



Identomat

COMPLIANCE GUIDE

Crypto & Virtual Assets Compliance in Germany

COUNTRY **Germany**

INDUSTRY **Crypto & Virtual Assets**

LAST UPDATED **29 October 2026**

KEY REGULATORS **Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) · Financial Intelligence Unit (FIU) · Deutsche Bundesbank**

Key takeaways

- Any business offering crypto exchange, custody, trading or transfer services to people in Germany needs an EU crypto licence under the Markets in Crypto-Assets Regulation (MiCA), granted in Germany by the financial supervisor BaFin. The German grace period for older licences ended on 31 December 2025, and the EU-wide one on 1 July 2026.
- A firm licensed in another EU country can serve German customers after notifying its home regulator. A firm outside the EU that targets German residents online without a licence commits a criminal offence.
- Every customer must be identified and verified before the account opens. Online, only a short list of methods set by law is accepted: the German electronic ID, an EU-recognised electronic ID, a qualified electronic signature combined with a bank transfer from the customer's own account, or BaFin-style live video identification. A photo upload alone is not enough.
- Every crypto transfer must carry the sender's and recipient's identity data, with no minimum amount. Transfers to or from a customer's own private wallet need extra risk checks, and above EUR 1,000 the firm must assess whether the customer owns or controls that wallet.
- Since 2026 crypto firms must also collect customers' tax residence and report them to the Federal Central Tax Office every year. Existing customers must be covered by 1 January 2027. From 10 July 2027 new EU anti-money laundering rules apply directly and ban accounts in privacy coins.

Germany is open to crypto businesses, but only through MiCA authorisation or an EU passport. The Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) licenses and supervises crypto-asset service providers and is also their anti-money laundering supervisor. Suspicious activity goes to the Financial Intelligence Unit (FIU), financial sanctions are administered by the Deutsche Bundesbank, and tax reporting goes to the Bundeszentralamt für Steuern.

For a new entrant the hardest part is usually not the licence itself but building onboarding that satisfies Germany's narrow list of accepted remote verification methods, together with Travel Rule messaging and self-hosted wallet controls that must work before the first transfer leaves the platform.

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 crypto businesses	Level	Official site
Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)	MiCA authorisation and supervision of crypto-asset service providers (CASPs) and token issuers; anti-money laundering (AML) supervision; enforcement against unauthorised business	Federal	bafin.de
Deutsche Bundesbank	Receives a copy of every CASP application (competence centre for payment and crypto supervision); Servicezentrum Finanzsanktionen administers financial sanctions	Federal	bundesbank.de
Financial Intelligence Unit (Zentralstelle für Finanztransaktionsuntersuchungen)	Receives suspicious activity reports; every obliged entity must register electronically	Federal	zoll.de

Bundeszentralamt für Steuern (BZSt)	Receives annual crypto tax reports and fines breaches of the Crypto-Asset Tax Transparency Act	Federal	KStTG
European Securities and Markets Authority (ESMA)	Interim MiCA register of authorised and notified CASPs, token white papers and non-compliant entities	EU	esma.europa.eu
Anti-Money Laundering Authority (AMLA)	EU AML authority; issues advisory notes and future standards under the AML Regulation	EU	amla.europa.eu

Federal and state data protection authorities supervise onboarding data.

2 Licensing and authorisation

Who needs authorisation. MiCA (Regulation (EU) 2023/1114) applies to crypto-asset services from 30 December 2024 (Article 149). Only CASPs authorised under Article 63, or financial institutions that notify under Article 60, may provide them (Article 59). BaFin's guidance notice (January 2025) requires authorisation for commercial services provided "in Germany": through a seat, branch or other presence here, or by targeting German residents from abroad online. Reverse solicitation (Article 61) is narrow.

Transition. Under § 50 of the Kryptomärkteaufsichtsgesetz (KMAG), holders of German banking, securities, payment, exchange or fund licences providing crypto services on 29 December 2024 could continue at the latest until 31 December 2025. The EU-wide transitional period ended on 1 July 2026.

