bankenverband

Association of German Banks (BdB)

KYC Industry Standard (BdB)

1 September 2026

This document contains interpretations, developed by the expert groups of the Association of German Banks, regarding the Know Your Customer (KYC) requirements set forth in Regulation (EU) 2024/1624 (AMLR). Specifically, the explanations address questions of interpretation related to Articles 19-26 AMLR and related technical standards and guidelines.

It should be noted that the Level 2/3 legal acts referred to were still in the draft stage at the time this document was prepared. These interpretations therefore reflect the state of knowledge as of the date of preparation.

This document has been prepared in both German and English.

Lines	Issues and legal determination AMLR	Interpretation
1	**Preliminary remarks: principles of interpretation under EU law**	1. Existing national law and national methods of interpretation are not decisive for the interpretation of supranational EU law. This would be incompatible with the objective of harmonisation. Instead, EU law must be interpreted autonomously. Each term must be construed in accordance with its specific meaning under EU law; given the need for the uniform application of EU law, there is no reference to meanings derived from national legal systems. 2. The interpretation of a provision of EU law is determined not only by its wording, but above all by its context, systematic structure and the objectives or purpose pursued by the provision (teleological interpretation). The legislative history of an EU law provision may also provide relevant guidance for its interpretation, although the historical interpretation method generally plays a subordinate role. In addition, specific principles of EU law interpretation play an important role, such as comparative legal analysis and the principle of effet utile (the "useful effect" or practical effectiveness of an EU law provision), under which a provision should be interpreted in a manner that enables it to achieve its full effect. The recitals also serve as an important interpretative guideline, provided they do not conflict with the provisions of the legislation. 3. Generally, it can be observed that, when interpreting indeterminate legal concepts and legal terms requiring further specification, the CJEU gives preference to those methods of interpretation that most effectively promote the attainment of the objectives of the Treaties. These distinctive characteristics of EU law require a specific weighting of the various methods of interpretation, notably a greater emphasis on systematic and teleological interpretation, taking into account the principle of effet utile. This is especially important given that reliance on the wording of a provision is complicated by the existence of 24 equally valid versions of EU legislation in different languages. At the same time, a comparison of the different language versions of a text can provide valuable guidance for the interpretation of EU law.

		4. The FATF Recommendations may also serve as an additional aid to interpreting the AMLR. Recital 4 AMLR clarifies that *"...measures adopted by the Union in that field should therefore be compatible with, and at least as stringent as, actions undertaken at international level. Union action should continue to take particular account of the Financial Action Task Force (FATF) Recommendations and instruments of other international bodies active in the fight against money laundering and terrorist financing."*
2	**Existence of a "business relationship" – Article 2(1)(19) AMLR**	Article 2(1)(19) of the AMLR defines a business relationship as: "a business, professional or commercial relationship connected with the professional activities of an obliged entity, which is set up between an obliged entity and a customer, including in the absence of a written contract and which is expected to have, at the time when the contact is established, or which subsequently acquires, an element of repetition or duration;" This definition emphasises that the relationship must be **connected** to the obliged entity's professional activities and must be established **directly with the customer**. As a result, the scope of the concept is clarified and more narrowly defined than under previous legal frameworks, such as the German Anti-Money Laundering Act (Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten, GwG) and AMLD5. A business relationship also presupposes that the customer seeks and obtains a product or service from the obliged entity, meaning that **the obliged entity provides a product or service to the customer** (see also recital 56 AMLR, which states: "The process of establishing a business relationship or carrying out the steps necessary to conduct an occasional transaction is triggered when the customer expresses an interest in acquiring a product or receiving a service from an obliged entity.") Accordingly, the existence of a business relationship requires that the customer acquires a product or receives a service from the obliged entity. As a result, and for example, where a party acts solely as a **guarantor or provider of a guarantee/credit insurer, that requirement is not met**. The guarantor neither receives a service nor

		acquires a product from the obliged entity. In such circumstances, the measures laid down in the AMLR would not apply, however, the obliged entity may at its own discretion decide whether any **additional risk-mitigating measures** should be applied in relation to the guarantor or provider of the guarantee/credit insurer. From an effective AML/CFT risk management perspective, this could include, in particular, sanctions screening and adverse media screening of the guarantor or provider of the guarantee. Where the guarantee is called, the source of funds should be established. Similarly, **no business relationship** within the meaning of the AMLR exists where the parties merely enter into a **legally binding contract** and the subject matter of that contract is unrelated to the obliged entity's professional activities. This is the case, for example, where the obliged entity procures goods or services for its own purposes, such as office equipment, or where it seeks to manage its own assets (proprietary trading), such as in refinancing and hedging transactions conducted in the bank's own interest. The element of '**repetition**' also means that a business relationship may be established through repeated conduct or ongoing contacts. However, this repetition must be objectively discernible to the obliged entity.
3	**Scope of the trigger for customer due diligence measures under Article 19(1)(f) AMLR**	1. Article 19(1)(f) AMLR corresponds to the current Section 10(3)(4) GwG. Under this provision, the customer or the person purporting to act on behalf of the customer (see also Article 20(1)(i) AMLR) as the corresponding due diligence measure) must be re-identified where there are doubts as to the accuracy or adequacy of the information previously obtained. 2. The KYC trigger does not extend to persons within the customer's sphere who are authorised to represent the customer, such as employees. Rather, it concerns persons acting independently of the customer who purport to act on the customer's behalf as agents or representatives.

		3. It is sufficient to (**re-**)**identify the customer** pursuant to Article 20(1)(a) AMLR and/or the person purporting to act on behalf of the customer pursuant to Article 20(1)(i) AMLR. In this situation, it is **not necessary** to **carry out all customer due diligence measures** again, unless the re-identification process reveals new information, such as additional names. In that case, further customer due diligence measures may be required, including assessing whether the person is a politically exposed person (PEP) or conducting sanctions screening. The risk-based approach applies here. Where there are indications that the customer has sought to create an **inability to conduct customer due diligence within the meaning of Article 69(1) subparagraph 2 AMLR** in order to evade the application of customer due diligence measures, consideration should be given to reporting a suspicion and/or terminating the business relationship where the customer has also, at least, attempted to execute a suspicious transaction.
4	**Scope of the new customer due diligence measures relating to targeted financial sanctions pursuant to Article 20(1)(d) AMLR (also taking into account Articles 29 and 30 of the draft RTS under Article 28 AMLR)**	The introduction of Article 20(1)(d) AMLR is intended to align compliance with embargo regimes relating to targeted financial sanctions with customer due diligence measures relating to money laundering law. According to recital 34 AMLR, Council Guidelines on Implementation and Evaluation of Restrictive Measures and EU Best Practices for the Effective Implementation of Restrictive Measures must be taken into account when assessing whether a customer that is a legal entity is owned or controlled by a sanctioned person. A consistent approach is thus intended here. The EU Best Practices adopt a corporate ownership approach when determining whether a shareholder is relevant for sanctions purposes, as set out in paragraph 63. This is also reflected in Article 20(1)(d) AMLR, which refers to a majority interest or ownership of more than 50% of the proprietary rights. Accordingly, the assessment does not require simply multiplying ownership interests; rather, the relevant question is whether a person subject to targeted financial sanctions, individually or jointly with others, holds or controls more than 50% of the ownership interests in the entity. This is also reflected in Article 29 of the draft RTS under Article 28(1) AMLR.

