AMLR, CDD RTS, DIdG, GwBG: New anti-money laundering requirements from 2027

HOW ANTI- MONEY LAUNDERING RULES ARE CHANGING CUSTOMER IDENTIFICATION, WHAT ROLE THE EUDI WALLET CAN PLAY, AND WHEN TRADITIONAL VIDEO IDENTIFICATION CAN STILL BE USED



Executive Summary

From 10 July 2027, the EU Anti-Money Laundering Regulation (AMLR) will apply directly. At the same time, a new German Anti-Money Laundering Act (GwBG) is supposed to replace the previous Money Laundering Act (GwG). A final report on the draft regulatory technical standards (CDD RTS) issued by the EU's anti-money laundering authority, AMLA, sets out in detail how obliged entities will need to verify the identity of their customers and keep their customer information up to date in future. In Germany, the Digital Identities Act (DIdG) has already made amendments to the GwG for the transitional period. This update explains how obliged entities can prepare for the new requirements, in which cases traditional video identification may still be an option in future, and why banks and financial service providers in particular should strategically merge their AMLR implementation efforts with the integration of the EUDI Wallet under eIDAS 2.0.

1. Introduction and legal framework: from directive to regulation

The 10 July 2027 deadline is fast approaching for obliged entities under the EU Anti-Money Laundering Regulation[1] (AMLR). Until now, Member States have transposed the EU's customer due diligence (CDD) and "Know Your Customer" (KYC) requirements into national law based on the

[1] Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

EU Money Laundering Directives. In Germany, this is the Money Laundering Act (*Geldwäschegesetz*; GwG). The new AMLR marks a change of instrument by the EU legislator. Going forward, the requirements will stem directly from an EU regulation. In Germany, the amendments to national law required by the AMLR will be implemented by the new Anti-Money Laundering Act (*Geldwäschebekämpfungsgesetz*; GwBG), for which a draft bill[2] has already been proposed. The GwG will be repealed on 10 July 2027.

While this means that the AMLR will directly define the core elements of customer due diligence in future, i.e. grounds for CDD measures, their scope, and the collection and verification of the identity of customers and beneficial owners, more specific technical standards are required for their operational implementation. The recently published final report by the Authority for Anti-Money Laundering and Countering the Financing of Terrorism[3] (AMLA) on the draft regulatory technical standards under Article 28(1) of the AMLR (hereinafter "CDD RTS") provides a detailed regulatory framework setting out the customer due diligence requirements. Not only do the CDD RTS set out the general requirements for data collection, data verification and ongoing monitoring, they also significantly strengthen the role of digital identities in CDD and KYC processes.

Given the standard timeframes for adoption by the Commission by means of a delegated regulation, as well as for any objections from the European Parliament and the Council – and given that the delegated regulation is not due to take effect until six months after its entry into force – the CDD RTS are not expected to formally apply until after the AMLR takes effect on 10 July 2027. Obliged entities that implement the new rules early face a certain data protection risk, as there is no clear regulatory obligation during the interim period. This risk could have been avoided if the legislature had coordinated its timetable more carefully. However, given the solid foundation laid down in the AMLR – which the CDD RTS merely elaborate upon – it seems entirely reasonable and, given the limited time remaining and absence of alternative standards, even advisable for obliged entities to start adapting their processes in line with the CDD RTS now, with the aim to be ready on July 10, 2027.

At the national level in Germany, these developments are accompanied by the Digital Identities Act[4] (*Digitales Identitätengesetz*; DIdG), which implements the eIDAS Regulation[5]. Alongside the new Act on the European Digital Identity Wallet (*Gesetz über die Europäische Brieftasche für die Digitale Identität*; EBDIG), the DIdG has already made targeted amendments to the GwG – and in the future, to its successor, the GwBG – in order to prepare for the transition to the new EU regulatory framework.