Full CASP authorisation

Application to BaFin under Article 62 using the forms in Implementing Regulation (EU) 2025/306, with evidence of compliance with the Digital Operational Resilience Act (DORA). A copy goes to the Bundesbank.

Notification route

Credit institutions, investment firms, e-money institutions, fund managers, central securities depositories and market operators may provide crypto services equivalent to their existing licence, within the limits of Article 60, after notifying BaFin at least 40 working days in advance.

EU passport

A CASP authorised elsewhere in the EU notifies its home authority; it may start in Germany when informed that the notice was passed on, or at the latest 15 calendar days after submitting it (Article 65).

Process and capital. BaFin checks completeness within 25 working days and decides within 40 working days of a complete application (Article 63); it normally allows four weeks for missing documents and charges fees by time spent. Minimum capital (Annex IV) is EUR 50,000 (class 1, e.g. order execution, transfer services, advice), EUR 125,000 (class 2, adding custody and exchange) or EUR 150,000 (class 3, trading platforms). A CASP needs a registered office in a Member State where it provides at least part of its services, effective management in the EU and at least one EU-resident director (Article 59(2)). On 22 October 2026 ESMA's interim register listed 117 entries with Germany as home state: 8 authorised under Article 63 and 109 notified under Article 60.

Unauthorised business is a crime under § 46 KMAG: up to five years' imprisonment or a fine (three years if negligent).

3

AML, KYC and customer due diligence

Scope. CASPs and some issuers of asset-referenced tokens (ARTs) are obliged entities under § 2(1) No. 2 of the Geldwäschegesetz (GwG, Money Laundering Act; last amended 29 June 2026). Firms offering only crypto advice are excluded (§ 1(31)); ART issuers authorised under Article 21 MiCA are covered unless they offer and list their tokens exclusively through a CASP (§ 1(32)).

When due diligence applies. Under § 10(3) GwG: on opening a relationship; for occasional crypto transfers of EUR 1,000 or more; for other occasional transactions of EUR 15,000 or more; on suspicion; and on doubts about identity data. Transfers are valued at execution at the current price on any CASP authorised in Germany (BaFin guidance, 4.2.3), and linked transactions count together.

Content. Identify the customer and anyone acting for them, establish beneficial owners (more than 25% of capital or votes), obtain the purpose, check for politically exposed persons (PEPs) and monitor on a risk basis (§ 10(1)); otherwise refuse or terminate (§ 10(9)).

Enhanced due diligence (§ 15) applies to PEPs, their family and close associates (for at least 12 months after leaving office), links to EU-listed high-risk third countries and unusual transactions. Cross-border correspondent relationships between CASPs require information on the respondent's authorisation (§ 15(7)).

Reporting. Suspicious activity is reported to the FIU without delay, regardless of amount (§ 43(1)), electronically; every obliged entity must register with the FIU whether or not it files (§ 45(1)). A reported transaction may proceed only with FIU or prosecutor consent or after the third working day, Saturdays excluded (§ 46(1)). Since 1 March 2026 the GwG Reporting Ordinance (GwGMeldV) requires structured reports with mandatory fields; for crypto cases these include the CASP's name, the account holders, the blockchain transaction ID and the amount in crypto units with the exchange rate.

Sanctions. EU sanctions regulations apply directly. The Bundesbank's Servicezentrum Finanzsanktionen polls crypto custodians and banks after new listings; frozen assets must be reported, or a nil return filed. Since 23 April 2026, transactions with Russia-based crypto service providers and platforms are banned (Article 5bb of Regulation (EU) No 833/2014).

Records. Kept five years and destroyed after ten at the latest (§ 8(4)). Firms must copy or fully digitise identity documents, and video and audio recordings made for CDD are records (§ 8(2)).

4 Identity verification and onboarding

Data to collect. For individuals: first and last name, place and date of birth, nationality and residential address (§ 11(4) GwG). Identification must be complete before the relationship starts; completion during onboarding is allowed only where needed for normal business and the risk is low (§ 11(1)).

