



Identomat

COMPLIANCE GUIDE

Banking & Digital Banking Compliance in Germany

COUNTRY **Germany**

INDUSTRY **Banking & Digital Banking**

LAST UPDATED **29 October 2026**

KEY REGULATORS **Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) · European Central Bank · Financial Intelligence Unit (FIU)**

Key takeaways

- Taking deposits or lending in Germany needs a banking licence. Applications go to the German financial supervisor, BaFin; for a full bank the European Central Bank (ECB) makes the decision, normally within six months of a complete application, and at least EUR 5 million of starting capital is required. Banks licensed elsewhere in the European Economic Area can passport in instead.
- Every new customer must be identified and verified before the account is opened. If a bank cannot complete these checks, it must not open the account and must close existing ones.
- Online, German law allows only a short list of remote methods: the electronic ID function of the German identity card (eID), a qualified electronic signature combined with a first transfer from the customer's own bank account, an EU-notified electronic ID, or live video identification run to BaFin's rules. A photo of an ID card plus a selfie is not, on its own, an accepted method today.
- Banks must register with the Financial Intelligence Unit (FIU) whether or not they ever file, report suspicious activity electronically without delay and regardless of amount, and hold a reported transaction for up to three working days.
- The EU Anti-Money Laundering Regulation applies directly from 10 July 2027 and will replace most of the German rules on customer checks. The EU anti-money laundering authority, AMLA, sent detailed draft standards on remote verification to the European Commission on 1 October 2026; they are not yet law. A German law passed by the Bundestag in October 2026, still awaiting the Bundesrat, would also accept the EU Digital Identity Wallet.

Germany is open to digital banks: remote account opening is an established practice, regulated in detail by statute and BaFin guidance. The framework is strict and prescriptive, however. The Money Laundering Act (Geldwäschegesetz, GwG) lists the documents and procedures that may be used to verify a customer, and anything outside that list needs a federal ordinance that has never been issued.

The principal authorities are BaFin (licensing work, prudential and anti-money laundering supervision), the ECB (licence decisions and supervision of significant banks), the Deutsche Bundesbank (supervision and financial sanctions) and the FIU. The biggest obstacle for a new entrant is building a remote onboarding journey, and the monitoring behind it, that meets BaFin's detailed expectations from day one: BaFin's recent enforcement has targeted late suspicious activity reports, weak transaction monitoring and backlogs in updating customer data.

CONTENTS

- 1 Who regulates this sector
- 2 Licensing and authorisation
- 3 AML, KYC and customer due diligence
- 4 Identity verification and onboarding
- 5 Digital channels: what's different
- 6 Data protection and biometrics
- 7 Sector-specific obligations
- 8 Risk indicators and red flags
- 9 Enforcement and penalties
- 10 Recent changes and what to watch
- 11 What this means for identity verification
 - Sources

1 Who regulates this sector

Authority	Remit for banks	Level	Official site
BaFin	Receives licence applications; prudential supervision; anti-money laundering (AML) supervisor for credit, financial services, payment and e-money institutions (GwG § 50 No 1)	Federal	bafin.de
European Central Bank	Grants and withdraws licences for all credit institutions; directly supervises significant banks (Regulation (EU) No 1024/2013, arts. 4 and 14)	EU	eur-lex.europa.eu

Deutsche Bundesbank	Ongoing supervision with BaFin; Servicezentrum Finanzsanktionen implements financial sanctions	Federal	bundesbank.de
Financial Intelligence Unit (Zentralstelle für Finanztransaktionsuntersuchungen)	Receives suspicious activity reports through goAML; part of the customs administration	Federal	zoll.de
Transparenzregister	Beneficial ownership register; banks inspect it and report discrepancies	Federal	transparenzregister.de
AMLA	EU AML rulebook (standards and guidelines, took over the European Banking Authority's AML mandates on 1 January 2026); future direct supervision of selected groups	EU	amla.europa.eu
Federal and state data protection authorities	Processing of identity and biometric data under the GDPR	Federal and state	datenschutzkonferenz-online.de

Licensing and authorisation

Anyone who conducts banking business in Germany commercially, or on a scale that requires a commercially organised operation, needs a written or electronic licence under § 32(1) of the Banking Act (Kreditwesengesetz, KWG; as last amended on 12 May 2026). Banking business (§ 1(1) KWG) includes deposit-taking, lending and securities custody. Under the Single Supervisory Mechanism the application is filed with the national authority, and the ECB is exclusively competent to grant the licence (Regulation (EU) No 1024/2013, arts. 4(1)(a) and 14).