2. Two equally valid default methods for identitychecks: identity document or eIDAS solution

Article 22(6) of the AMLR already sets out two equally valid default methods for collecting information for verifying the identity of a customer or any individual claiming to act on a customer's behalf:

- **Document-based (a):** using an identity document, passport or equivalent; or
- **Electronically (b):** through electronic identification means which meet the requirements of the eIDAS Regulation with regard to the assurance levels "substantial" or "high" and relevant qualified trust services as set out in that Regulation.

Which methods specifically fall under the category of "electronic identification means" according to Article 22(6)(b) of the AMLR? The CDD RTS specify these as electronic identification means as defined in Article 3(2) of the eIDAS Regulation, regardless of whether they have been

[2] Available (only in German) at https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Downloads/Gesetz/2026/20260715-geset-zentwurf-12-gwb-novelle.pdf.

[3] Available at https://www.amla.europa.eu/document/download/e15ab2e5-4074-4de8-bb9d-613dd8b7fdd1_en.

[4] Available (only in German) at https://dip.bundestag.de/vorgang/gesetz-zur-durchf%C3%BChrung-der-unionsrechtlichen-vorschriften-%C3%BCber-die-europ%C3%A4ische-brieftasche/335473.

[5] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

notified, as long as they comply with the requirement of either "substantial" or "high" assurance levels, and relevant qualified trust services. Specifically, these include:

- **Existing national electronic identification means,** such as the eID, which has been in existence since the end of 2010 (e.g. in the online ID function of German identity cards); however, its adoption varies greatly across the Member States.

- **EUDI Wallet:** The future European Digital Identity Wallet is, by law, classified as having a "high" assurance level and is expressly highlighted by the AMLA as a means of identification in the recitals of the CDD RTS. In Germany, the Digital Identities Act (DIdG) is already anticipating this option for the transition period up until 10 July 2027. Article 6 of the DIdG introduces the EUDI Wallet as a new means of identification into Section 12(1) sentence 1 no. 4a of the Money Laundering Act (GwG), as amended, and stipulates that the electronic data generated during the authentication and validation of person identification data must be recorded for documentation purposes in accordance with Article 5b(9) of the eIDAS Regulation (Section 8(2) sentence 9 GwG, as amended).

- **Qualified trust services,** in particular, procedures based on qualified electronic signatures (QES), qualified certificates or qualified electronic attestation of attributes (QEAA). Here, too, the German Digital Identities Act ensures practical, ex ante harmonisation by removing the requirement, previously set out in Section 12(1) sentence 3 of the GwG, to request an additional reference transfer from the customer's payment account when using a qualified electronic signature (QES). By relaxing this requirement, German lawmakers are anticipating the future legal situation under the AMLR and the CDD RTS, which no longer require a reference transfer for a QES.

Article 6(4) of the CDD RTS also expressly clarifies that electronic identification means and qualified trust services may be used to verify the identity of natural persons, even when the customer is physically present. This makes it clear that eIDAS-compliant solutions are not treated as subordinate under the AMLR, but are **at least equivalent to physical identity documents**. In practice, this means that such electronic means can be used as a standardised form of identification across all sales channels – both digital and brick-and-mortar.

3. Video identification: trust service or strictly limited exception (Article 7 of the CDD RTS)

What does this new priority given to eIDAS-compliant methods for remote identificationj mean for existing video identification procedures? In future, this will depend on how they are integrated into other regulated services. eIDAS-certified video identification procedures may be used for identity verification purposes when issuing qualified certificates or qualified electronic attestations of attributes (QEAA) in accordance with Article 24(1a)(c) of the eIDAS Regulation and may thus indirectly form part of an identification method in accordance with Article 22(6)(b) of the AMLR.
However, standalone video identification procedures that are not integrated into a qualified trust service – such as many of those currently in use in Germany under the GwG and BaFin Circular 3/2017 (GW) – will become a subsidiary exception under Article 7(1) of the CDD RTS. Compared with the consultation draft, the AMLA has made Article 7 of the CDD RTS stricter. The means of identification set out in Article 22(6) of the AMLR remain the strict default; alternative remote identification solutions may only be used if none of these default methods can be utilised.
Such alternative solutions may only be used in situations where the following conditions are both met:

1. A natural person cannot reasonably be expected to present their identity document in a face-to-face context, and

2. they do not have access to eIDAS-compliant electronic identification means or qualified trust services.