		For the purpose of determining whether multiple sanctioned shareholders collectively hold more than 50% of the ownership interests or exercise control, the assessment should, in principle, be based on the persons and entities identified pursuant to the AMLR's customer due diligence requirements. In accordance with Article 52 AMLR, the assessment will generally be limited, across all levels of ownership, to persons or entities holding or controlling at least 25%, given that the power to reduce the relevant threshold to 15% has not been exercised to date. By way of exception, a risk-based approach may require an ownership chart to be obtained in the case of complex structures. This may result in more detailed information becoming available, which may need to be taken into account where relevant. Paragraph 63, second subparagraph of the EU Best Practices also assumes that only significant shareholdings are relevant for the aggregation of interests held by sanctioned shareholders (citing holdings of 25% and 30% as examples). Paragraph 40 of the EU Best Practices generally bases the sanctions assessment – including the assessment of whether control exists – on the information collected under the applicable KYC requirements, unless the relevant financial sanctions regime contains an express provision requiring a more detailed or different approach. Similarly, Article 30(a) of the draft RTS under Article 28(1) AMLR requires screening against sanctions lists only in respect to persons who meet the ownership or control threshold referred to in Article 20(1)(d) AMLR.
5	**Identification of natural persons on whose behalf or for whose benefit a transaction or activity is conducted – Article 20(1)(h) AMLR**	Article 20(1)(h) AMLR requires banks to identify and verify the identity of natural persons where a transaction or activity is conducted on their behalf or for their benefit. This requirement is particularly relevant in opaque or higher-risk trust and similar fiduciary arrangements where it is unclear who is ultimately behind the customer, or where there are indications of concealment, an unusual source of wealth or funds, or elevated ML/TF risks. The scope of this requirement must always be determined in accordance with the risk-based approach. The obligation to identify and verify the identity of the natural persons on whose behalf, or for whose benefit, a transaction or activity is conducted will generally not apply where the immediate customer is itself an obliged entity under the AMLR or

		equivalent anti-money laundering legislation (e.g. banks, payment service providers or insurance undertakings). In such cases, the customer is itself subject to statutory KYC requirements. To avoid duplicate checks, the application of simplified due diligence measures may therefore be appropriate, provided that the institution's risk assessment indicates a low level of risk. Accordingly, identification of the end customers or of the natural persons on whose behalf, or for whose benefit, a transaction or activity is conducted is generally not required in the event that the purpose of the arrangement, the business model and the source of funds are transparent and no higher ML/TF risk is identified. Similarly, Article 20(1)(h) AMLR will generally not apply, or will apply only to a limited extent, in the context of clearly defined and structurally low-risk arrangements where the underlying economic rationale is transparent and the use of funds is readily traceable. In particular, these include: • WEG (homeowners' association) accounts, tenancy deposit accounts and comparably administrated client funds; • school class funds, small association accounts and resident or care accounts with a narrowly defined purpose; • debt collection service providers that collect funds from large numbers of end users through standardised processes; and • other accounts with low transaction amounts, a high degree of transparency and a clearly defined purpose. In such cases, the individual end customers or underlying beneficiaries do not typically give rise to a separate ML/TF risk. Rather, the bank should understand the customer's business model, be aware of the purpose of the account and ensure risk-based monitoring. In these circumstances, identifying all natural persons involved would not be proportionate. **Rationale** Problem/situation: Under the previous regime, situations involving persons acting on behalf of another were addressed in Section 3(2) to (4) GwG. In such cases, the person on whose behalf the transaction was conducted was the beneficial owner. By contrast, a person who

		merely benefited indirectly from the transaction did not fall within the concept of a person acting on behalf of another. This is consistent with the wording used both in the FATF Recommendations and in the previous AMLD, which refers to persons acting "on behalf of" another person. Article 20 AMLR expands the wording by adding the phrase "or for the benefit of". This indicates therefore that the provision extends beyond persons acting on behalf of another and may also encompass beneficiaries. There is a risk in this case of an overly broad interpretation amounting to an obligation to Know Your Customer's Customer (KYCC), particularly in the context of fiduciary account structures. This risk can, however, be mitigated in structures where the contracting party is itself an obliged entity (in particular notarial escrow accounts) by clarifying that only the immediate contracting party must be identified, and not the non-customer natural persons on whose behalf or for whose benefit a transaction or activity is conducted. This is consistent with the existing principle that reliance may be placed on customer due diligence carried out by another obliged entity - see Recital 51 AMLR, which states: *"Obliged entities should also understand on whose behalf or for the benefit of whom a transaction is carried out, for example in situations where credit institutions or financial institutions provide accounts to legal professionals for the purposes of receiving or holding their client's funds as defined in Article 4, point (25), of Directive (EU) 2015/2366. In the context of customer due diligence, the person for the benefit of whom a transaction or activity is carried out does not refer to the recipient or beneficiary of a transaction carried out by the obliged entity for their customer."* The recital above shows that it was clear, once the term "beneficiary" was added, that this rule could lead to excessive verification obligations – if the rule is interpreted purely based on wording, for example, not only the trustor of an omnibus account would be subject to a verification obligation, any payees would also fall under this obligation. Currently, in Germany, once the holder of an omnibus escrow account has been identified, lower due diligence requirements are permitted pursuant to 7.2.1 of the special notes for credit institutions in Bafin's interpretation and application guidelines (AuA BT KI). Therefore, credit institutions may apply simplified due diligence for

		omnibus escrow accounts belonging to specific low-risk groups (e.g. accounts for class kitties, bowling clubs, nursing home residents). Determination of the beneficial owner is considered complete once there is a guarantee that the trustee will provide a list of current beneficial owners at the request of the institution. The AMLR itself lists a risk-based approach as material to ensure that the requirements remain practical, provided that this approach does not put the objectives of the regulation at risk, Recital 52 AMLR. In light of this, it is both expedient and necessary to exempt banks from identification obligations for common trustor/beneficiary configurations that they can categorise as standard. The teleological interpretation in particular, which is distinctly relevant under EU law and its emphasis on the principle of effet utile, supports this viewpoint. The AMLR focuses on guaranteeing high, harmonised standards for money laundering prevention across the Union, while also using a risk-based approach to apply these standards. To the extent that these objectives must be weighed against one another, it is important to take into account that the regulators themselves have understood that the obligation to verify beneficiaries is to be interpreted restrictively, and that the FATF recommendations, which represent, for the regulator, the scope on which the requirements are to be based, do not foresee verification of beneficiaries. If, therefore, as stated, the obligation to verify the beneficiary must be weighed against the application of a risk-based approach, then the risk-based approach will take priority in cases that are low-risk. In particular in the context of escrow accounts, it is permissible, when using a risk-based approach, to assume a low risk for some specific configurations. Another argument in favour of this is Recital 18 of the draft RTS under Article 28(1) AMLR, which exempts payment institutions and electronic money institutions from applying Article 20, arguing that end customers should not be classed as beneficiaries. In this respect, it must also be taken into account that AMLR envisages that the standards will be based on the FATF recommendations. The recommendations require, for the assumption that an initiator is subject to KYC due diligence, that the criterium “on behalf of” is met – “for the benefit of” does not meet the criteria. The AMLR thus

		goes beyond the FATF recommendations in this respect. In our opinion, there is no basis in European law, i.e. when implementing the principle of effet utile, for creating requirements that go above and beyond those in the FATF. Instead, the goal of the regulation is to ensure that due diligence requirements are applied in a risk-based manner, as can be determined from the recitals listed above and the EBA response to the EC Call for Advice (EBA/REP/2025/35), Page 5.
6	**Definition of the person purporting to act - PPA, pursuant to Article 20(1)(i)**	1. The PPA may be a legal or natural person. 2. The AMLR does not necessarily require that an acting natural person be identified. 3. Identification as a PPA is required if they are outside the customer's sphere of influence. The role of the PPA is limited to **natural or legal persons** that are **outside the customer's sphere of influence** and are engaging independently with the obliged entities based on **power of attorney, a mandate or a similar representative relationship.** The decisive factor is that this is a legally independent entity acting outside of the organisational sphere of influence or responsibilities of the customer. **Natural persons** may include, for example, a guardian, a legally appointed caregiver or an insolvency administrator. **Legal persons** may include, for example, an attorney's office, a consultancy, an auditing association or an arranger. Identification of a legal person as a "person purporting to act" is adequate in this case. Additional identification of the natural persons acting on behalf of these legal persons (e.g. an employee or official representative) is not required. **The following is a non-exclusive list of entities that cannot be considered persons purporting to act on behalf of the customer:** • Customer's employees (e.g. executives holding a general power of attorney or directors) • Employees with power of attorney as part of their usual duties and