BaFin remains the applicant's sole point of contact and forwards the ECB's decision; for banking business that does not include both deposit-taking and lending, BaFin decides alone.

The application must include proof of funds, details of the managing directors' reliability, qualification and time commitment, and a viable business plan (§ 32(1) KWG). BaFin expects at least two qualified managing directors, and a licence must be refused if a CRR credit institution lacks at least EUR 5 million of Common Equity Tier 1 initial capital in Germany (§ 33(1) No 1(d) KWG). The applicant must be told within six months of a complete application whether the licence is granted; an application still incomplete twelve months after filing is rejected (§ 33(4) KWG).

Banks authorised in another EEA state may passport in through a branch or cross-border services (§ 53b KWG).

Conducting banking business without a licence is a criminal offence punishable by up to five years' imprisonment or a fine, and up to three years for negligence (§ 54(1) No 3 and (5) KWG). Deposits are covered by statutory deposit guarantee up to EUR 100,000 per depositor (§ 8 Deposit Guarantee Act, EinSiG).

AML, KYC and customer due diligence

Credit institutions, financial services institutions and investment firms (the securities side) are obliged entities under GwG § 2(1) Nos 1 and 2 (GwG as last amended on 29 June 2026). They must apply customer due diligence (CDD) when establishing a business relationship, for occasional funds transfers of EUR 1,000 or more, for other occasional transactions of EUR 15,000 or more, whenever facts suggest money laundering or terrorist financing, and when they doubt identity data already held (§ 10(3)). All new customers must be subject to CDD; existing customers at appropriate times on a risk basis, in particular when relevant circumstances change (§ 10(3a)).

Core CDD elements

Identify the customer and any person acting for them, establish whether a beneficial owner exists and understand the ownership and control structure, obtain the purpose of the relationship, screen for politically exposed persons (PEPs), and monitor the relationship with risk-based updates of customer data (§ 10(1)).

Beneficial ownership

A beneficial owner holds or controls more than 25% of capital or votes, or exercises comparable control (§ 3(2)). Data must be collected from the customer; a Transparenzregister extract alone is not enough (§ 11(5)). Discrepancies with the register must be reported without delay (§ 23a).

Enhanced due diligence

Required for PEPs (for at least 12 months after leaving office), high-risk third countries, unusually complex or large transactions and cross-border correspondent relationships, with senior management approval, source-of-funds measures and enhanced monitoring (§ 15).

Cash

BaFin's guidance for credit institutions (June 2021) treats walk-in cash transactions above EUR 2,500 as higher risk: the source of funds must be documented before execution or the cash refused. Cash above EUR 10,000 within a relationship needs documentary proof of origin.

Tax identification. Banks must also record the tax identification number of every account holder, authorised person and beneficial owner (§ 154(2a) Fiscal Code).

Monitoring and reporting. Credit institutions must operate data-processing systems that detect unusual relationships and payment transactions (§ 25h(2) KWG). Facts suggesting that assets derive from a predicate offence or relate to terrorist financing must be reported to the FIU without delay, regardless of amount (GwG § 43(1)). Reports are electronic through goAML, and every obliged entity must register with the FIU whether or not it files (§ 45(1)). A reported transaction may be executed only with FIU or prosecutor consent or after the third working day following dispatch, Saturdays excluded (§ 46(1)). Tipping off the customer is prohibited (§ 47).

Records. Records, including copies or digital captures of identity documents and video and audio recordings made for CDD, are kept for five years and destroyed after ten years at the latest (§ 8(2) and (4)).