If both conditions are met, the person's identity may be verified remotely through their identity document, passport or equivalent using an alternative verification solution. However, any fallback solution must meet strict minimum requirements (Article 7(2) of the CDD RTS):

- **Reliability:** Reliable and independent sources of information must be used, and appropriate safeguards must be put in place.
- **Document holder verification:** It must be ensured that the person presenting the identity document is in fact the document holder.
- **Secure communication:** The integrity and confidentiality of communications must be ensured.
- **Data quality:** Any images, video, audio and other data must be captured in a readable format and of sufficient quality that the person is unambiguously identifiable.
- **Discontinuation:** The identification process must not continue if technical shortcomings or unexpected connection interruptions are detected, or there are any doubts or suspicions regarding the identity of the person or the integrity of the verification process.
- **Documentation:** The information and documents must be valid and up to date; copies must be time-stamped and stored securely and must allow for *ex post* verification.

In particular, the requirements regarding data quality and process integrity are becoming increasingly challenging for obliged entities. Generative AI, deepfakes and attacks in which manipulated content is fed into the verification process make deception attempts considerably easier. Although the video identification procedures currently in use in Germany on the basis of BaFin Circular 3/2017 (GW) may largely meet these standards, they should nevertheless be reviewed on a case-by-case basis, particularly in light of current requirements for addressing these attack vectors.
In addition, obliged entities must be able to **justify** their use of alternative solutions by explaining and documenting, on a case-by-case basis, why the customer's identity could not be verified via the default methods set out in Article 22(6) of the AMLR. They must also be able to demonstrate to the supervisory authority that the alternative solution used complies with the requirements of Article 7 (Article 7(3) of the CDD RTS). In practice, this gives rise to considerable legal uncertainty. As eIDAS-compliant means of identification and qualified trust services become increasingly available and widespread, it is likely to become ever more difficult to provide a convincing justification for resorting to an alternative method.

4. Detailed specifications of the CDD RTS: data, equivalent documents and electronic attributes

A smooth onboarding process is a competitive advantage for financial institutions. This makes the CDD RTS all the more important, where they specify in greater detail, beyond the scope of the AMLR, the data to be collected from natural persons in accordance with Article 22(1)(a) of the AMLR (Articles 2 to 5 of the CDD RTS):

- **Name(s):** All names, including first name(s) and surname(s) that feature on the identity document or through the electronic identification means must be obtained.
- **Address:** The following address information must be provided: full country name or the abbreviation in accordance with the International Standard for country codes (ISO 3166), the name of a city, municipality, town or village, including postal code if such code has been issued and the name of the state where relevant, and the street name, building number, apartment number and post-box number, where such information exists.

- **Place of birth:** The information provided must consist of at least the name of the country, state, city, municipality, town or village as it features on the identity document or through electronic identification means.

- **Nationality:** Obliged entities must take reasonable measures to establish whether a person holds more than one nationality.

The data collected must then be verified. If this is done **on the basis of documents**, this must, in accordance with Article 22(6)(a) of the AMLR, be done by means of an identity card, passport or **equivalent document**. According to the CDD RTS, a document is deemed equivalent if it meets the following requirements (Article 6(1) of the CDD RTS):

- **Issuer:** a designated authority in accordance with the applicable law;

- **Information:** the document holder's first name(s) and surname(s), place and date of birth, as well as the document number and date of expiration;

- **Photograph and signature:** photograph of the document holder's face and their signature;

- **Protection against forgery:** security features to ensure the authenticity of the document.

