

## **EDPB contribution to the EBA public consultation on draft regulatory technical standards on AML/CFT**

**Adopted on 8 July 2025**

## 1. BACKGROUND

1. On **12 March 2024**, the European Banking Authority (EBA) received a Call for Advice from the European Commission on certain draft regulatory technical standards (RTS) under the new EU framework on anti-money laundering/countering the financing of terrorism (AML/CFT). The EBA's response to this Call for Advice will inform the work of the new AML/CFT Authority (AMLA).
2. On **6 March 2025**, the EBA launched a Public Consultation<sup>1</sup> on four draft RTS that will be part of the EBA's response to the European Commission's Call for Advice:
  - The draft RTS under Directive 2024/1640 (hereafter, '**AMLD**') setting out the benchmarks and methodology for assessing and classifying the inherent and residual risk profile of obliged entities, as well as the frequency of its revision;
  - The draft RTS under Regulation 2024/1620 (hereafter, '**AMLAR**') specifying the assessment methodology of credit institutions, financial institutions and groups of credit and financial institutions for the purpose of selection for the direct supervision of the Authority for Anti-money laundering and Countering the Financing of Terrorism;
  - The draft RTS under Regulation 2024/1624 (hereafter, '**AMLR**') specifying information and requirements necessary for the performance of customer due diligence for the purposes of Article 28(1);
  - The draft RTS under the AMLD, specifying indicators to classify the level of gravity of breaches, criteria to be taken into account when setting the level of pecuniary sanctions or applying administrative measures and the methodology for the imposition of periodic penalty payments for the purposes of Article 53(10).
3. On **21 March 2025**, the EBA informed the EDPB about the initiation of the public consultation and of the opportunity for the EDPB to provide comments on the draft RTSs.

## 2. GENERAL COMMENTS

4. The EDPB notes that the draft RTS prepared by the EBA set out rules for the application of the AML/CFT framework, including on the types of personal data that obliged entities may collect in order to fulfil their obligations under AML/CFT.
5. At the same time, the EDPB is aware that the work of the EBA on these draft RTS should not pre-empt the decision of AMLA as to the draft RTS that it will ultimately develop and submit to the Commission for adoption<sup>2</sup>. In this regard, it should be recalled that, in accordance with Article 42(2) of Regulation (EU) 2018/1725 (hereafter 'EUDPR'), the EDPS and, as appropriate, the EDPB, can be formally consulted when such delegated acts will be adopted by the Commission. The following preliminary

---

<sup>1</sup> EBA, Consultation Paper on Proposed Regulatory Technical Standards in the context of the EBA's response to the European Commission's Call for advice on new AMLA mandates, EBA/CP/2025/04, 6 March 2025, available at: <https://www.eba.europa.eu/publications-and-media/press-releases/eba-consults-new-rules-related-anti-money-laundering-and-countering-financing-terrorism-package>.

<sup>2</sup> European Commission, Provisional request for advice to the European Banking Authority (EBA) regarding regulatory technical standards and guidelines under the future anti-money laundering/countering the financing of terrorism (AML/CFT) framework, 12 March 2024, available at: <https://www.eba.europa.eu/about-us/organisation-and-governance/accountability/calls-advice>.

comments to the EBA's public consultation are without prejudice to further informal or formal consultation of the EDPS or the EDPB and EDPS that may take place at a late stage pursuant to Article 42 EUDPR.