For a natural person the bank collects first and last name, place and date of birth, nationality and residential address (GwG § 11(4)) and verifies them before the relationship is established, unless completion during onboarding is necessary and the risk is low (§ 11(1)). Verification is permitted only on the basis of the means in § 12(1):

- a valid official photo ID that satisfies the German passport and identity card obligation (German ID card or passport, EU citizens' ID cards, recognised foreign passports and replacement documents);
- the electronic proof of identity under § 18 of the Identity Card Act (PAuswG), the eID card for EU citizens, or the electronic residence permit;
- a qualified electronic signature, validated under eIDAS article 32, plus a payment made directly from an account in the customer's name at an EU, EEA or equivalent institution (the "reference transfer");
- an electronic identification scheme notified under eIDAS articles 8(2)© and 9;
- for basic and minors' payment accounts, the documents listed in the Payment Account Identity Verification Ordinance (ZIdPrüfV).

§ 13(1) allows either an appropriate check of the document presented on site or another procedure with an equivalent security level. BaFin's interpretive guidance (Auslegungs- und Anwendungshinweise, July 2025, section 5.1.3.2) states that the eID, the qualified signature route and notified schemes are equivalent procedures, that further procedures may only be approved by ordinance under § 13(2), and that no such ordinance or trial procedure had been issued. Documents must be presented in the original unless a legal exception applies.

Video identification

Entities supervised by BaFin may also use video identification under Circular 3/2017 (GW) of 10 April 2017, which BaFin confirms still applies. Trained staff in access-controlled rooms run a live, encrypted session; only IDs with white-light security features and a machine-readable zone qualify; staff check at least three random security features; a one-time code sent by email or SMS is entered during the call; and the session is recorded. Legal persons cannot be identified by video, although their representatives can. Sub-outsourcing of video identification is not allowed.

Reliance and outsourcing

A bank may rely on CDD by another EEA obliged entity, keeping responsibility (§ 17(1)), including reuse of an identification no more than 24 months old (§ 17(3a)), or outsource

identification by contract to vetted, sampled providers (§ 17(5) to (7)). BaFin's guidance names Deutsche Post's PostIdent as a suitable procedure under these rules.