If someone is unable to provide such a document for a legitimate reason – such as being stateless or a refugee or under subsidiary protection – documents containing their name(s), date of birth and facial image are sufficient; any missing information must then be obtained using additional reliable and independent means (Article 6(2) of the CDD RTS).
If verification is carried out **electronically** in accordance with Article 22(6)(b) of the AMLR, Annex I to the CDD RTS defines the list of attributes electronic identification means or qualified trust services are required to feature for this purpose; these attributes are based on the person identification data in the EUDI Wallet in accordance with the eIDAS Implementing Regulation (EU) 2024/2977 (Article 27(1) of the CDD RTS). If the eIDAS solution used transmits all the required attributes, these attributes are already deemed to have been verified and, according to the AMLA, do not need to be verified again against other sources. However, as the eIDAS data set treats certain information as optional attributes, depending on the Member State or the means used, the following applies: Where the specific eIDAS solution used does not possess individual attributes required under the AMLR and the CDD RTS, this missing information must be obtained and verified through other means (Article 27(2) of the CDD RTS).

5. Customer due diligence as an ongoing obligation: ongoing monitoring and existing business relationships

Onboarding is by no means the end of the customer due diligence process. From an operational perspective, the ongoing monitoring obligations relating to existing business relationships (Article 26 of the AMLR) are likely to be particularly significant:

- **Regular updates:** Customer information must be updated for all customers at least every five years; in the case of higher-risk customers, this must be done at least once a year.

- **Ad hoc reviews:** Even between these regular updates, certain circumstances may make a review necessary.

- **Screening:** A risk-sensitive assessment must be conducted without delay to determine whether customers or beneficial owners are, or have become, politically exposed persons (PEPs), whenever new information becomes available or the list of prominent public functions is updated. A financial sanctions screening must be carried out when establishing a business relationship, whenever there are changes to the lists or to customer data, and at regular intervals. Automated screening tools, manual checks or a combination of the two are permitted.

Digital identities can help in this context, too, enabling customers to submit up-to-date and verified data seamlessly as part of a **KYC refresh**.

There is no leeway regarding the review periods. The AMLA has expressly rejected calls for longer update intervals. The maximum time limits of one and five years, respectively, stem directly from Article 26(2) of the AMLR and cannot be altered or extended by the RTS. Monitoring and updating processes must therefore be fully aligned with these periods.

Preexisting business relationships also needs to be taken into account. Documents, data and information relating to business relationships established prior to the entry into force of the delegated regulation adopting the CDD RTS must be brought in line with the requirements of the AMLR and the CDD RTS with a risk-based approach and within the specified maximum periods (Article 28 of the CDD RTS). However, according to Recital 26, the maximum periods for updating customer information only start with the date of entry into force of the Delegated Regulation for ongoing business relationships established before that date.

6. Note for eIDAS relying parties: strategic integration of AMLR implementation, DIdG and the EUDI Wallet

While the CDD RTS cover all eIDAS-compliant means of identification and qualified trust services without favouring any specific technology, companies in the financial sector would be wise to take a closer look at the future EUDI Wallet (see also our GSK Update from July 2026). This is because the wallet not only serves as the reference model for the list of attributes contained in the CDD RTS, but – unlike previous national eID solutions – its widespread market penetration is supported by the legal framework of the revised eIDAS Regulation (eIDAS 2.0) and the German Digital Identities Act (DIdG):

- Each Member State must provide at least one EUDI Wallet by **24 December 2026**. With the introduction of the Act on the European Digital Identity Wallet (EBDIG) as Article 1 of the German Digital Identities Act, German lawmakers have now established the national framework and defined responsibilities – under the leadership of the Federal Ministry for Digital Affairs and Government Modernisation (BMDS) and with the Federal Network Agency acting as the supervisory authority. The German government is set to launch its own EUDI Wallet, **"d-you"**, on **2 January 2027**, which will then gradually be expanded to include qualified electronic attestations of attributes, QES and more.
- Public sector bodies that require electronic identification to access an online service must accept EUDI Wallets for this purpose at the user's request (Article 5f(1) of the eIDAS Regulation). Providers of very large online platforms (VLOPs) within the meaning of the Digital Services Act[6] must accept the EUDI Wallet as a means of authentication for their users in certain transactions **as soon as the first EUDI Wallet is made available** (Article 5f(3) of the eIDAS Regulation).
- From **24 December 2027**, certain private companies (with the exception of microenterprises and small enterprises) – including, in particular, **banks and financial service providers** – will be obliged in their capacity as "relying parties" to accept the EUDI Wallet upon the voluntary request of the user, provided that they are legally or contractually required to use strong user authentication for online identification (Article 5f(2) of the eIDAS Regulation). These obligations are likely to significantly accelerate the adoption of digital identities, as customers will come to expect to be able to use a digital wallet to verify their identity with their bank as well.