		• Messengers Identification of the person purporting to act in the name of the customer is to take place by gathering the information listed in Article 22(1)(a) to (d) AMLR. In addition, the obliged entities must verify whether these persons do in fact have the right to represent the customer, e.g. whether they have a valid power of attorney or commission, Article 20(1)(i) AMLR. **Rationale:** The obligation to verify whether a person has a right to represent the customer arises from Article 20(1)(i), Article 22(1) AMLR. To begin, this includes natural and legal persons. It matches the wording and the systematic structure of the regulation, in particular that of Article 22(1) AMLR. This article refers, when referencing identifying the PPA, to a "person", but in the following clause, when referencing identifying the beneficial owner, refers to a "natural person". The term "person" includes, in the AMLR, both natural and legal persons; at various points, the term "legal person" is used (although this is alternated with "legal arrangement"). However, even if the following clause refers to "natural persons", then from a systematic viewpoint "person" must include legal persons. Therefore, the PPA can be a legal or a natural person. However, only those natural or legal persons that are not in the customer's sphere of influence must be identified (if the customer is a legal person, then this does not include, for example, the management or employees). Further identification of the representative (management/employees) of the PPA - if the PPA is a legal person - is not included in the systematic structure. Legal persons can necessarily only actually act via natural persons as their official representative. If we were to assume that the specific representative, a natural person, had to be identified, then the reference to an obligation to identify a natural or legal person as

		the PPA in Article 22 AMLR would be in systematic contradiction to the reference to identification of the beneficial owner, a natural person, in the following clause. No other interpretation can be found within the autonomous interpretation principles of European Law, in particular effet utile, according to which the objectives of the regulation in question must be implemented as effectively as possible. The recitals in the Regulation do not stipulate that natural persons must always be identified. As the recitals stipulate that European standards should not fall behind international standards (recital 4), any other interpretation could only be justified in the event that the FATF recommendations always required identification of a natural person. But this is not the case; the FATF recommendations do not, either in the relevant recommendation 10 or in the notes, stipulate a specific obligation to identify natural persons. Footnote 35 (page 66) stipulates, as an example, in regard to trusts or other arrangements, that the relevant natural or legal person is to be identified as the trustee. This approach is also fundamentally compatible with the FATF standards. The FATF always applies a risk-based approach. In terms of external actors (such as consultants, agents or attorneys) it is not as clear whether the actor must be connected to the legal subject. For those acting internally on behalf of a legal person, the fact that they are doing so is typically obvious, based on characteristics such as internal e-mail addresses or telephone numbers. Unlike external actors, there is no economic separation from the authorised entity, which could increase the risk, as is clearly the rationale used to require verification of the beneficial owner. If a legal person acts through their official representative, this does not increase the underlying risk of money laundering. Verifying whether or not a natural person acting for a PPA is actually authorised to act on behalf of the legal person serves as a protective measure for legal and business transactions and is part of the due diligence of any sound businessperson but does not play a role in preventing money laundering.
7	**Obligation to terminate the business relationship when unable to update customer information, Article 21**	Pursuant to Article 21, there is – if applied literally – an obligation to terminate the business relationship in the event that the obliged entity cannot comply with ongoing monitoring pursuant to Article 20(1)(f).

		However, against the background of the overarching risk-based approach, it is appropriate to apply a proportionate approach and not to impose an absolute obligation to terminate the business relationship where regular review of a client file cannot be completed following the legal minimum requirements. This is reflected in Section 2.5 of the AMLA Draft Guidelines on ongoing monitoring of a business relationship under Art. 26(5) AMLR of 3 June 2026, expressly providing for a graduated approach, whereby suspension or restriction measures may be used as interim steps before the business relationship is ultimately terminated. Against the background of proportionality, a temporary delay of customer update not caused by the customer should not justify immediate termination of the business relationship.
8	**Identification and verification of the identity of customers and beneficial owners, Article 22**	**Basic process:** Article 22 AMLR specifies that the identification obligations pursuant to Article 20(1)(a), (b), (h) and (i) AMLR are part of general due diligence. The AMLR does not contain a definition of the term identification. However, based on the wording of Article 20(1)(a), (b), (h) and (i) AMLR, and the systematic structure of Article 22 AMLR, it can be inferred that the current two-part understanding of the term "Identify" in Section 1(3) GwG also applies under the AMLR. Identification will continue to consist of two elements, that is (1) Determining identity by collecting information (step 1) and (2) Verifying data points material to identification (step 2) by providing specific documentary evidence. This two-part process is in line with FATF Recommendation 10. The scope of the measures to be taken can be determined based on risk (see recital 52 AMLR, which explicitly allows obliged entities to apply due diligence to customers based on risks and only requires "evidence-based decision-making"). This particularly applies to measures for verifying the information collected in order to carry out identification. That means it is not strictly necessary to verify with a document every piece of identification data for a person/role provided that the obliged entity has no doubt as to the identification of the person or role that requires identification. Once there is no doubt as to identity, the objective of the identification requirement has been achieved.

		Transparency has been created in order to prevent participation in anonymous or untransparent business relationships or occasional transactions and the associated ML/TF risks have been understood (see also FATF interpretive note to recommendation 10). The assumption that there is an obligation to verify with documentation all data collected as part of the identification process would be an excessive obligation on and burden to the obliged entity, which would directly contradict the principles of proportionality and effet utile. This limited interpretation of the obligation to verify a person's identity is also supported by statements made by the EBA in their answer to the Call for Advice from the European Commission on six RTS mandates (EBA/REP/2025/35 from 30 October 2025). The EBA clarifies at various points in response to questions from the consultation that a declaration from the customer is sufficient for fulfilling this obligation. AMLA has not taken a contrary view. The obliged entity does not have to obtain any special documents in order to verify customer information (see, for example, EBA/REP/2025/35 from 30 October 2025, page 136 in regard to a company's commercial name or additional nationalities of a natural person). Data such as the national identification number (if assigned) or tax identification number, which must be collected as part of the identification process, do not have to be verified by obliged entities via viewing of special documentation.
9	**Identification data for natural persons pursuant to Article 22(1)(a)**	1. The identification data prescribed in Article 22(1)(a) AMLR apply equally to a natural person in the role of a • customer (e.g. private customers, but also self-employed persons (*Freiberufler*), small business operators (*Kleingewerbetreibende*) or sole traders (**note:** for sole traders, the register number and legal form information e.K. *(Einzelkaufmann,* sole trader) should be collected as part of identification)*).* • Initiator (=natural person on behalf of or for the benefit of whom a transaction or activity is being conducted), see Article 20(1)(h) AMLR or • a person purporting to act in the name of the customer, see Article 20(1)(i) AMLR. 2. The identification data listed in Article 22(1)(a) AMLR is only mandatory for business relationships or occasional transactions that the obliged entity has classified as having