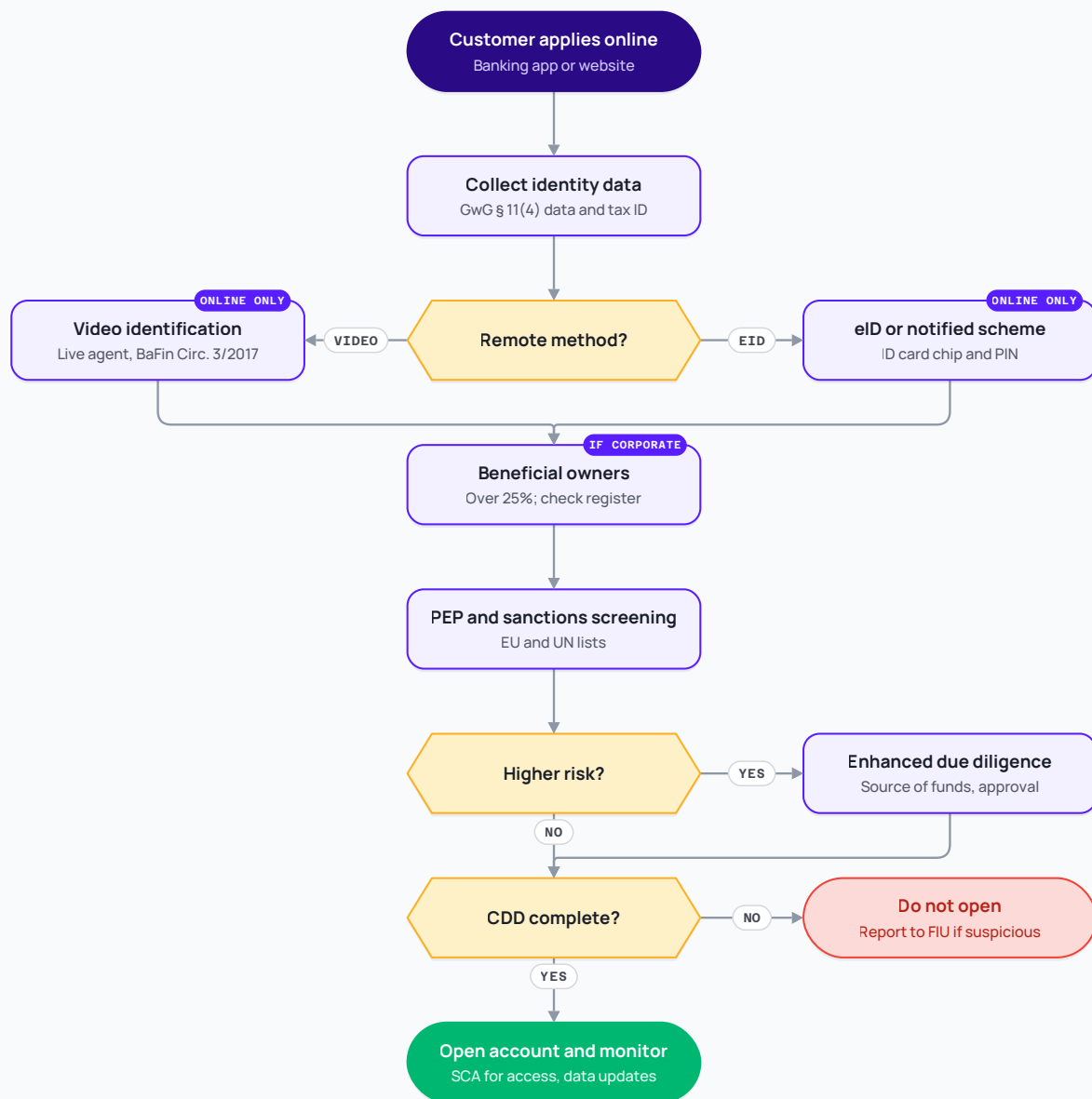


Figure 1. Remote retail account opening at a German bank under the GWG and BaFin Circular 3/2017.

Bottom line: the duty to identify and verify is the same in a branch and in an app, but online a bank may use only the remote means the GwG lists or video identification under BaFin's circular; automated document and selfie checks are not yet an accepted stand-alone method.

Requirement	In person / branch	Online / remote	Difference
Data to collect	GwG § 11(4) data	Same data	Same
When to verify	Before the relationship (§ 11(1))	Before the relationship	Same
Verification method	Original photo ID checked on site (§ 13(1) No 1)	eID, QES plus reference transfer, notified eID, or BaFin video identification	Differs
Accepted ID documents	Any ID meeting the German passport and ID obligation	Video: only IDs with white-light security features and a machine-readable zone	Differs
Risk classification	Risk-based	Non-face-to-face without eID, trust services or approved remote procedures is a higher-risk factor (GwG Annex 2 No 2©)	Differs
Evidence kept	ID copy or digital capture	Plus full audio-visual recording and screenshots for video identification	Differs
Outsourcing	Contractual outsourcing allowed (§ 17(5))	Allowed; no sub-outsourcing for video identification	Differs
Account access	Branch authentication	Strong customer authentication for online access and remote payments (ZAG § 55)	Differs
Suspicious activity reporting	FIU via goAML (§§ 43, 45)	Same	Same

A fixed list, not a principle

The GwG does not ask whether a remote method is "reliable"; it names the permitted means in § 12(1) and allows other equivalent procedures only by federal ordinance (§ 13(2)). The Federal Ministry of Finance published a draft ordinance on video identification (GwVideoidentV) on 18 April 2024 **Draft, not adopted** ; no such ordinance has been promulgated in the Federal Law Gazette as of October 2026, so Circular 3/2017 continues to set the rules.

Remote is not automatically high risk

GwG Annex 2 treats relationships without personal contact as a potentially higher-risk factor only where safeguards such as electronic identification or eIDAS trust services are missing. Video identification counts as identification among those present. BaFin has notified the EBA that it complies, since 14 March 2024, with the EBA remote onboarding guidelines (EBA/GL/2022/15), which expect liveness detection wherever a remote solution runs without a staff member.