Against this backdrop, organisations that are both obliged entities under the AMLR and relying parties obliged to

[6] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)

accept digital wallets under Article 5f(2) of the eIDAS Regulation would be well advised to make strategic use of the tight sequence of deadlines in 2027. There are only a few months between the launch of the German EUDI Wallet – including the amendment of Section 12(1) no. 4a of the GwG introduced by the DIdG (early January 2027), the date from which the AMLR applies (10 July 2027, followed shortly afterwards by the CDD RTS) and the date from which the obligation to accept the wallet comes into force in the financial sector (24 December 2027). Rather than considering these requirements in isolation, it makes sense to bring forward the integration of the EUDI Wallet to July 2027 (or even earlier, as part of the GwG amendment) and to combine it with the AMLR implementation in a single project. In this regard, financial institutions should bear in mind that, in accordance with Sections 2(2) sentence 1 no. 2(b), and 10 of the EBDIG, read in conjunction with Article 5b(1) to (3) of the eIDAS Regulation, relying parties must register with the competent registration authority, in Germany the **Federal Office of Administration**, in order to obtain the necessary authorisation certificates prior to their first wallet interaction. As the data to be requested must be specifically listed and justified at the time of registration, and only these registered attributes may be requested from customers, the scope of registration with the Federal Office of Administration should be aligned with the requirements of the AMLR and Annex I of the CDD RTS at an early stage.

The use of the EUDI Wallet is voluntary for customers, and it is not expected that all customers will have one by 10 July 2027. Therefore, alternative identification methods must continue to be supported until further notice. Nevertheless, the advantages of synchronised implementation clearly outweigh the disadvantages. As the CDD RTS already establish eIDAS-compliant procedures as the new standard for remote identification, institutions can avoid duplicating IT project efforts within the space of five months by consolidating efforts at an early stage. This also allows them to set up a legally compliant target architecture in accordance with Article 22(6)(b) of the AMLR from day one, which, as the use of digital wallets becomes more widespread, will gradually reduce the time-consuming justification and documentation requirements associated with subsidiary alternative solutions under Article 7 of the CDD RTS.

7. Conclusion and outlook

The CDD RTS set out the specific requirements of the AMLR for onboarding and ongoing customer due diligence and – in conjunction with the German Digital Identities Act – send a clear message concerning methods of remote identification. eIDAS-compliant solutions, such as national eIDs, qualified trust services and the future EUDI Wallet, will become the default method for digital customer identification, while traditional video identification and similar procedures may only be used in exceptional cases and require justification. The following steps are recommended for a smooth implementation of the new requirements by July 2027:

- **Gap analysis:** Align existing onboarding and KYC processes with the more specific data and documentation requirements of the CDD RTS, and review the relief under the Money Laundering Act introduced by the Digital Identities Act (in particular, the removal of the requirement for a reference transfer for QES and the recording of validation data in accordance with Section 8(2) sentence 9 GwG, as amended);

- **Remote identification and eIDAS strategy:** Review existing video identification and other remote identification procedures and, where possible, integrate them into a qualified trust service. Expand adoption of eIDAS-compliant identification methods and, where necessary, document alternative solutions for exceptional cases in accordance with Article 7 of the CDD RTS, and establish processes for justifying exceptions on a case-by-case basis;

