Identomat

COMPLIANCE GUIDE

Banking & Digital Banking Compliance in Austria

COUNTRY Austria

INDUSTRY Banking & Digital Banking

LAST UPDATED 11 November 2026

KEY REGULATORS Financial Market Authority (FMA) · European Central Bank (ECB) · Financial Intelligence Unit (A-FIU)

Key takeaways

- Taking deposits or lending in Austria needs a banking licence. For deposit-taking banks the European Central Bank (ECB) decides, but the application goes to the Austrian Financial Market Authority (FMA), and the bank needs at least EUR 5 million in initial capital.
- Fully remote account opening is allowed. In place of showing an ID in person, a bank can use live video identification, a state electronic ID such as ID Austria, a qualified electronic signature, or a first payment from an account at another bank, each with conditions set in law.
- Automated selfie-and-document onboarding is allowed only with identity documents whose chip data is digitally signed by the issuing authority, plus a check that a live person is present. Video calls must be fully audio-recorded, with screenshots of the face and both sides of the ID.
- Identity checks must, as a rule, be finished before the business relationship starts. An account can be opened early, but no money may move until due diligence is complete, and records must be kept for ten years.
- The EU Anti-Money Laundering Regulation applies directly from 10 July 2027 and takes over most of these due diligence rules, and the EU anti-money laundering authority's detailed due diligence standards (including remote verification) are drafted but not yet adopted.

Austria is open to digital banks, and its rules set out in detail how remote identification must work. The market is reachable either through an Austrian licence or by passporting an existing EEA licence into the country.

The principal authorities are the ECB, which grants and withdraws licences for deposit-taking credit institutions, and the FMA, which supervises banks, enforces anti-money laundering rules and, since 1 January 2026, handles financial sanctions matters for financial market participants. Suspicious transaction reports go to the Financial Intelligence Unit (A-FIU) at the Federal Criminal Police Office.

The biggest practical obstacle for a new entrant is building a remote onboarding flow that meets the Online Identification Regulation in detail, while defending it against the forged and AI-generated identities that Austria's 2025 national risk assessment reports as frequent in online account opening.

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	Level	Official site
European Central Bank (ECB)	Grants and withdraws licences of CRR credit institutions (deposit-taking banks)	EU (Single Supervisory Mechanism)	bankingsupervision.europa.eu
Financial Market Authority (FMA)	Receives all licence applications and licenses non-CRR banks and branches; banking supervision; anti-money laundering supervision of the financial sector; sanctions supervision of financial market participants	National	fma.gv.at

Oesterreichische Nationalbank (OeNB)	Consulted before a licence is granted (Banking Act, § 4(6)); handled sanctions matters until they passed to the FMA on 1 January 2026	National	oenb.at
Financial Intelligence Unit (A-FIU, Geldwäschemeldestelle)	Receives suspicious transaction reports; instructs banks on suspended transactions	National (Federal Criminal Police Office)	bundeskriminalamt.at
Federal Ministry of Finance (BMF)	Anti-money laundering policy and the national risk assessment; national sanctions orders	National	bmf.gv.at
EU Anti-Money Laundering Authority (AMLA)	Drafts EU technical standards under the Anti-Money Laundering Regulation	EU	amla.europa.eu

The Federal Administrative Court hears appeals against FMA penalties.

2 Licensing and authorisation

The Banking Act (BWG, consolidated version of 11 November 2026) reserves banking transactions, including deposit-taking, giro and current-account business, lending, securities custody and issuing payment cards, to licensed credit institutions when carried on commercially (§ 1(1)). Each requires a licence (§ 4(1)).

Who decides

Since 4 November 2014 the ECB has sole competence to grant and withdraw licences of CRR credit institutions, banks that take deposits from the public and lend on their own account (SSM Regulation, Regulation (EU) No 1024/2013, Articles 4(1)(a) and 14). Applications are filed with the FMA, which prepares a draft decision for the ECB. The ECB says decisions usually take six to twelve months. The FMA alone licenses non-CRR credit institutions and branches of foreign credit institutions, and must hear the OeNB before a licence is granted (§ 4(6)).

Capital and form

At least EUR 5 million initial capital freely available in Austria; a corporation, cooperative or savings bank (§ 5(1)).

Management and seat

At least two qualified, reliable directors without sole powers of representation; registered and head office in Austria (§ 5(1) nos. 12 to 14).

Business plan

Risk strategies, a three-year budget and, for deposit-takers, a forecast of covered deposits (§ 4(3)).

Owners

Qualifying shareholders must be suitable and reliable, and close links must not impede supervision (§ 5(1)).