Account security

Strong customer authentication is required for online account access, electronic payments and risky remote actions; remote payments need dynamic linking to amount and payee (§ 55 ZAG).

What changes next

The Digital Identities Act (DIdG, BT-Drs. 21/7408), passed by the Bundestag on 15 October 2026, would add the EU Digital Identity Wallet to the § 12(1) list and drop the reference-transfer requirement for the qualified signature route

Passed Bundestag, awaiting Bundesrat . Germany's state wallet, d-you, is scheduled to launch on 2 January 2027. From 10 July 2027 the EU Anti-Money Laundering Regulation (AMLR) requires verification either by an identity document plus reliable independent sources where relevant, or by eIDAS electronic identification at "substantial" or "high" assurance (art. 22(6)) **Adopted, applies 10 Jul 2027** . AMLA's final draft standards on CDD, submitted to the European Commission on 1 October 2026, allow alternative remote solutions only where neither route is available, with safeguards on document-holder matching, data quality and process interruption **Final draft, not adopted** .

Data protection and biometrics

The GwG gives banks both the right and the duty to copy or digitally capture the ID document (§ 8(2)), so that step does not rest on consent. Video identification adds one: Circular 3/2017 requires explicit, logged consent to recording.

Biometric face matching is a different matter. The German data protection authorities' position paper on biometric analysis (version 1.0 of 3 April 2019, adopted against the votes of Bavaria and Baden-Württemberg) treats biometric processing for unique identification as prohibited in principle under GDPR article 9(1) unless an exception applies, typically explicit consent that refers expressly to the biometric data and is freely given. Banks using automated face matching should therefore obtain specific consent and offer a non-biometric route such as the eID.

Sector-specific obligations

Account register for authorities

Every credit institution must maintain a file of account, securities account and safe-deposit box numbers with holder, authorised person and beneficial owner data, which BaFin and the FIU can retrieve automatically without the bank's knowledge (§ 24c KWG).

Correspondent banking and virtual IBANs

Correspondent relationships with third-country respondents require enhanced due diligence (GwG § 15(3) No 4). BaFin's supervisory notice 06/2026 on virtual IBANs (27 July 2026, valid until 10 July 2027) requires account-holding banks to obtain transparency on end customers behind vIBAN structures, record them in the § 24c account file and check regularly whether enhanced due diligence is needed.

Risk indicators and red flags

The FIU received 374,693 suspicious activity reports in 2025; digital financial service providers accounted for 29%, up from 13% in 2022, reflecting fast, remote and often cross-border account opening (FIU Annual Report 2025).

BANKING RED FLAGS FROM BAFIN, THE FIU AND THE GWG

- **viBAN layering**: many virtual IBANs feeding one master account of a foreign, especially third-country, payment provider.
- **Shell company inflows**: high receipts from newly formed firms sharing an address or with generic websites.
- **Vague payment references**: generic purposes such as "payment for goods" on high volumes.
- **Rapid pass-through**: short-lived accounts or funds moving out almost as fast as they arrive.
- **Fragmented routes**: several intermediary payment providers and complex international payment chains.
- **Walk-in cash**: occasional cash above EUR 2,500 without a credible source of funds.
- **Opaque ownership**: nominee shareholders or structures unusually complex for the business.
- **Transaction laundering**: sham merchant accounts used to push fraudulent card payments into the payment system.

9

Enforcement and penalties

GwG § 56 sets tiered administrative fines. Ordinary breaches carry up to EUR 150,000 if intentional, otherwise EUR 100,000; serious, repeated or systematic breaches up to EUR 1 million or twice the economic benefit; and for financial-sector legal persons up to the higher of EUR 5 million or 10% of prior-year total turnover. BaFin publishes final measures (§ 57 GwG) and may order remediation (§ 51(2)).