Accepted verification means. § 12(1) GwG lists the only evidence that may be used for individuals:

Means (§ 12(1) GwG)	How it works online	Conditions
No. 1: valid official photo ID meeting German passport and ID rules	Checked on site, or remotely through BaFin video identification	Original document; video identification under BaFin circular 3/2017
No. 2: electronic proof of identity (German ID card, eID card for EU citizens, electronic residence permit)	Chip read with PIN through an authorised eID service	Treated as equivalent to an on-site check
No. 3: qualified electronic signature (QES)	QES plus a "reference transfer"	Firm validates the QES under Article 32 eIDAS and receives a payment directly from an account in the customer's name at a supervised EU/EEA (or equivalent) institution
No. 4: eIDAS-notified electronic identification scheme	Another Member State's notified eID	Notified under Articles 8 and 9 eIDAS
No. 5: documents under the payment-account identification ordinance (ZIdPrüfV)	Limited cases, e.g. minors via birth certificate plus verified legal representative	Narrow; mainly relevant to payment accounts

Under § 13(1) GwG verification is an adequate on-site check of the document or a procedure of equivalent security. BaFin's guidance (July 2025, 5.1.3.2) treats the eID, QES and notified eID as equivalent, keeps circular 3/2017 in force for video identification by BaFin-supervised entities, and notes that further remote procedures need a Federal Ministry of Finance ordinance, of which none had been issued. Documents must be presented in the original, so an uploaded photo of an ID card does not by itself verify identity.

Video identification (circular 3/2017), open under BaFin's guidance to all BaFin-supervised entities, including CASPs, requires trained staff in access-controlled rooms, explicit recorded consent, an end-to-end encrypted live session, IDs with white-light security features and a machine-readable zone, checks of at least three randomly selected security features, automated check-digit validation, a one-time code (TAN) sent by email or SMS and entered during the session, and full audio-visual recording kept for five years. Sub-outsourcing is not allowed.

Reliance and outsourcing. A firm may rely on another obliged entity, or outsource identification to a provider by contract, but remains responsible (§ 17(1) and (5)). Ongoing monitoring and enhanced due diligence cannot be delegated (BaFin guidance, 8). Since 1 July 2026 the Crypto Markets Notification Ordinance (KMAnzV, § 5) sets the content of the notice a CASP must give BaFin before and after a material outsourcing, including the data transferred and where it is stored.