- **Integration with the EUDI Wallet (for obliged entities that are also relying parties):** Plan for the early integration of the EUDI Wallet by 10 July 2027 at the latest, including registering as a relying party with the Federal Office of Administration using data aligned with the list of attributes in Annex I of the CDD RTS;

- **Data protection:** Adapt data protection governance, in particular privacy notices, check whether a data protection impact assessment is required, and review contracts with "eIDAS-intermediaries";

- **Ongoing monitoring and existing business relationships:** Align the monitoring and screening processes with the statutory maximum periods (one or five years) and draw up a plan for bringing existing customer information in line on a risk-based approach in accordance with Article 28 of the CDD RTS.

Organisations that address the CDD RTS and the changes introduced by the DIdG early on will not only ensure compliance by the July 2027 deadline, but will also be able to make targeted use of the new regulatory guidelines to reorganise their onboarding and KYC processes for both new and existing customers seamlessly and efficiently.

Do you have any questions? Our lawyers will be happy to assist you.

Per Meyerdierks
Rechtsanwalt
Hamburg
per.meyerdierks@gsk.de

Dr Harald Feiler
Rechtsanwalt
Frankfurt
harald.feiler@gsk.de

Disclaimer
This client briefing exclusively contains general information which is not suited to addressing the particular circumstances of an individual case. The client briefing does not qualify as advice or a binding offer to provide advice or information and it is not suitable as a substitute for personal advice. GSK Stockmann – all rights reserved.

GSK
STOCKMANN

Copyright
GSK Stockmann – all rights reserved. The reproduction, duplication, circulation and / or the adaption of the content and the illustrations of this document as well as any other use is only permitted with the prior written consent of GSK Stockmann.

Disclaimer
This client briefing exclusively contains general information which is not suitable to be used in the specific circumstances of a certain situation. It is not the purpose of the client briefing to serve as the basis of a commercial or other decision of whatever nature. The client briefing does not qualify as advice or a binding offer to provide advice or information and it is not suitable as a substitute for personal advice. Any decision taken on the basis of the content of this client briefing or of parts thereof is at the exclusive risk of the user.

GSK Stockmann as well as the partners and employees mentioned in this client briefing do not give any guarantee nor do GSK Stockmann or any of its partners or employees assume any liability for whatever reason regarding the content of this client briefing. For that reason, we recommend you to request personal advice.

www.gsk.de

GSK Stockmann
Rechtsanwälte Steuerberater Partnerschaftsgesellschaft mbB

BERLIN
Anton-Wilhelm-Amo-Str. 42
10117 Berlin
T +49 30 203907 - 0
F +49 30 203907 - 44
berlin@gsk.de

HEIDELBERG
Europaplatz 3
69115 Heidelberg
T +49 6221 4566 - 0
F +49 6221 4566 - 44
heidelberg@gsk.de

FRANKFURT/M.
Bockenheimer Landstr. 24
60323 Frankfurt am Main
T +49 69 710003 - 0
F +49 69 710003 - 144
frankfurt@gsk.de

MUNICH
Karl-Scharnagl-Ring 8
80539 Munich
T +49 89 288174 - 0
F +49 89 288174 - 44
muenchen@gsk.de

HAMBURG
Neuer Wall 69
20354 Hamburg
T +49 40 369703-0
F +49 40 369703-44
hamburg@gsk.de

LUXEMBOURG
GSK Stockmann SA
44, Avenue John F. Kennedy
L - 1855 Luxembourg
T +352 271802 - 00
F +352 271802 - 11
luxembourg@gsk-lux.com

LONDON
GSK Stockmann International
Rechtsanwaltsgesellschaft mbH,
London branch
Queens House, 8-9 Queen Street
London EC4N 1SP
United Kingdom
T +44 20 4512687-0
london@gsk-uk.com

Registered office: Munich
Munich Local Court
HRB 281930
Managing directors:
Dr. Mark Butt, York-Alexander
von Massenbach

YOUR PERSPECTIVE.
GSK.DE | GSK-LUX.COM