### 3. COMMENTS ON THE RTS SETTING OUT THE BENCHMARKS AND METHODOLOGY FOR ASSESSING AND CLASSIFYING THE INHERENT AND RESIDUAL RISK PROFILE OF OBLIGED ENTITIES, AS WELL AS THE FREQUENCY OF ITS REVISION UNDER THE AMLD

6. The EDPB notes that the risk profile assessed under this RTS does not concern the AML/CTF risk of the customers of the obliged entities but those of the obliged entities themselves<sup>3</sup>. However, 'obliged entities' may be natural persons<sup>4</sup> and therefore qualify as data subjects under the GDPR<sup>5</sup>. Therefore, the application of the RTS may entail processing of personal data within the meaning of Article 4(1) of the GDPR. In line with Recital 122 of AMLD, the EDPB recommends inserting in the RTS a reference to the applicability of the GDPR.
7. The EDPB highlights that the application of the RTS may impact the individuals concerned, in particular as a higher risk profile entails a higher frequency and intensity of on-site, off-site and thematic supervision by AML/CFT supervisors<sup>6</sup>. At the same time, the data points on which the risk profile of the obliged entity is calculated in most cases concern high-level statistical information (e.g. total value of outgoing transactions in the previous year, total number of customers using prepaid cards, number of e-money transactions in the previous year, the number of customers owning crypto-assets, etc.)<sup>7</sup>. Taking the broad range of data points that are listed under Annex 1 of the consultation paper into account, it is important to ensure that the data is processed only by the appropriate staff of the AML/CFT supervisors, is obtained from reliable sources, and that appropriate technical and organisational measures are implemented to guarantee the security of the data processed. Therefore, the EDPB recommends inserting a recital including these considerations in this RTS.

### 4. COMMENTS ON RTS SPECIFYING INFORMATION AND REQUIREMENTS NECESSARY FOR THE PERFORMANCE OF CUSTOMER DUE DILIGENCE UNDER ARTICLE 28(1) AMLR

8. The EDPB notes that this RTS involves the processing of various types of customer information, which may fall under the category of 'natural persons' as defined in Article 22(2) AMLR, thereby constituting processing of personal data within the meaning of the GDPR. Therefore, the EDPB recommends including a reference to the applicability of the GDPR in the RTS.

---

<sup>3</sup> See Article 40(1)(2) of Directive (EU) 2024/1640.

<sup>4</sup> See Article 2(4) of AMLD6 referring to the definition of 'obliged entities' under Article 3 of AMLR which include "natural or legal persons acting in the exercise of certain professional activities, namely auditors, external accountants, tax advisors, lawyers, notaries, estate agents, among others".

<sup>5</sup> It is the case of personal data related for instance to the management of the obliged entity. In this regard, see the recent judgment of the Court (first Chamber) of 3 April 2025, *L.H. v Ministerstvo zdravotníctví*, C-710/23, ECLI:EU:C:2025:231, paragraphs 30-31.

<sup>6</sup> Article 40(1)(c) AMLD6.

<sup>7</sup> See Annex 1, Section A, of the Annexes to the RTS.