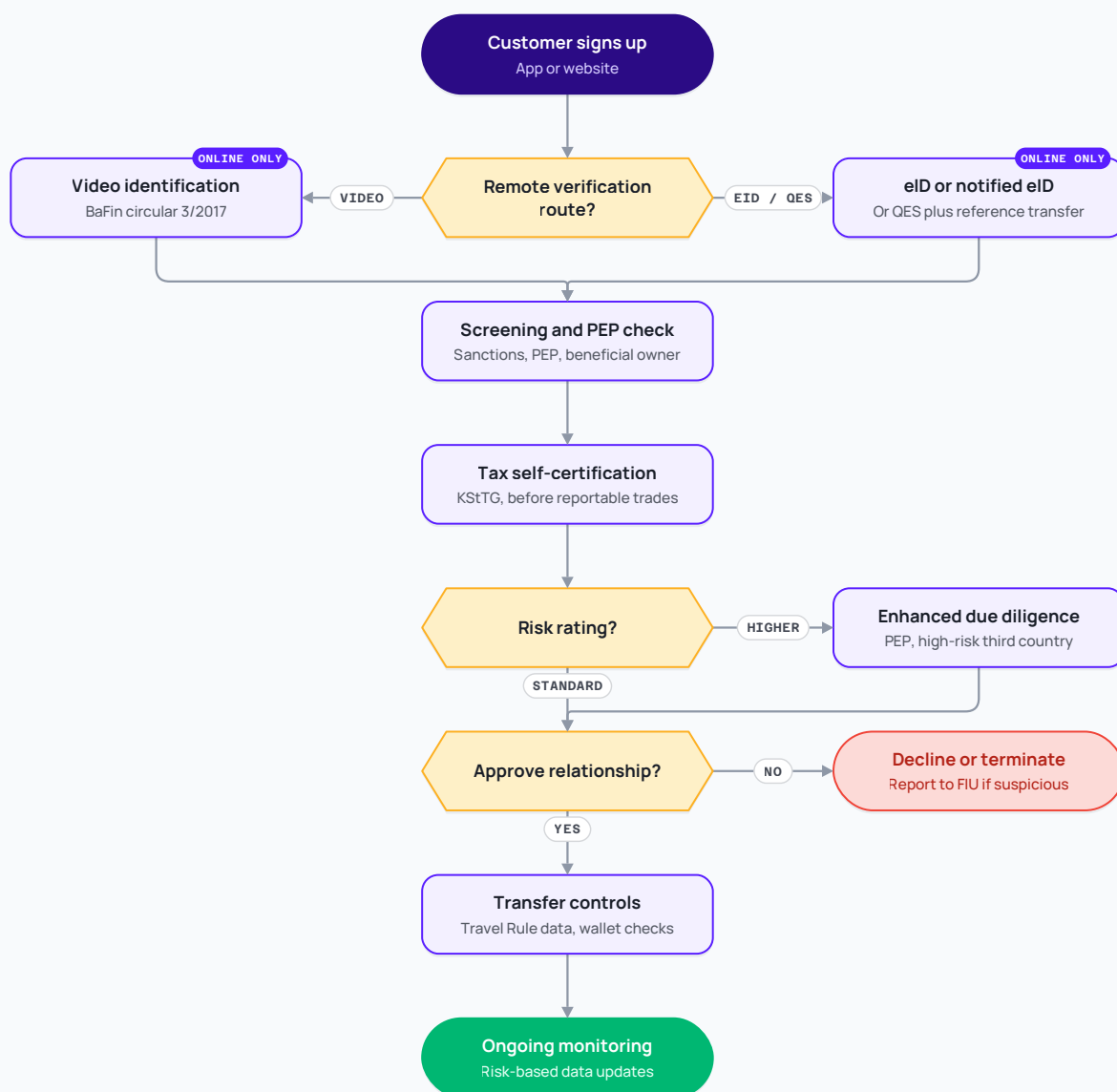


Figure 1. Remote customer onboarding for a crypto-asset service provider in Germany.

Bottom line: the licence and the due diligence duties are the same online and in person, but a remote customer can only be verified through a short statutory list of electronic methods or BaFin-compliant video identification, and an online offer aimed at German residents from abroad counts as business in Germany.

Requirement	In person (e.g. crypto ATM, office)	Online / remote	Difference
Authorisation	MiCA authorisation or passport	MiCA authorisation or passport	Same
When CDD is triggered	New relationship; occasional crypto transfer of EUR 1,000 or more	Same triggers	Same
Verification method	On-site check of original photo ID	eID, notified eID, QES plus reference transfer, or video identification	Differs
Risk treatment	Standard risk-based approach	Remote contact without electronic identification safeguards is a higher-risk factor (GwG Annex 2)	Differs
Evidence kept	Copy or scan of the ID	ID capture plus full audio-visual recording for video identification	Differs
Biometric data	Not required	Face images in video sessions are biometric data when used to identify	Differs
Territorial reach	Seat, branch or physical presence	Cross-border online offer targeting German residents also requires authorisation	Differs
Travel Rule and self-hosted wallets	Apply to every transfer	Apply to every transfer	Same

A fixed list, not a free choice of method

§§ 12(1) and 13 GwG fix the permitted evidence. Document-and-selfie checks with automated liveness are not on the list, so video identification and the eID chip are the practical online routes.

Remote contact as a risk factor

GwG Annex 2 treats non-face-to-face relationships without safeguards such as electronic identification as a higher-risk factor.

Online offers from abroad

An app or website aimed at German residents is business in Germany, so capture country of residence early.

Adopted, applies 10 Jul 2027 Under Article 22(6) of Regulation (EU) 2024/1624 (AMLR), identity may be verified by an identity document plus reliable independent sources where relevant, or by eIDAS electronic identification at assurance level "substantial" or "high".