- **J.P. Morgan SE**: EUR 45 million fine (final 30 October 2025) for systematically late suspicious activity reports between October 2021 and September 2022. [BaFin, 6 November 2025](#)
- **Helaba**: order to remedy failures in customer identification, data updates, risk analysis and transaction monitoring. [BaFin, 20 July 2026](#)
- **Norddeutsche Landesbank**: order (final 14 June 2026) to remedy serious deficiencies and a backlog in updating customer data. [BaFin, 3 August 2026](#)
- **Deutsche Bank AG**: new deadlines (final 6 October 2026) to fix transaction monitoring systems under § 25h KWG. [BaFin, 9 October 2026](#)

Recent changes and what to watch

- **15 October 2026:** **Passed Bundestag, awaiting Bundesrat** The Digital Identities Act would accept the EU Digital Identity Wallet for GwG verification and remove the reference transfer for qualified signatures, from the day after promulgation.
- **9 October 2026:** **Bill, not enacted** The Bundestag held the first reading of the government bill on strengthening customs and combating financial crime (BT-Drs. 21/8282), which amends the GwG on the FIU, Transparenzregister access and state supervision. Most provisions would apply from 1 January 2027, the GwG amendments from the day after promulgation.
- **1 October 2026:** **Final draft, not adopted** AMLA submitted final draft standards on CDD, including non-face-to-face verification, to the Commission; proposed to apply six months after entry into force.
- **27 July 2026:** **In force** BaFin supervisory notice 06/2026 on virtual IBAN risks applies until 10 July 2027.
- **1 January 2026:** **In force** AMLA took over the European Banking Authority's AML mandates; existing guidelines, including the remote onboarding guidelines (EBA/GL/2022/15), stay in force until replaced.
- **10 July 2027:** **Adopted, applies 10 Jul 2027** The AMLR applies directly, with five-year maximum intervals for updating standard-risk customer data and one year for higher-risk customers (art. 26(2)).

What this means for identity verification

- **Design around the legal list.** Offer eID (card chip and PIN, or smart eID on a phone, for holders aged 16 and over) and BaFin-compliant video identification; add the qualified signature route where useful, noting that the reference transfer may soon be dropped.
- **Biometrics.** Use face matching to support, not replace, a permitted method until the AMLR and AMLA standards apply, and obtain explicit biometric consent.
- **Evidence.** Store ID captures, recordings, screenshots and one-time code logs for five years after the relationship ends, and delete them within ten.
- **Re-verification.** Plan risk-based data updates now; BaFin is enforcing backlogs, and the AMLR will cap update intervals at one and five years.
- **Prepare for wallets.** Plan for the EU Digital Identity Wallet now; eIDAS "substantial" or "high" electronic identification becomes a standard route under AMLR art. 22(6).

How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- Video KYC with agent-led sessions, recording and audit trail for remote account opening.
- ID document capture and verification, including NFC chip reading, with face match and biometric liveness.
- KYB and beneficial owner verification for corporate customers.
- AML screening against sanctions, PEP and adverse-media lists, with ongoing monitoring.
- No-code workflow builder with cloud, on-premises or hybrid deployment.

[Request a meeting](#)

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- Geldwäschegesetz (GwG) [Money Laundering Act], §§ 2, 3, 8, 10, 11, 12, 13, 14, 15, 17, 23a, 43, 45, 46, 47, 50, 56 and Annex 2, as last amended by Art. 12(4) of the Act of 29 June 2026 (BGBl. 2026 I Nr. 197), Gesetze im Internet, [gesetze-im-internet.de/gwg_2017](https://www.gesetze-im-internet.de/gwg_2017)
- Kreditwesengesetz (KWG) [Banking Act], §§ 1, 24c, 25h, 32, 33, 53b, 54, as last amended by Art. 9 of the Act of 12 May 2026 (BGBl. 2026 I Nr. 139), [gesetze-im-internet.de/kredwg](https://www.gesetze-im-internet.de/kredwg)
- Einlagensicherungsgesetz (EinSiG) [Deposit Guarantee Act], § 8, [gesetze-im-internet.de/einsig/___8.html](https://www.gesetze-im-internet.de/einsig/___8.html)
- Abgabenordnung (AO) [Fiscal Code], § 154, [gesetze-im-internet.de/ao_1977/___154.html](https://www.gesetze-im-internet.de/ao_1977/___154.html)
- Zahlungsdiensteaufsichtsgesetz (ZAG) [Payment Services Supervision Act], § 55, [gesetze-im-internet.de/zag_2018/___55.html](https://www.gesetze-im-internet.de/zag_2018/___55.html)