9. The EDPB welcomes the specification in the RTS of the types of personal data to be processed for the performance of customer due diligence under AMLR. The EDPB recalls that, in accordance with the principle of data minimisation, only information that is strictly necessary for compliance with the AMLR can be processed. Therefore, the EDPB encourages the EBA to carefully assess the proportionality of each type of personal data where collection is mandatory under this RTS, and in particular to determine whether the collection of this personal data is strictly necessary to meet the obligations under the AMLR. In addition, the EDPB notes that several articles in the RTS do not provide an exhaustive list of information that obliged entities are required to obtain or verify but illustrates them in a non-exhaustive manner by using the term ‘at least’. The EDPB recommends deleting such reference to ‘at least’ in **Articles 1(1), 5, 18(1), 24, 25, 27 and 29** of the RTS in order to ensure the clarity and precision of the legal obligation to process personal data<sup>8</sup>.
10. This RTS does not set out security measures to be implemented by obliged entities when processing personal data under their obligation under Article 28(1) AMLR. Due to the nature of the information collected, and the risk of identity fraud in case of data breaches, the EDPB recommends recalling in a recital that obliged entities have to comply with the obligation to take appropriate technical and organisational measures under Article 32 GDPR to ensure an appropriate level of security and confidentiality. Notably, personal data should be pseudonymised as soon as it is no longer necessary to have directly identifiable personal data. The copies of identity documents should be stored with appropriate security measures. Where appropriate, identity documents should be marked as confidential and their access restricted. Whenever possible, only the essential data should be extracted and stored, rather than retaining a full photocopy of the entire document.
11. Furthermore, measures should be taken to ensure regular review of the accuracy of the customer information and that data that are found to be inaccurate are deleted or rectified without delay<sup>9</sup>. In this regard, the EDPB notes that **Article 22(2)** of the RTS sets out the conditions under which Article 33(1)(b) AMLR may apply. The EDPB recommends however to clarify in the RTS that for both lower and higher risk customers, obliged entities shall ensure that the information collected on the customer are kept up to date and rectified without delay.
12. Under **Article 1(1)** of the RTS, obliged entities are required to obtain ‘at least the names that feature on [customers’] identity documents, passports, or equivalent’. The EDPB understands that a document would be considered ‘equivalent’ if it fulfils the conditions set out under Article 5 of the RTS. The EDPB recommends clarifying the term ‘equivalent’, for instance by adding a cross-reference to Article 5 in Article 1(1) of the RTS.
13. Regarding **Article 3** of the RTS, which defines ‘place of birth’ as both the city and country of birth, the EDPB notes that the city of birth may not always be indicated on identity documents recognised as valid means of identification in certain Member States. The EDPB therefore recommends adopting a more flexible approach to the definition of ‘place of birth’, taking into account that the presence of

---

<sup>8</sup> See in this regard judgment of the Court (Grand Chamber) of 22 November 2022, *WM and Sovim SA v Luxembourg Business Registers*, Joined Cases C-37/20 and C-601/20, ECLI:EU:C:2022:912, paragraphs 80 and 81: “81. [...] it is apparent from the use of the expression ‘at least’ that those provisions allow for data to be made available to the public which are not sufficiently defined and identifiable. Consequently, the substantive rules governing interference with the rights guaranteed in Articles 7 and 8 of the Charter do not meet the requirement of clarity and precision recalled in paragraph 65 above (see, by analogy, Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 160).”

<sup>9</sup> In accordance with Article 5(1)(d) GDPR.

this information is one of the requirements for a document to be considered equivalent to an identity document or passport under Article 5(1) and (2) of the RTS.

14. With regard to **Article 4** of the RTS, the EDPB notes the broad wording used in this article concerning the collection of nationality-related information under Article 22(1)(a) AMLR, and recommends clarifying and specifying the conditions under which obliged entities can reasonably be expected to 'satisfy themselves that they know of any other nationalities their customers may hold'.
15. **Article 5(1)** of the RTS lists the conditions under which an identity document can be used for the purpose of verifying the identity of a person in accordance with Article 22(6)(a) and 22(7)(a) AMLR. Among the conditions for a document to be considered equivalent to an identity document or passport, Article 5(1)(g) of the RTS specifies that such a document should contain, where available, biometric data. The EDPB recommends clarifying that this provision does not imply an obligation for obliged entities to use technical means to read such biometric data in order to uniquely identify the customer, which is subject to specific rules under Article 9(1) GDPR.
16. In addition, the EDPB notes that the list of conditions in Article 5(1) of the RTS may exclude the use of alternative documents (such as driving licences) which are recognised as valid means of identification in certain Member States but may not contain all the information listed under Article 5(1) of the RTS. However, in situations where the customer is, for a 'legitimate reason', unable to provide a document containing all the information required under Article 5(1), **Article 5(2)** of the RTS allows identity verification using documents issued by a state or public authority that include only the customer's full name(s), place and date of birth, nationality, and facial image. Recital 7 of the RTS suggests that such 'legitimate reason' may apply in cases where the customer is an asylum seeker. However, it is not clear whether such exemption would extend to other cases in which customers are in a vulnerable position. The EDPB further notes that there may be additional reasons for not possessing documents containing all the information required under Article 5(1) of the RTS - such as the existence of alternative, less costly documents that are accepted as valid identification in certain Member States. The EDPB therefore recommends clarifying these aspects in the RTS.
17. For the verification of the customer in a face-to-face context, **Article 6(3)** of the RTS provides that in case of use of remote solutions under Article 6(2) of the RTS, obliged entities 'must obtain from the person to be identified their explicit consent' and record it. Nonetheless, the EDPB notes that consent in this case would not meet the condition of being 'free' considering that it is not optional for customers to provide such information to the obliged entity. Instead, the appropriate legal basis under Article 6(1) of the GDPR for obliged entities to process customers' personal data in the context of customer due diligence pursuant to Article 19 AMLR is the necessity to comply with a legal obligation under Article 6(1)(c) GDPR. Therefore, the EDPB recommends removing the reference to 'explicit consent' in this Article.
18. The EDPB recommends inserting in **Article 12** of the RTS the specification, currently mentioned only in recital 10 of the RTS, that the identification of senior management officials will only take place where the obliged entity has been unable to identify beneficial owners having exhausted all possible means of identification or where there are doubts that the persons identified are the beneficial owners.
19. **Articles 15 and 16** of the RTS refer to the information to be obtained by the obliged entity on the purpose and economic rationale of the occasional transaction or business relationship. Considering the open-ended nature of the information to be collected under this provision, the EDPB recommends clarifying that the information listed in the articles should not be collected in all instances but that, in accordance with the principle of data minimisation, processing of personal data by obliged entities should be limited to what is necessary for the purpose of complying with the relevant provisions of the