		a high or medium ML/TF risk. In low-risk cases and when applying simplified due diligence, the obliged entity fulfils their identification obligation for natural persons independent of their role by collecting the identification data required by Article 20 of the final draft RTS under Article 28 AMLR. 3. Specification of identification data a) **All initial and surnames:** The obligation to collect all names and surnames is sufficiently fulfilled if the obliged entity collects all names and surnames that feature on the identity document, passport or equivalent (see also Article 2(1) draft RTS under Article 28 AMLR). b) **Place of birth and full date of birth:** Pursuant to the draft RTS under Article 28 AMLR, the obliged entity must collect at least the country name for the place of birth of a natural person to be identified. The country of birth must therefore be included in the obliged entity's KYC systems as a mandatory field. Article 4 draft RTS under Article 28 AMLR also requires collection of additional information on place of birth should the identity document, passport or equivalent of the customer provide such information. In practice, this means that for German citizens identified using their German ID card, the city of birth must also be collected. Obliged entities must therefore include a second optional field in the KYC systems for the place of birth and provide clarification in internal instructions as to when this additional field for place of birth is relevant and must be filled out. The date of birth must be noted in the KYC system in the format DD.MM.YYYY. c) **Nationalities:** The obligation to collect information on additional nationalities is sufficiently fulfilled if the obliged entity requests information on possible additional nationalities from the natural person to be identified and sufficiently documents the answer (e.g. as part of a form to be filled out by the customer or a mandatory answer box in an online application form). Additional investigative or verification obligations, in particular in regard to the customer's answer, are not required of the obliged entity (see Article 5 draft RTS under Article 28 AMLR and EBA/REP/2025/35 from 30 October 2025, page 136). Provided that the obliged entity can determine that a person to be identified has one or more nationalities, this person cannot be stateless. There is then no need to ask if

		the person has a status as a refugee or subsidiary protection status. This is clear from the wording in Article 22(1)(a)(iii) AMLR (*"nationalities, or statelessness"*). • A natural person is stateless if they are not recognised as a citizen by any state of the world and therefore do not have any citizenship. A stateless person in Germany generally has a residence permit pursuant to Section 4(1) AufenthG (*Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet*, German Act on the Residence, Economic Activity and Integration of Foreigners in the Federal Territory). • The refugee status of a person in Germany is determined based on provisions in Section 3 AsylG (*Asylgesetz*, German Asylum Act). Criteria in Section 4 AsylG are material when determining status as a person with subsidiary protection status. A natural person's status as a refugee pursuant to Section 3 AsylG or subsidiary protection status pursuant to Section 4 AsylG is noted on the residence permit issued by the relevant immigration authority (see also Section 25(2) AufenthG). d) **Usual place of residence:** The usual place of residence refers to the address of the natural person (as registered at the registry office). The requirements from Article 3 draft RTS under Article 28 AMLR must be met. Determining and registering the country and city or the nearest alternative in the KYC systems is enough to meet requirements according to the articles above. Obliged entities are only required to enter the postal code, street name, a post office box, the building number and/or apartment number into their KYC systems if such information is available. As a result, when collecting the usual place of residence and in terms of the distinction between minimum requirements and additional information to be provided if available, it will be sufficient in practice, for example when identifying natural persons with German citizenship, to use a German passport to collect/verify the information, even though a person's complete address is not listed. Viewing an additional document to verify the complete address provided by a natural person is no longer necessary. Collection of a post office box only is not sufficient to meet this obligation. **e) National identification number:** A national identification number is a unique identification number that is assigned to a natural person by a government agency.

		The number is always valid and does not change. Not all countries assign such numbers, and this also applies to Germany (for a list of EU states personal unique identifiers see Interpretive Notes draft ITS on formats of suspicious activity reports, 69(3) AMLR, p. 11 from 2 July 2026). Article 22(1)(a)(iii) AMLR takes this into account, as the national identification number is only to be collected "where applicable". At least with regard to third countries, it is therefore sufficient if the obliged entities can prove that they have asked the natural person to be identified for their national identification number (e.g. with an optional field in a form or online application). There are no additional inquiry or research obligations, even if the person indicates that they do not have such a number or does not fill out the field. In particular, the obliged entity does not have to interrupt or terminate establishment of a business relationship or occasional transaction. ***Particulars relating to German nationals:*** *When identifying a natural person with a German nationality, there is no need to ask about a national identification number, as Germany, as mentioned above, does not assign a separate national identification number.* f) **Tax identification number:** Pursuant to Article 22(1)(a)(iv) AMLR, a natural person's tax identification number only has to be collected as part of identification if such a number is available. The obliged entities have thus fulfilled this obligation if they can prove that they have asked the natural person to be identified for their tax ID (e.g. with an optional field in a form or online application). There are no additional inquiry or research obligations, even if the natural person does not provide their tax ID. In particular, the obliged entity does not have to interrupt or terminate establishment of a business relationship or an occasional transaction. ***Particulars relating to natural persons residing in Germany:*** *In Germany, as of 2008, the Bundeszentralamt für Steuern (BZSt, Federal Central Tax office) assigns a Tax ID to every German citizen. Banks are able to request the Tax ID using an automated query (Maschinelles Anfrageverfahren der Identifikationsnummer, MAV). When opening accounts or safe deposit boxes, banks are required to do so, provided that their contractual partner does not provide a Tax ID, Section 154(2b) AO (Abgabenordnung, The Fiscal Code of Germany). If possible, banks can and should use this query process to collect a German citizen's Tax ID as part of the identification process.*

10	**Identification of legal entities, Article 22(1)(b)**	***General notes:*** The term "legal entity" stems from EU law and is not necessarily identical with the definition in the varied legal systems within the member states. It must be understood broadly and therefore includes registered partnerships in addition to private corporations (*eingetragene Personengesellschaften, Kapitalgesellschaften des privaten Rechts*). Due to the special identification information required for "other organisations that have legal capacity under national law" listed in Article 22(1)(d) AMLR and the fact that the identification information pursuant to Article 22(1)(b) AMLR appears to be aimed at registered corporate forms, liable parties should, when identifying body corporates, associations and public corporations (*Körperschaften, Verbänden and Kapitalgesellschaften des öffentlichen Rechts*) which are legal persons according to national law, use the identification information listed in Article 22(1)(d) AMLR. The same applies to professional associations (*Berufsvereinigung*), unions (*Gewerkschaften*), religious organisations and regional administrative authorities (*Gebietskörperschaft*) that are, in accordance with national law, capable of being party to a lawsuit or of being sued. In practice, it will not always be possible to make a clear distinction between the identification information in Article 22(1)(b) and (d) AMLR. This is particularly true for foreign legal persons and other organisations with legal capacity in accordance with the relevant national laws. When using a risk-based approach it can therefore, in individual cases, make sense for the obliged entities to combine identification elements from the various identification information listed in Article 22(1)(b) to (d) AMLR.
11	**Identification of legal entities, Article 22(1)(b)** - **What German legal forms are covered by (b)?**	1. The identification information in Article 22(1)(b) and (d) AMLR applies to legal persons under private law and registered partnerships. In Germany, therefore, it covers the following legal forms: • Aktiengesellschaft (stock corporations) • GmbH (including UG (limited liability) and gGmbH) • KGaA • KG • GmbH & Co. KG