6 Data protection and biometrics

The General Data Protection Regulation (GDPR) governs onboarding data; the GwG supplies the legal basis for copying ID documents and caps retention (§ 8).

The Datenschutzkonferenz position paper on biometric analysis (3 April 2019, adopted against the votes of Bavaria and Baden-Württemberg) holds that biometric identification is prohibited under Article 9(1) GDPR unless an Article 9(2) exception applies, typically explicit consent naming the biometric data.

Under the Crypto-Asset Tax Transparency Act (KStTG) the self-certification includes the tax identification number and date of birth (§ 6), may be checked against data already held for AML due diligence (§ 4(1)), and the related records are kept for ten years and then deleted (§ 14(2)), a different period from AML records.

7 Sector-specific obligations

Travel Rule

Under Regulation (EU) 2023/1113 (Transfer of Funds Regulation, TFR), applicable from 30 December 2024, every crypto transfer, with no minimum amount, must carry the

originator's name, ledger address, account number, and address with document and customer number (or date and place of birth), plus the beneficiary's name, ledger address and account number (Article 14(1) and (2)). Data travels before or with the transfer, originator data must be verified from reliable sources, and nothing may be sent until the Article is met (Article 14(4), (6) and (8)). Breaches: up to EUR 200,000 (§ 56(2a) GwG).

Self-hosted wallets

For transfers to or from a self-hosted address, originator and beneficiary data must still be held, and above EUR 1,000 the CASP must assess whether the customer owns or controls the address (TFR Articles 14(5) and 16(2)). § 15a GwG adds a risk assessment and at least one mitigating measure, such as identifying the holder, establishing origin and destination, or enhanced monitoring. BaFin (guidance 7.6) accepts proof of control by a reference transfer or a signed message, not a wallet screenshot.

Tokens, stablecoins and custody

Security tokens, unique NFTs and tokenised deposits fall outside MiCA. E-money tokens may be issued only by credit or e-money institutions (Article 48); asset-referenced tokens need their own authorisation; other tokens' white papers go to BaFin 20 working days before publication and are not approved. Custodians must segregate client assets on the ledger and are liable for losses attributable to them (Article 75(7) and (8)).

Tax reporting of users

In force since 24 Dec 2025 The KStTG implements EU crypto tax reporting. Tax residence must be self-certified and checked before reportable transactions (§§ 4, 7(1)); for customers onboarded by 31 December 2025 the deadline is 1 January 2027 (§ 7(2)), and non-responders must be blocked within 60 to 90 days (§ 8(3)). Reports go to the BZSt by 31 July, first for 2026 (§§ 9, 21); fines reach EUR 50,000, and repeat fines are passed to BaFin (§ 18).

CRYPTO TYPOLOGIES FROM BAFIN AND THE FIU (RED-FLAG PAPER, JULY 2026)

- **Straw-man accounts:** accounts opened in third parties' names to hide who controls the funds.
- **Mixer use and rapid swaps:** assets passed through mixing services or exchanged quickly across many crypto-assets.
- **Crypto ATM patterns:** cash split below thresholds, unusually many or large ATM purchases, or use far from home despite high fees.
- **Bridges and chain-hopping:** deposits from bridge-linked addresses the customer cannot explain, traced to ransomware or darknet wallets.
- **Pass-through accounts:** incoming crypto forwarded at once to non-custodial wallets, making no economic sense after fees.
- **Migrated customers:** users moving in bulk from providers that lost the right to operate when MiCA transitional periods ended.
- **Unlicensed or high-risk platforms:** counterparties seated in sanctioned or high-risk jurisdictions, or not registered with any supervisor.
- **Anonymity-enhancing coins:** requests to move privacy coins, which the AMLR bars CASPs from supporting through anonymising accounts from 10 July 2027.

MiCA breaches (§ 47 KMAG). Most CASP breaches: up to EUR 700,000 for individuals and EUR 5 million for firms, or 5% of turnover above EUR 100 million, or twice the profit. Market manipulation: up to EUR 15 million or 15% of turnover, or three times the profit.