Deposits are covered up to EUR 100,000 per depositor and institution, up to EUR 500,000 for twelve months for certain temporary high balances such as proceeds of a private home sale, with repayment within seven working days (Deposit Guarantee Schemes and Investor Compensation Act, ESAEG, §§ 7, 12 and 13). Banks licensed elsewhere in the European Economic Area can serve Austrian customers by passport notification.

Conducting CRR banking business without authorisation is punishable by the FMA with a fine of up to EUR 5 million or twice the benefit gained (§ 98(1)); other unauthorised banking business carries up to EUR 100,000 (§ 98(1a)). Names such as "Bank" are reserved to licensed institutions (§ 94), and misuse carries up to EUR 60,000 (§ 99(1)).

3 AML, KYC and customer due diligence

Credit and financial institutions are obliged entities under the Financial Markets Anti-Money Laundering Act (FM-GwG, § 1(1); consolidated version of 11 November 2026). This includes branches of EEA banks operating in Austria and investment firms (§ 2 nos. 1 and 2).

When due diligence applies

- On establishing a business relationship; savings deposit and securities custody business always count as one (§ 5 no. 1).
- For occasional transactions of EUR 15,000 or more, single or linked, and transfers of funds above EUR 1,000 (§ 5 no. 2).
- For each savings deposit payment in or out of EUR 15,000 or more (§ 5 no. 3).
- On suspicion, or on doubts about earlier identification data (§ 5 nos. 4 and 5).

What due diligence covers

Section 6(1) requires identifying and verifying the customer and any representative; identifying the beneficial owner and understanding the ownership and control structure; the purpose and nature of the relationship; obtaining and verifying information on the source of funds; ongoing monitoring; and regular updating of data. Every customer is placed in a risk class (§ 6(5)).

A beneficial owner is a natural person holding more than 25% of shares, voting rights or participation, directly or indirectly, or exercising control (Beneficial Owners Register Act, WiEReG, § 2). At the start of every relationship with an Austrian legal entity, the bank must obtain an extract from the beneficial owners register (FM-GwG § 7(1)).

Enhanced and simplified due diligence

Enhanced measures are mandatory for high-risk third countries (§ 9a), cross-border correspondent relationships with third-country respondents (§ 10) and politically exposed persons, who need senior management approval and source-of-wealth checks (§ 11), and wherever the bank's risk assessment finds higher risk (§ 9(1)). Simplified measures require a documented low risk, and monitoring continues (§ 8).

Monitoring, reporting and retention

AI-based monitoring is allowed if documented (§ 7a). Suspicious transaction reports go to the A-FIU without delay, electronically (§ 16(1)); related transactions are then held pending its instructions (§ 17). There is no general cash reporting threshold; the only threshold notice covers withdrawals from unidentified savings deposits of EUR 15,000 or more, which wait seven calendar days (§ 16(3)). Due diligence and transaction records are kept for ten years after the relationship ends, then deleted (§ 21).

4 Identity verification and onboarding

The default method for a natural person is **in-person presentation of an official photo ID** issued by a state authority, with photo, name, date of birth, signature and the issuing authority (FM-GwG § 6(2) no. 1). Legal persons are verified from conclusive documents showing existence, name, legal form, representation and seat (§ 6(2) no. 2).

Remote identification

Where there is no personal contact, in-person presentation may be replaced by one of four safeguards (§ 6(4)). Name, date of birth and address must always be known. Trustees must still appear in person (§ 6(3)).

Video identification

The official photo ID presented in a video-based electronic procedure (online identification), under the FMA's Online Identification Regulation (Online-IDV).

Electronic ID

A statutory procedure giving the same assurance as an ID. The E-ID under the E-Government Act (ID Austria) qualifies: its simplified proof of name, date of birth and photo has the evidential force of an official photo ID (E-Government Act, § 4(6)).

Qualified signature or registered post

A qualified electronic signature on the customer's declaration, or registered postal delivery to the stated address with an ID copy. Third-country residents also need a confirmation from a bank they hold a relationship with.

First payment

The first payment comes from an account in the customer's name at a credit institution in Austria, another EU member state or an equivalent supervised third country, plus document copies or that bank's confirmation, received before the payment.

Agent-led and biometric procedures

Under the Online-IDV, trained staff run agent-led calls in an access-controlled room (§ 3). The call is audio-recorded in full, with screenshots of the face and both sides of the ID (§ 4(2)). The customer moves their head and reads out the ID serial number or a random code of at least four characters (§ 4(3)); the agent tilts the document to check holograms or equivalent features, laminate, photo and data consistency (§ 4(4)); and the customer enters a one-time code sent by email or SMS (§ 4(5)). Any inconsistency or uncertainty ends the session (§ 5).