	- **Use case "nominee directors"**	• OHG • Professional partnerships (PartGG), including PartGmbB • Eingetragene (registered) GbR • Eingetragener Verein (registered association) • Eingetragene Genossenschaft (registered cooperative) • Deutsche Societas Europaea (European stock corporation) • European Economic Interest Grouping (EEIG) • Companies from foreign countries within the EU or third countries 2. This function is not regulated in German law per se. A nominee director (or proxy director) can, however, be understood as a natural person formally appointed as a member of the legal body of a company (e.g. member of the Board of Directors, CEO) that, however, does not actually have control or responsibility for the management of the company. Often, a nominee director is appointed by the actual owner of the company or a major stockholder on the basis of a contractual agreement; their main responsibility is to implement and enforce the instructions and decisions of the owner/major stockholder. The nominee director is thus acting under their direction and does not actually make any independent decisions, even though they function, legally, as a member of the legal body of the company. Their role is to offer the actual decision-makers anonymity and confidentiality, often for reasons of maintaining privacy or for strategic business reasons. The obliged entities fulfil the requirement to collect the names of the nominee shareholders or directors, including their status, if they can prove that they have asked the legal person to identify such functions (e.g. with an optional field in a form or online application).
12	**Identification of a trustee of an express trust/person holding an equivalent position in a similar legal arrangement, Article 22(1)(c)**	1. The identification information from Article 22(1)(c) AMLR applies when a trust or similar legal arrangement (e.g. a foundation) does not have their own legal capacity. This can be derived from the definitions of the terms "express trust" and "legal arrangement" in Article 2(1)(29) and (32) AMLR. In Germany, Article 22(1)(c) AMLR is therefore material largely for a "Treuhandstiftung" (fiduciary trust without legal capacity).

		2. In Germany, the business relationship is established with the administrator of the trust (trustee) or legal arrangement who acts on behalf of the trust assets or has fiduciary management of the assets, and any account to be opened is therefore opened as a trust account. The administrator of the trust/legal arrangement is seen as the customer and holder of the account. The administrator would also be the originator of an occasional transaction. 3. The term "basic information on the legal arrangement" in Article 22(1)(c)(i) AMLR is defined in Article 2(1)(33) AMLR, which differentiates between basic information in relation to a legal entity (a) or a legal arrangement (b). The relevant definition of the term in Article 22(1)(c)(i) AMLR should, as a rule, be the basic information in relation to a legal arrangement pursuant to Article 2(1)(33)(b) AMLR. The requirement to collect information on assets held in or managed through the legal arrangement includes, in light of the wording of Article 22(1)(c)(i) AMLR, only those assets that are managed as part of the business relationship or subject of occasional transactions. In the case of a Treuhandstiftung, an additional limit can be added to the assets in question, that is the assets held by the foundation to pursue its purposes (from Article 2(1)(33)(a)(vii) AMLR). 4. "The powers that regulate and bind the legal arrangement" pursuant to Article 22(1)(c)(ii) AMLR refers to the framework conditions for management of the assets held in trust, which can usually be determined from the Articles of Association and/or a trust agreement with the manager of the trust or legal arrangement. 5. The requirements in Article 22(1)(c)(ii) AMLR to collect the tax identification number and Legal Entity Identifier if available is not in relation to the manager of the trust/legal arrangement but instead refers to the assets held in trust themselves. The requirement in Article 2(1)(33)(b)(i) AMLR to collect a "the unique identifier of the legal arrangement" is equivalent to the requirement in Article 22(1)(c)(ii) AMLR, that is it does not represent a different or more advanced requirement, so that the requirement to collect this information is to be understood as qualified with "if available". As such,

		the explanations above regarding fulfilling obligations in regard to natural persons apply here (see 9, page 15 et seq.). It is sufficient if the obliged entity can prove that they have at least asked for the tax identification number and Legal Entity Identifier (if relevant). ***Note:*** *In Germany, a Treuhandstiftung also receives a unique and unchanging tax identification number from the Federal Central Tax Office. However, Treuhandstiftung and other similar foundations do not have a Legal Entity Identifier pursuant to the definition in Article 2(1)(27) AMLR, as these are not independent legal (and tax) subjects. The definition of the term "Legal Entity Identifier" is, according to the wording, clearly connected to a legal person.* 6. The identification information from Article 22(1)(c) AMLR in conjunction with Article 2(1)(33)(b) AMLR can, in a modified version, also be used by obliged entities in order to establish a business relationship or carry out an occasional transaction for an association without legal capacity. However, it is important to note that an association without legal capacity has neither a tax identification number nor a Legal Entity Identifier. Obliged entities therefore do not have to ask an association without legal capacity for their tax identification number or Legal Entity Identifier.
13	**Identification information for "other organisations that have legal capacity under national law", Article 22(1)(d)**	1. KYC data for "other organisations that have legal capacity under national law" serves as a catchall. Article 22(1)(d) AMLR applies to all other legal forms with a legal capacity under local law that are not legal persons, a term that refers to corporate forms within the meaning of Article 22(1)(b) AMLR. In Germany, this includes the following legal forms in particular: • Legal persons under public law: (1) **Regional administrative authorities (*Gebietskörperschaften*)** such as the EU, countries, federations, states, districts and municipalities (2) **Professional bodies and umbrella organisations for same (*Verbands- oder Personalkörperschaften*)** under public law, such as a. recognised religious and philosophical bodies, in particular churches (e.g. the Protestant church, in Germany this refers specifically to parishes and parish

		associations, the Catholic church and its diocese and parishes and public religious communities) b. University-level institutions (such as universities, comprehensive universities, technical colleges, etc.) c. Professional associations (such as the bar for lawyers and associations for notaries, doctors, Chambers of Crafts and Trade, or Chambers of Industry and Commerce) d. Health insurance firms and carriers of accident insurance (such as workers' compensation boards), carriers of old age insurance (such as state insurance companies for workers and craftspeople or the Federal Insurance Institution For Employees) (3) **Organisations with legal capacity under public law**, such as Bafin, the KFW, the Deutsche Bundesbank, the Federal Employment Agency, city and county savings banks, public broadcasting corporations or Studentenwerk (student's unions) (4) **Foundations under public law** (such as the *Hilfswerk für behinderte Kinder* (aid organisation for disabled children)), **note:** *Obliged entities can consider requesting additional information as part of a risk-based approach in accordance with the catalogue of "basic information in relation to a legal entity" pursuant to Article 2(1)(33)(a) AMLR (e.g. information on the instrument of constitution or information on the assets held by the foundation to pursue its purposes and used as part of the business relationship/occasional transaction)* • Foundations under private law with legal capacity (pursuant to Sections 80 et seq BGB (German Civil Code, Bürgerliches Gesetzbuch)); ***note:*** *The note above regarding requesting additional information as part of a risk-based approach in accordance with the catalogue of "basic information in relation to a legal entity" pursuant to Article 2(1)(33)(a) AMLR also applies here.* • *Wohnungseigentümergemeinschaften* (Commonhold associations) • *Nicht-eingetragene* (non-registered) GbRs • Political parties • Unions • UN specialised agencies (such as the WHO)