AML breaches (§ 56 GwG). Basic fines reach EUR 150,000 for intentional breaches and EUR 100,000 otherwise. Serious, repeated or systematic breaches reach EUR 1 million or twice the economic benefit, and for financial-sector firms, including CASPs, the higher of EUR 5 million or 10% of prior-year total turnover. Travel Rule breaches reach EUR 200,000.

Recent actions. On 20 August 2024 BaFin, with police and the Bundesbank, seized 13 unauthorised crypto ATMs at 35 locations and retained almost EUR 250,000 in cash, citing money laundering risk (then under the banking licence regime). BaFin's annual report for 2025 (12 May 2026) records that it refused the first asset-referenced token applied for

under MiCA's transitional rule and prohibited its further distribution, accompanied four crypto custodians through orderly wind-down, and for the first time appointed a special representative at a crypto custodian to restore proper business organisation.

10 Recent changes and what to watch

- **10 Jul 2027** **Adopted, applies 10 Jul 2027** The AMLR applies directly, including identity verification under Article 22(6) and the Article 79 ban on anonymous crypto accounts and anonymity-enhancing coins.
- **1 Jan 2027** **In force, deadline ahead** KStTG self-certifications due for customers onboarded by 31 December 2025; first annual tax report due 31 July 2027.
- **7 Oct 2026** **Review, no proposal yet** AMLA set out AML priorities for the Commission's MiCA review, including staking, DeFi and unauthorised stablecoins.
- **Jul 2026** **In force** The EU-wide MiCA transitional period ended on 1 July; BaFin and the FIU warned on 8 July that customers taken over from unlicensed providers need full due diligence, and the FIU updated its crypto red-flag paper.
- **1 Jul 2026** **In force** The KMAAnzV sets the content of KMAG notifications, including material outsourcing.
- **23 Apr 2026** **In force** EU ban on transactions with Russia-based crypto-asset service providers and platforms.
- **1 Mar 2026** **In force** GwGMeldV: structured suspicious activity reports with crypto-specific mandatory fields.

11 What this means for identity verification

- **Method choice is legal, not just technical.** German onboarding needs eID or notified eID, QES plus reference transfer, or video identification meeting circular 3/2017; automated document and selfie checks can support but not replace these.
- **Biometrics and evidence.** Obtain explicit, recorded consent where face images are used, and store full session recordings as AML records.
- **Data model.** Place of birth, nationality, address, tax residence and tax ID feed Travel Rule messages, KStTG reports and structured FIU reports.
- **Re-verification triggers.** Doubts about identity data, a new PEP status, self-hosted addresses above EUR 1,000 and customers migrated from other providers.

- **Vendors and retention.** Material outsourcing of identification must be notified to BaFin; keep AML records five years (delete by ten) and tax records ten.
- **2027 readiness.** Plan for AMLR verification by eIDAS "substantial" or "high" means.

IDENTOMAT

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 and ID document capture and verification, including NFC chip reading, for remote onboarding flows.
- Biometric liveness and face match to support remote identification steps alongside the methods German law accepts.
- AML screening against sanctions, PEP and adverse-media lists at onboarding and through ongoing monitoring.
- KYB and beneficial owner verification for corporate customers, with KYC questionnaires for tax self-certification data.
- No-code workflow builder and an audit trail of each check, deployable in the cloud, on-premises or hybrid.

[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]**, §§ 1(31) and (32), 2, 3, 8, 10, 11, 12, 13, 15, 15a, 17, 43, 45, 46, 56 and Annex 2, 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](https://www.gesetze-im-internet.de)