Fully automated **biometric identification** is permitted if it is state of the art, at least as secure as agent-led identification, documented and actively monitored (§ 4(6)). It may use only IDs whose content is electronically signed by the issuing authority; the bank reads the NFC chip, verifies its signature and stores the signed data. A presence check based on video recorded in the session, which may be passive, replaces the head movement and codes.

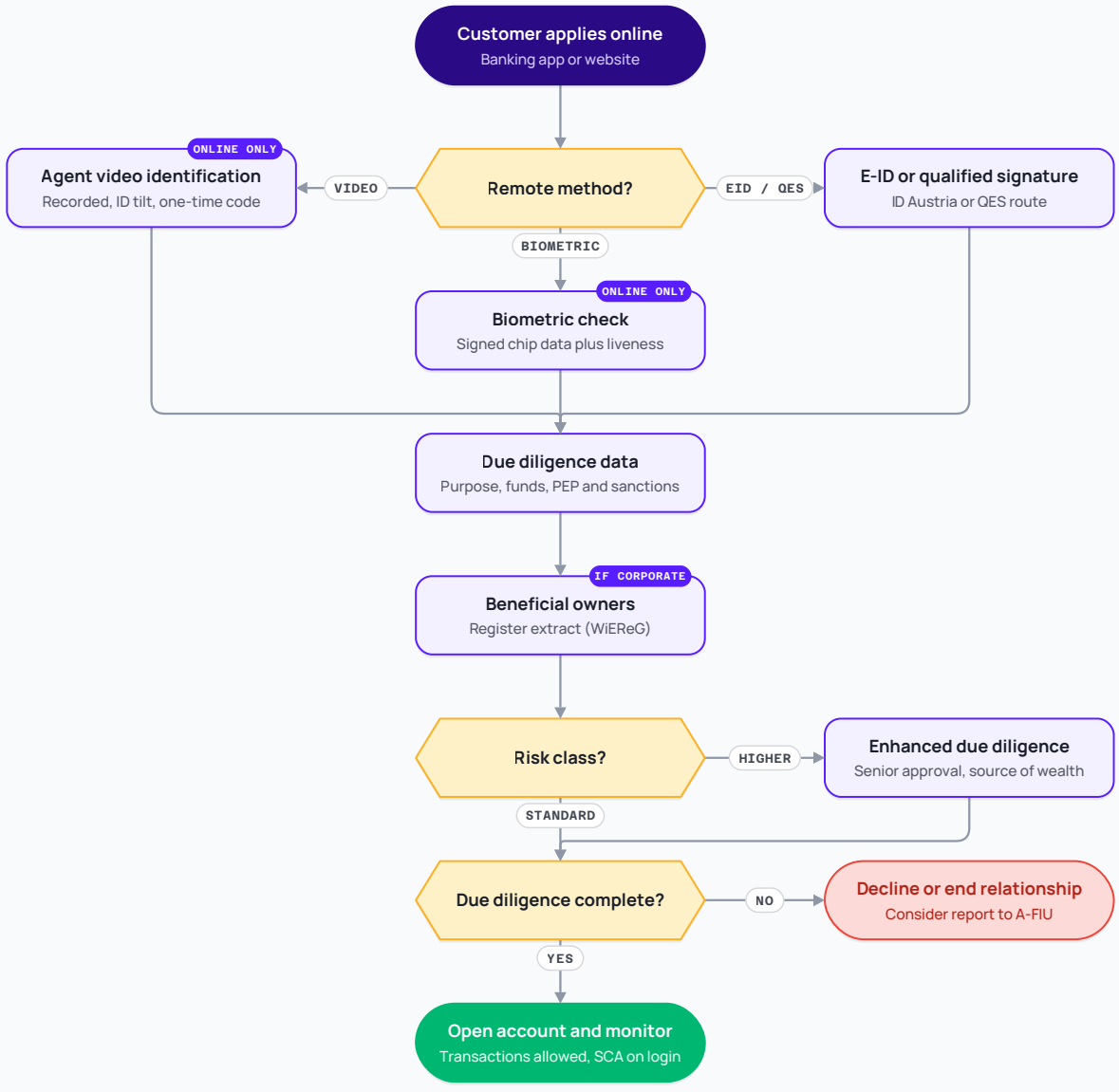


Figure 1. Remote retail account opening at an Austrian bank under the FM-GwG and the Online Identification Regulation.

Reliance and processors

A bank may rely on a credit or financial institution in Austria, another EU member state or an equivalent supervised third country (never a high-risk one), but keeps final responsibility (FM-GwG § 13). An identity verification provider acting as processor must

meet the Online-IDV in full under a written agreement, without impairing FMA audits (Online-IDV § 6).