		• International organisations (such as the IWF) 2. The explanation above regarding obligations for natural persons (see 9, page 16) also applies to the requirement in Article 22(1)(d)(ii) AMLR to ask for the tax identification number and Legal Entity Identifier for other organisations with legal capacity, as well as other information, where applicable. It is sufficient if the obliged entity can prove that they have at least asked for the tax identification number and Legal Entity Identifier.
14	**Identification of the beneficial owner, Article 22(2) in conjunction with Article 62(1)(a)**	Pursuant to Article 20(1)(b) AMLR, the beneficial owner must be identified, and the obliged entity must take reasonable measures to verify the identity of the beneficial owner (see Art. 10 draft RTS under Art. 28(1) AMLR). The obliged entity should be satisfied that it knows who the beneficial owner is and that it understands the ownership and control structure of the customer. Pursuant to Article 22(2), all possible means of identification must be used or, alternatively, all the natural persons holding the positions of senior managing officials in the legal entity shall be determined and identified. For this purpose, institutions can determine the beneficial owner using reliable and independent sources, by contacting the customer or via reliance on other obliged entities pursuant to Article 48 AMLR. The **identification information for the beneficial owner** includes all names and surnames, place of birth and full date of birth, address, country of residence and nationality or nationalities of the beneficial owner, the number of an identification document such a passport or ID card and - if available - a unique personal identification number assigned to the person by their usual country of residence, as well as a general description of the source of this number. The interpretation of the data points follows the same rules as the interpretation of data points concerning natural persons as described under 9.

15	**"Senior managing officials" - SMOs pursuant to Article 22(2)**	"For the purpose of this paragraph, 'senior managing officials' means the natural persons who are the executive members of the management body, as well as the natural persons who exercise executive functions within a legal entity and are responsible, and accountable to the management body, for the day-to-day management of the entity.", Article 63(4) subparagraph 2 AMLR. Therefore, obliged entities should take into account that "executive members of the management body" and "natural persons..." are listed as alternatives to one another. The part starting with "as well" should, within the spirit and purpose of the regulation, only be applied to those cases in which the contractual partner does not, due to the legal form of the company, have a formal management body, such as, for example, in a *PartnerschaftsG*. Only in this case there is a need to collect information on other persons who are not part of the formal management body. This follows from the nature of the requirement to collect information on SMOs: it serves as an alternative to collecting information on the beneficial owner, which demands similar treatment. A cumulative understanding of the aforementioned alternatives would result in individual persons under the level of management being included in KYC, meaning that a lack of a beneficial owner would result in significantly higher requirements for institutions and collection of personal data from many more customer employees. Recital 125 AMLR and the draft RTS under Article 28 AMLR clarify that "senior managing officials" does not refer to beneficial owners. There is therefore no requirement to carry out PEP verification or registration with the *Kontoabrufsystem* (government access to bank accounts) pursuant to Section 24c KWG (*Gesetz über Kreditwesen*, German Banking Act). If the obliged entity is uncertain that the persons they have identified are the customer's beneficial owners, then they must record these uncertainties and determine the members of management as described as mentioned above.

	- **Scope of application for Article 22(2) subparagraph 3**	Where identity verification may tip off the customer that the obliged entity has doubts regarding the beneficial ownership of the legal entity, the obliged entity shall, pursuant to Article 22(2) subparagraph 3 AMLR, abstain from verifying the senior managing officials' identity, and shall instead record the steps taken to ascertain the identity of the beneficial owners and senior managing officials. This provision is to be understood as a special rule added to the general due diligence pursuant to Article 22(1) AMLR. The obliged entity has thus met their due diligence identification obligations if they have undertaken the steps laid out in Article 22(1) AMLR. Conversely, there is no need to terminate the business relationship or interrupt establishment of same pursuant to Article 21 AMLR.
16	**Verification pursuant to Article 22(6) and (7)** - **Scope of the verification obligation**	The AMLR and draft RTS under Art. 28(1) AMLR do not fundamentally define specific data points that must be verified to identify the customer. This is in line with the risk and principles-based approach, that is that measures taken should always be (risk) appropriate and expedient. Verification requirements are designed to verify the identity of the person in question, including ensuring that a person with the relevant information/characteristics exists. As such, the objective is not to verify individual data points, but rather to verify that the information conforms with/can be mapped to a person who does indeed exist. In terms of customer identity, some master data is material and must be collected at a minimum in order to ensure that the data can be mapped to a specific person. This includes • All names and surnames • Date of birth • Place (country) of birth • Nationality in order to ensure positive identification of a person that is accurate as possible and/or that the data can be clearly mapped to a single person.

		This data should be compared at the least with the customer information available and a suitable source, and this comparison should be documented. Depending on the situation and risk, it may be advisable for the institution to obtain additional information and documentation for identity verification based on risk, e.g., to verify additional nationalities, (country of) residence, etc., in exceptional cases. **In short, the obliged entity must be sufficiently convinced that the person they are interacting with is who they are claiming to be and that the material data related to risks is correct.**
	- **When is it necessary, pursuant to Article 22(6)(a) AMLR, to collect additional information as part of verification through submission of an identity document?**	The document must be suitable for verifying the identity of the customer - it must provide a clear connection to the individual person to be identified, for example by means of a photo on an ID or possession of an eID. If the person can be identified clearly based on the document presented, additional proof must only be collected if a risk-appropriate approach requires it. This can be determined using the risk factors named in Annex 1 to the regulation, as these are relevant for risk assessment and therefore must be taken into account based on the importance of the information: the more material a piece of information is (or the customer risk is), the more likely it is to be appropriate to also verify that information.
	- **Use of non-eIDAS qualified services by group corporations in third countries**	The risk/principle-based approach is also material in this case. The regulation is designed to define, to the extent possible, a unified standard framework within the EU. That means that as a general rule, not all facts from outside the EU are taken into account, which does not necessarily mean that they are irrelevant.

		In these cases, the obliged entity should verify and document that alternative processes fulfil the requirements as set out in the AMLR and the respective RTS. In addition, obliged entities should document why lawful EU processes cannot be implemented in another country, requiring and making permissible use of equivalent processes. In addition to technical security requirements that ensure validity of the data, obliged entities can base their process on the alternate process pursuant to Article 32 draft RTS under Art. 28(1) AMLR in conjunction with Annex 1 to the regulation, which provides a risk-based approach to minimum requirements for "electronic identification". This means of verification is already part of the framework of implementing group standards in non-EU countries, along with a (gap) analysis with a relevant assessment analysis as to why group standards need to be implemented, which group standards cannot be implemented, or can only be implemented with discrepancies, or may not be implemented.
	- **Which documents meet the requirement "equivalent" in Article 6(1) draft RTS under Article 28 AMLR?**	A list of all relevant documents is not possible, because other (EU) countries may have useful documents that meet the requirements in question. For example, the criteria defined are met by the EU driver's license - although it should be noted that each obliged entity may determine if and which documents may be recognised. The EU driver's license does not contain any information on the country of residence, so it may be necessary to collect further proof, such as a registration of address or a utility bill. Provided that the alternative document does not contain all information to be verified (see above), alternative proof/sources containing said information must be checked.

