We refer to paragraph 3c for the general comments on verification through electronic identification means. In Article 31(1) it should be made clear that the use of electronic identification means is voluntary and that it is the responsibility of the obliged entity to verify if the customer and the natural person understand the risks of this means of verification. Article 31(2) should be deleted as it undermines the idea of harmonisation and leads to unnecessary complications if this way of verification is chosen.

3h. Retention of information | request to add an article

Currently in the Netherlands, obliged entities, especially financial institutions, employ insecure practices in relation to verification of the identity. Privacy First in September 2024 has called on the Dutch central bank (De Nederlandsche Bank) and the Minister of Finance to improve identification practices of financial institutions, see the article '*Privacy First calls on De Nederlandsche Bank and finance minister to adjust identification practices of*

financial institutions'.[23] In May 2025 we had a meeting with representatives of De Nederlandsche Bank and the Ministry of Finance and we have explained that the risks attached to verification of the identity are the responsibility of the financial legislator, that apparently wants the supervisors (e.g. De Nederlandsche Bank) to check indefinitely[24] on the basis of copies of identity documents whether the obliged entity has fulfilled its verification obligation. This is against the fundamental principles of data protection, that require data minimisation.

We would like to draw the attention of the EBA, AMLA and the European Commission to this topic and suggest that the draft RTS will be complemented with an article on retention of information and copies of documents that reflect the data protection requirements.

Details of the risks and the mitigation possibilities you will find in the paper we sent to De Nederlandsche Bank and the Minister of Finance.[25] We suggest amongst others:

- no copies of identity documents to prevent misuse of these copies, only taking of notes of relevant information in the document;
- no retention of biometric data (selfies, videos, other photographs, fingerprints, etcetera) unless strictly necessary and if that is the case retention as short as possible to prevent misuse;
- retention of copies of other documents as short as possible, only taking notes of relevant information (as short as possible) which may be retained longer;
- no use of e-mail or regular post by obliged entities when they require KYC-information, for which a secure channel should always be offered.

[23] https://privacyfirst.nl/en/articles/privacy-first-calls-for-adjustment-of-identification-practices-of-financial-institutions/, original version in Dutch: https://privacyfirst.nl/artikelen/privacy-first-verzoekt-aanpassing-identificatiepraktijken-van-financiele-instellingen/

[24] Financial institutions have long relationships with their customers and only may delete the KYC information five years after the customer has ended the relationship with the obliged entity. As a consequence financial institutions collect a dangerous amount of personal data, with all the security risks attached.

[25] https://privacyfirst.nl/wp-content/uploads/Wwft_identificatie_verzoek_PrivacyFirst_sept2024.pdf

4. Final remark

For further information or any queries relating to the above, Privacy First can be reached at any time on telephone number +31-20-8100279 or by email: info@privacyfirst.nl.

Yours sincerely,
on behalf of Privacy First,

Vincent Böhre
director