AMLR. This is to ensure that controls to be performed by the obliged entity are proportionate to the risk posed by the customers under scrutiny. This consideration also applies in relation to **Article 23** of the RTS.

20. **Article 17** of the RTS concerns the identification of politically exposed persons. In this regard, the EDPB recommends inserting a reference to the reliability of the sources of information (along the lines of Article 7 of the RTS). Moreover, the EDPB recommends inserting in Article 17(2) of the RTS that the obliged entity must inform customers about the elements mentioned in Article 76(5) of the AMLR, due to the potential impact of the decision-making on the persons concerned. This consideration also applies to the screening pursuant to **Article 29** of the RTS.
21. The EDPB recommends replacing the wording ‘internet research’ with ‘reliable publicly available websites’ in **Article 19(c)** of the RTS, taking the need to ensure that data is only obtained from accurate and reliable sources into account<sup>10</sup>. The EDPB also recommends assessing whether the same reason would justify further qualification or deletion of the reference to ‘sources using a combination of public and private records’ in **Article 9(b)** of the RTS.
22. In addition, the EDPB notes that **Article 24(d)** of the RTS provides that ‘in case the obliged entity has reasonable grounds to suspect criminal activity’ the additional information on the customer and the beneficial owners under Article 34(4)(a) AMLR shall enable this ‘obliged entity to obtain a more holistic view on ML/TF risks by obtaining information on family members, persons known to be a close association or any other close business partner or associates of the customer or the beneficial owner’. The EDPB would like to express serious concerns regarding the proportionality of such provision allowing the collection of third-party data, as this seems to go beyond the requirement under Article 34(4)(a) AMLR to simply obtain additional information on the customer and the beneficial owners.

## 5. COMMENTS ON THE RTS ON PECUNIARY SANCTIONS, ADMINISTRATIVE MEASURES AND PERIODIC PENALTY PAYMENTS

23. Having regard to this RTS, the EDPB considers that, for the same reasons express under the above paragraph 6, a reference to the GDPR and to the EUDPR should be added in a recital of the RTS considering that this RTS also foresees the processing of personal data by AMLA.

---

<sup>10</sup> See recital 5 of the RTS; see also EDPS Opinion 12/2021 on the anti-money laundering and countering the financing of terrorism (AML/CFT) package of legislative proposals, 22 September 2021, paragraph 45, referring to the duty for obliged entities to verify the accuracy and the reliability of the information collected.