	- **Which documents meet the simplified requirements for an equivalent document as listed in Article 6(2) draft RTS under Article 28 AMLR?**	In some legitimate cases, if no regular ID document can be presented, official/government documents may be used that allow for, at a minimum, data to be mapped to a single person using the material master data, such as name and birth date to a person via the photo on the document. Documents that have previously been acceptable in Germany, such as simple letters from immigration offices (without a photo) will no longer be acceptable if they are not connected to a document including a photo (e.g. contain a reference to such a document). This will also apply to birth certificates, as these do not meet the minimum requirements. Article 6(2) does provide the option of deviating from the rules listed above with legitimate reasons for doing so. The simplified requirements represent an exception and not an alternative and are thus only a fall-back solution. To use this solution, an obliged entity must provide audit-proof argumentation for doing so in each individual case. In terms of birth certificates, this would mean that they can only be used when there is no identification document for a minor that meets the requirements in Article 6(1) or (2). In all other cases, the existing identification document must be used.
	- **Other requirements from Articles 6 and 7 draft RTS under Article 28(1) AMLR.**	Identification and verification based on documentation remains the norm (in addition to electronic identification verification). The standard is therefore ID cards or passports, which always allow for unique identification of a person. Even if additional alternative documents can also be used as a standard or fall-back solution after internal verification, their use should be limited to exceptions with appropriate justification. The requirements of Articles 6 and 7 draft RTS under Article 28 AMLR can also be relevant when verifying trustees/those with similar positions, provided they are natural persons. They also apply to identification of the beneficial owner, provided the obliged

		entity wishes to use a verification method pursuant to Article 22(6) (see reference in Article 22(7)(a)).
	- **Which documents can be used to verify identification information for a legal person or other organisations under public law (list of potential sources and reference to Article 8 draft RTS under Article 28 AMLR)**	In terms of legal persons and organisations under public law (PP), obliged entities must first determine which general requirements from the AMLR are risk based and appropriate (risk and principle-based approach). In addition, obliged entities must distinguish between legal persons and organisations under public law. Obliged entities must use the relevant legal system to verify and determine which legal requirements are capable of being implemented and are appropriate for these specific legal forms. In terms of identifying a legal person under public law, there are no changes to the systematic structures previously in use in Germany: • Identification - that is proof of existence - is usually the legal act used to create the PP and which usually contains all information on designation, representation, country the entity was founded in/headquarters, etc. • Viewing a register is not relevant, as there are no existing registers. (If it is a public law entity or owner operated company, check for special cases if they are commercially active and operating as a *Formkaufmann* (merchant by legal form)). • Determining a beneficial owner should not be relevant given the purpose and legal form, as there are no shareholder structures, voting rights or natural persons with relevant controlling interests. In regard to organisations under public law that have legal capacity under national law (partially legally capable entities such as DWD (German weather service)), the difference lies solely in the legal classification. In practice, identification can be done as with legal persons under public law.

		In terms of foreign entities under public law, it is important to check local requirements and framework conditions (e.g. requirement to register/availability of a register).
	- **Which "reasonable measures" must obliged entities employ to verify identification information for beneficial owners, taking into account a risk-based approach and requirements from Article 10 draft RTS under Article 28 AMLR?**	The identity of the beneficial owner (BO) must be verified using appropriate means. This means collecting all data that make it possible to identify the individual person. A risk-based approach is the material standard of interpretation in this case, as it defines the scope and intensity of identification measures. The goal is to provide the flexibility to find the most appropriate and risk-appropriate solution for each BO. Customers with a higher risk require more proof that the person exists, and this must be verified with additional measures. This verification does not cover specific individual data points, but rather must ensure, to a sufficient risk-appropriate degree, that the BO is not a *fictional* person or one who *cannot be found* - simply making a determination is not sufficient. The core data must be defined (see 14, page 26 above) as those are needed to uniquely identify the person, and additional data points if required in order to measure and control risks. Identification verification must be independent from the collection source; it always requires at least two independent sources. Additional data points may require provision of associated proof/supporting documents or sources for plausibility checks. For low-risk customers/customers within the SDD framework, it may be sufficient to collect data from the customer or to view a reliable source. The central or commercial register would suffice here. However, verification may not take place using the central or commercial register.

		For customers that are not low risk, obliged entities must define measures that are both more thorough and secure. For example, presentation of an uncertified copy of an identification document (possibly taking into account Article 6 draft RTS under Article 28(1) AMLR). To verify the identity/existence of a BO in high-risk cases, a full identification (analogue to a customer identification) may be appropriate.
	- **Handling information to be collected on intermediate entities pursuant to Article 11 draft RTS under Article 28 AMLR.**	The requirement to collect data on intermediate entities within the ownership structure is closely related to collection of information on the BO, which must, as was previously the case, be verified. This means that the ownership structure must be understood and verified. Additional data must be collected on intermediate entities in order to prove that the structure of a customer has been verified and validated. Collection and verification is done using a risk-based approach, which requires each specific institution to define measures for same. Requirements for the BO can be used to derive measures in this case. Generally, the quality of plausibility checks/verification measures must be plausibly in line with the customer/business relationship risk and documented accordingly. This might look as follows: • Low risk: customers statement and perhaps an uncertified copy from the customer • Medium risk: use of reliable sources • High Risk: view registers and provide associated proof
	- **Obligation to consult the central registers, Article 22(7)**	Additional verification via an excerpt from the central register is always required as part of establishment of the business relationship in order to verify information on the identified beneficial owner.

		It is not strictly necessary to request another excerpt from the register when updating customer data. The obliged entity may nevertheless obtain a current excerpt if deemed risk adequate. The obligation to request an excerpt from a central register only applies to central registers in an EU member state, as this is the only case in which the legal framework is identical and even registration criteria are different in third countries. Nonetheless, an obliged entity could make use of such registers as supporting documentation, provided they are comparable. NOTE: As a general rule, business partners are required, when establishing a relationship with a bank in Germany (or the EU) to register with a central register within an EU member state. If equivalent to AMLR standards, Art. 16(1), 17 AMLR require the group entity in a third country to view the central register only where required under local obligations in accordance with local requirements. If the third country of the group entity is less strict than AMLR, local central registers have to be consulted where available, not however the EU Central Register.
17	**Timing of fulfilment of due diligence obligations, Article 23**	The identification and verification of the identity of a customer must, in principle, take place before the establishment of a business relationship. That means that in general the identification process must be started and completed as the first line of business when it comes to customer contact for the purpose of establishing a business relationship. This can be derived from Article 33 (Simplified Due Diligence), which states that verification, but not identification, can take place within 60 days. In regard to legal persons, identification and verification of the beneficial owner must also be completed before a business relationship is established. This includes viewing the central register. In general, it is important to note that this applies to the identification and verification of the customer or other involved persons. Therefore, these requirements do not apply to all information and data to be collected within the framework of a business

		relationship. The obliged entity must, using a risk-based approach, determine which data and information must be collected at an early stage during the establishment of the relationship in order to evaluate any potential risks - in particular if they plan to make use of relief pursuant to Article 23(2) AMLR.
	- **Regarding persons who are not the customer or beneficial owner**	When applying simplified due diligence, Article 33(1) offers the option of verifying the identity after the business relationship has been established. This simplification applies, according to the wording, only to customers and beneficial owners, however according to the spirit and purpose of the regulation, this exception also applies to other persons that are subject to KYC, e.g. PPA or person on whose behalf the customer is acting. This arises from not just the fundamental equal treatment of customers, BOs and other persons (e.g. as found in Article 23(1) AMLR), but also from the principle of a fortiori. If a customer that establishes a business relationship themself can be verified at a later date, than this must apply, a fortiori, to other persons that are subject to KYC. The same is true for identification at a later date pursuant to Article 23(2) AMLR. In accordance with the principle of a fortiori, this must also be possible for persons who are not the customer or beneficial owner.
	- **Effect of granting a Verfügungsbefugnis (power of sale) for an account**	A person can only have drawing authority over an account if the identification of the person with that authority is complete. This presumes that the customer has been identified, as without this step no business relationship can be established/no account can be opened. Note: in this case, there is risk-based relief available for low-risk cases.
18	**Discrepancies, Article 24**	