- Personalausweisgesetz (PAuswG) [Identity Card Act], § 18, gesetze-im-internet.de/pauswg/_18.html
- BaFin, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz [Interpretive guidance on the GwG], Stand July 2025, sections 5.1.3.2 and 8, [bafin.de](https://www.bafin.de)
- BaFin, Auslegungs- und Anwendungshinweise, Besonderer Teil: Kreditinstitute [Guidance for credit institutions], Stand June 2021, section 1, [bafin.de](https://www.bafin.de)
- BaFin, Rundschreiben 3/2017 (GW): Videoidentifizierungsverfahren [Circular on video identification], 10 April 2017, [bafin.de](https://www.bafin.de)
- BaFin, Aufsichtsmitteilung 06/2026 (A): Risiken virtueller IBANs [Supervisory notice on virtual IBANs], 27 July 2026, [bafin.de](https://www.bafin.de)
- BaFin enforcement notices: J.P. Morgan SE (6 November 2025), [bafin.de](https://www.bafin.de); Nord/LB (3 August 2026), [bafin.de](https://www.bafin.de); Deutsche Bank AG (9 October 2026), [bafin.de](https://www.bafin.de)
- BaFin, Erlaubnis für Bankgeschäfte [Licensing of banking business], [bafin.de](https://www.bafin.de)
- BaFin enforcement notice, Landesbank Hessen-Thüringen (Helaba), 20 July 2026, [bafin.de](https://www.bafin.de)
- Deutscher Bundestag, Drucksache 21/7408, Digitale Identitätengesetz (DIdG), government bill, 29 July 2026, art. 6, [bundestag.de](https://www.bundestag.de); committee report Drucksache 21/8617, 14 October 2026, [bundestag.de](https://www.bundestag.de)
- Federal Ministry for Digital Affairs and State Modernisation, EUDI-Wallet d-you, bmds.bund.de
- FIU, Jahresbericht 2025 [Annual Report 2025], published 21 July 2026, [zoll.de](https://www.zoll.de)
- EBA, compliance table for EBA/GL/2022/15, Germany (BaFin): complies as of 14 March 2024, eba.europa.eu
- Lobbyregister, GwVideoidentV draft (BMF, 18 April 2024), lobbyregister.bundestag.de
- Deutscher Bundestag, Drucksache 21/8282, government bill on customs and financial crime, 30 September 2026, [bundestag.de](https://www.bundestag.de); first reading 9 October 2026, [bundestag.de](https://www.bundestag.de)
- FIU, Software goAML, [zoll.de](https://www.zoll.de)
- Deutsche Bundesbank, Finanzsanktionen, [bundesbank.de](https://www.bundesbank.de)
- Datenschutzkonferenz, Positionspapier zur biometrischen Analyse [Position paper on biometric analysis], version 1.0, 3 April 2019, datenschutzkonferenz-online.de
- Regulation (EU) 2024/1624 (AMLR), arts. 22, 26 and 90, EUR-Lex, eur-lex.europa.eu
- Council Regulation (EU) No 1024/2013 (SSM Regulation), arts. 4 and 14, EUR-Lex, eur-lex.europa.eu
- AMLA, "AMLA finalises key standards for the private sector", 1 October 2026, and Final Report on draft RTS under Article 28(1) AMLR, 30 September 2026, art. 7, amla.europa.eu
- AMLA, "EBA and AMLA complete handover of AML/CFT mandates", 19 January 2026, amla.europa.eu
- EBA, Guidelines on the use of remote customer onboarding solutions (EBA/GL/2022/15), 22 November 2022, applicable from 2 October 2023, paras. 39 to 41, eba.europa.eu