- Kryptomärkteaufsichtsgesetz (KMAG) [Crypto Markets Supervision Act], §§ 9, 10, 46, 47, 50, Act of 27 December 2024 (BGBl. 2024 I Nr. 438), last amended by Art. 21 of the Act of 25 March 2026 (BGBl. 2026 I Nr. 81), [gesetze-im-internet.de](https://www.gesetze-im-internet.de)
- GwG-Meldeverordnung (GwGMeldV) [Reporting Ordinance], 26 August 2025 (BGBl. 2025 I Nr. 200), §§ 2, 3, 5 and Annex, [gesetze-im-internet.de](https://www.gesetze-im-internet.de)
- Kryptomärkteanzeigenverordnung (KMAnzV) [Crypto Markets Notification Ordinance], 20 May 2026 (BGBl. 2026 I Nr. 153), §§ 5, 9, [gesetze-im-internet.de](https://www.gesetze-im-internet.de)
- Kryptowerte-Steuertransparenz-Gesetz (KStTG) [Crypto-Asset Tax Transparency Act], 22 December 2025 (BGBl. 2025 I Nr. 352), §§ 4, 6, 7, 8, 9, 14, 18, 21, [gesetze-im-internet.de](https://www.gesetze-im-internet.de)
- Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA), Articles 48, 59, 60, 61, 63, 65, 75, 149 and Annex IV, EUR-Lex, eur-lex.europa.eu
- Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets (TFR), Articles 14, 16, 36, 40, EUR-Lex, eur-lex.europa.eu
- Council Regulation (EU) 2026/506 of 23 April 2026 amending Regulation (EU) No 833/2014, Article 5bb, EUR-Lex, eur-lex.europa.eu
- Regulation (EU) 2024/1624 (AMLR), Articles 22(6), 79, 90, EUR-Lex, eur-lex.europa.eu
- BaFin, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz [Interpretive guidance on the GwG], Stand July 2025, sections 1.3, 4.2.3, 5.1.3.2, 7.6, 8, [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, Merkblatt: Hinweise zu den Kryptowerte-Dienstleistungen nach MiCAR [Guidance notice on crypto-asset services], January 2025, sections III to V, [bafin.de](https://www.bafin.de)
- BaFin, Kryptowerte-Dienstleistungen [Authorisation procedure for CASPs], [bafin.de](https://www.bafin.de)
- BaFin, Kryptoinstitute [Supervision of crypto institutions and token issuers], [bafin.de](https://www.bafin.de)
- BaFin, "Bafin und FIU warnen vor Geldwäscherisiken", 8 July 2026, [bafin.de](https://www.bafin.de)
- BaFin, "Bafin warnt vor neuen Geldwäsche-Risiken", 9 July 2026, [bafin.de](https://www.bafin.de)
- BaFin, Risiken im Fokus 2026, No. 6: money laundering and terrorist financing risks, [bafin.de](https://www.bafin.de)
- BaFin press release, "BaFin-Razzia gegen Betreiber von Krypto-Automaten", 20 August 2024, [bafin.de](https://www.bafin.de)
- BaFin, Jahresbericht 2025 [Annual report 2025], 12 May 2026, sections on payment institutions and crypto service providers, [bafin.de](https://www.bafin.de)
- ESMA, Markets in Crypto-Assets Regulation (MiCA) and Interim MiCA Register (CASP file updated 22 October 2026), esma.europa.eu
- AMLA, "Advisory note on money laundering risks as the MiCAR transitional period ends", 1 July 2026, amla.europa.eu
- AMLA, "AMLA identifies AML/CFT priorities for the review of MiCA", 7 October 2026, amla.europa.eu

- Deutsche Bundesbank, Finanzsanktionen [Financial sanctions], [bundesbank.de](https://www.bundesbank.de); Häufig gestellte Fragen zum Thema Finanzsanktionen [FAQ], Stand June 2026, B.10 and C, [bundesbank.de](https://www.bundesbank.de)
- FIU, Anhaltspunktepapier "Alternative Zahlungsmethoden und neue Technologien" [Red-flag paper on alternative payment methods and new technologies], Stand July 2026, crypto sections, [zoll.de](https://www.zoll.de)
- FIU, Registrierung [goAML registration], [zoll.de](https://www.zoll.de)
- Datenschutzkonferenz, Positionspapier zur biometrischen Analyse [Position paper on biometric analysis], version 1.0, 3 April 2019, [datenschutzkonferenz-online.de](https://www.datenschutzkonferenz-online.de)