	- **Does this include discrepancies in terms of ownership/control structures and/or information on intermediate entities?**	Pursuant to Article 24(1) AMLR, obliged entities must also report discrepancies in the information collected on ownership or control structures or for intermediate entities. The obligation to report arises, in particular, from the fact that the ownership and control structure is material for the actual existence of a beneficial owner and their associated control over the use of the products and services. In addition, intermediate entities could be material for determining whether a natural person meets the required threshold for determining a beneficial owner or not.
	- **"Discrepancy" in regard to the beneficial owner**	Article 24(1) AMLR also states that, in principle, any discrepancy between the data entered into the register and the data collected by the obliged entity must be reported to the central register. The cases listed in Article 24(2) are the exceptions, that is typographical errors, different transliterations, or minor inaccuracies and outdated data, but the beneficial owners are known to the obliged entity from another reliable source.
	- **Scope of reporting obligations in Article 24(2) subparagraph 2**	Where an obliged entity concludes that information in the central register is incorrect, it has the option, within the meaning of Article 24(2) subparagraph 1 AMLR, instead of reporting the discrepancy, of inviting the customer to submit the correct information to the central register, but only if the discrepancy relates to the errors listed in Article 24(2)(a) and (b). The invitation to correct the information should be documented. If an obliged entity notices typographical errors, different transliterations or minor inaccuracies or information arising from outdated data, but the correct information is known to the obliged entity from another reliable source (e.g. current register excerpts, certified company documents, confirmation from an auditor), there is no need to report the discrepancies to the central register. This provision includes only that incorrect information that is covered by Article 24(2)(a) and (b) (less serious discrepancies). Expanding this to include serious discrepancies is, on the one hand, in contradiction to the systematic structural norm,

		which implies that only those less serious discrepancies pursuant to Article 24(2)(a) and (b) are included in the legal elements subsumed therein in regard to the invitation to the customer to correct the information (see also recital 54). In addition, extension of the option to invite the customer to correct the information to include serious discrepancies pursuant to Article 24(1) could result in two reports of the identical facts being submitted to the central register - from the obliged entity and then a correction from the customer. The requirement for obliged entities to report discrepancies to the central register remains unaffected and an exception based on a direct invitation to the customer is in contradiction to the nature of the requirement to report the discrepancy.
19	„**Commercial name/trade name" pursuant to Article 2(2) draft RTS under Article 28 AMLR**	A trade name is a designation that the customer uses to carry out their business on the market. This name may be different from the name under which the business is listed in the register (registered name). The definition of the trade name has replaced the previous label, commercial name, in order to match existing EBA regulations and ensure a unified designation across all member states. Obliged entities must record the customer's trade name in order to make sure that they have documentation of the customer's designation used to carry out their business on the market pursuant to Section 2 Article 2(2) EBA/REP/2025/35. The trade name serves to uniquely identify the customer in their commercial practice. It may not match their trade mark. When collecting a trade name, an obliged entity may record a shortened name or one used for marketing instead of the name registered in the commercial register, as long as the customer is uniquely identified. This can be derived from, among other sources, recital 13 of the EU EUR Trade Mark Regulation. Pursuant to EBA EBA/REP/2025/35 – Question 1 Article 1(2), in the event that the trade name differs from the registered name, the trade name can be collected from the customer in the form of a written declaration.
20	**Identification of the purpose and intended nature of a business relationship or occasional transaction, Article 25**	Due diligence requirements include, pursuant to Article 20(1)(c) AMLR - which is comparable to the existing requirements from Section 10(1)(3) GwG - the requirement,

		before establishment of a business relationship, to obtain and assess information on the business relationship in order to understand the purpose and intended nature of the business relationship or the occasional transactions. This should include how and why the contractual partner wishes to use the products or services of the obliged entity. This requirement is specified in Article 25 AMLR: Before entering into a business relationship or performing an occasional transaction, an obliged entity shall assure itself that it understands its purpose and intended nature. Where necessary, the obliged entity can collect information such as the purpose and economic rationale of the business relationship, the estimated amount of the envisaged activities, the source and destination of funds, the business activity or the occupation of the customer. Identifying the purpose of the business relationship is the foundation of basic customer due diligence. Understanding the business relationship is designed to allow the obliged entity to assess whether the activities observed, in particular those observed via monitoring, match the information collected. The wording of Article 25 AMLR means that collecting information on the purpose and intended nature of the business relationship or occasional transaction must only take place where necessary in order for the obliged entity to understand the business relationship. Proof of this (subjective) understanding should be easier to provide (and document) for classic investment products for safeguarding assets, specific securities accounts or insurance products than for more complex products or those that allow the contractual partner access to a large range of uses (e.g. business accounts or credit products that are tied to a specific project). For these products, it could make sense for the obliged entity to collect additional information, in general by asking the (occasional) customer. If new findings arise over the course of the business relationship, or the obliged entity discovers new facts within the framework of monitoring, it may be necessary to once

		again identify the purpose and intended nature of the business relationship or transaction.
21	**Ongoing monitoring of the business relationship, Article 26**	Article 20(1)(f) AMLR requires obliged entities to conduct ongoing monitoring of the business relationship as part of due diligence to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer and the business and risk profile, including where necessary the source of funds. This requirement is specified in Article 26 AMLR: obliged entities shall conduct ongoing monitoring of business relationships, including transactions undertaken by the customer throughout the course of a business relationship, to ensure that those transactions are consistent with the obliged entity's knowledge of the customer, the customer's business activity and risk profile, and where necessary, with the information about the origin and destination of the funds (source of funds, SOF). The goal is to identify those transactions that require, based on the suspicion that a report must be made pursuant to Article 69(2) AMLR, further assessment, and to release those transactions that are consistent with the knowledge of the customer. Here, the obliged entity must take into account the AMLA guidelines under Article 26(5) AMLR. It is only via ongoing monitoring that obliged entities are able to effectively combat risks of money laundering and terrorist financing. Ongoing, dynamic monitoring that is able to recognise abnormalities and discrepancies is therefore required. This is the only way to create a meaningful customer profile which takes into account individual business behaviour and continue to compare it with the transactions that take place. If business relationships cover more than one product or service, obliged entities must ensure that their due diligence covers all products and services. The recitals make it clear that obliged entities must set up a monitoring system that allows for recognition of suspicious transactions which could indicate money laundering or terrorist financing at an early stage. Ongoing monitoring can only be effective if it covers, at base, all the products, services and transactions offered to the

		customer, both those carried out in the customer's name and those offered to the customer. However, there is no need to check each individual transaction. Monitoring intensity may be calibrated using a risk-based approach. This should take into account, in particular, the customer's characteristics and the associated level of risk, products and services on offer and the countries or geographical areas in question. If obliged entities are part of a group and maintain a business relationship with customers that are also customers of another company within the same group, these additional business relationships must be taken into account as part of monitoring. Article 16 AMLR is particularly relevant in terms of the required scope of group-wide monitoring: a parent undertaking must establish and implement group-wide policies, procedures and controls, including on information sharing within the group for AML/CFT purposes. According to the wording of the law, information sharing applies, in particular, to the identity and characteristics of the customer, its beneficial owners or the person on behalf of whom the customer acts, the nature and purpose of the business relationship and of the occasional transactions and the suspicions (including the underlying analyses). The extent of the information to be shared is determined by the obliged entities. As such, appropriate group-wide monitoring that is risk-based, proportional and conforms with data protection rules already exists within the meaning of the regulation if the information listed above can be exchanged between group entities within the framework of monitoring.