5 Digital channels: what's different

Bottom line: the due diligence duties are the same online, but remote identification is allowed only through four safeguards named in the FM-GwG, and video and biometric identification must follow the Online Identification Regulation step by step.

Requirement	In person / branch	Online / remote	Difference
How identity is verified	Official photo ID presented in person	One of four safeguards: video, E-ID, qualified signature or post, first payment	Differs
Technical procedure	No prescribed procedure	Online-IDV: recording, screenshots, ID checks, one-time code; biometric only with signed chip data and liveness	Differs
Risk treatment	Standard risk-based approach	Remote without these safeguards is a listed higher-risk factor	Differs
Timing of verification	Before the relationship; account may open but no transactions until complete	Same rule	Same
Due diligence content	Purpose, source of funds, beneficial owner, PEP checks	Same, plus name, date of birth and address always required	Same
Evidence kept	Copies of documents, 10 years	Also call audio, screenshots or signed chip data, biometric check results, 10 years	Differs
Use of third parties	Reliance on regulated institutions (§ 13)	Same, plus processor rules for identification providers (Online-IDV § 6)	Differs

Account access	Online access rule does not apply	Strong customer authentication for online access, payments and risky remote actions (ZaDiG 2018, § 87)	`Differs`
Sanctions and PEP screening	Required	Required	`Same`

Remote is not automatically high risk

Annex III to the FM-GwG lists relationships "without personal contact and without certain safeguards" as a potentially higher-risk factor. The FMA's circular 01/2022 confirms that identification through a § 6(4) safeguard does not by itself require enhanced due diligence.

Chip-based biometrics versus video

Agent-led calls work with any official photo ID with holographic or equivalent features; fully automated flows only with chip-based passports and ID cards. Online identification is open to non-residents, but residence still shapes due diligence (FMA circular 01/2022).

Pending changes

From 10 July 2027 the EU Anti-Money Laundering Regulation `Adopted, applies 10 Jul 2027` allows verification through an identity document plus, where relevant, reliable independent sources, or electronic identification at eIDAS assurance level "substantial" or "high" with relevant qualified trust services (Article 22(6)). AMLA's due diligence standards on remote verification and electronic identification (final report dated 30 September 2026) went to the European Commission on 1 October 2026 `Final draft, not adopted`. Under the amended eIDAS Regulation, member states must provide European Digital Identity Wallets by 24 December 2026, and banks (other than micro and small enterprises) required to use strong authentication for online identification must accept them, at the user's voluntary request, by 24 December 2027 `Adopted, phased`. ID Austria is already a notified eIDAS scheme at assurance level "high", published in the Official Journal on 27 April 2022.

6 Data protection and biometrics

The General Data Protection Regulation (GDPR) applies, with the Austrian Data Protection Act. Processing for anti-money laundering purposes is a matter of public interest (FM-GwG § 21(6)), which gives banks a legal basis other than consent, but data processed only

under the FM-GwG may not be used for other purposes such as marketing (§ 21(4)). Customers must receive GDPR information before the relationship begins (§ 21(5)).

Biometric identification is the exception: the Online-IDV allows it only where GDPR Article 9(2)(a) (explicit consent) permits, with security measures meeting Article 32 (§ 4(6)). Banks should therefore offer a non-biometric route for customers who decline. Recordings and images are kept for ten years after the relationship ends, then deleted unless longer retention is required (FM-GwG § 21(1) and (2)).

7 Sector-specific obligations

Financial sanctions

Under the Sanctions Act 2024 (Sanktionengesetz 2024, § 7), financial market participants need written sanctions compliance strategies, controls and procedures, approved by a management body and applied at individual and group level. The FMA monitors compliance by financial market participants, receives their reports of frozen assets and decides on releases of frozen funds they hold (§§ 6(1) and 12); matters pending at the OeNB passed to it on 1 January 2026. The FM-GwG adds controls against circumvention of targeted financial sanctions (§ 23a).

Correspondent banking and shell banks

Shell-bank correspondent relationships are prohibited (§ 12). The 2025 national risk assessment restates the elevated banking risks found in 2021: non-resident customers, politically exposed persons and growing correspondent banking.

Branches of foreign banks

Banking Act amendments transposing the sixth Capital Requirements Directive (Federal Law Gazette I No. 93/2026) add rules for branches of foreign banks, partly from 11 January 2027 `Adopted, effective 11 Jan 2027`.

8 Risk indicators and red flags

BANKING TYPOLOGIES FROM THE NATIONAL RISK ASSESSMENT 2025 AND THE FMA

- **Fraud proceeds**: the predicate in around 70% of money laundering investigations, often surfacing as recalls from victims' banks.
- **AI-generated identities**: forged or deepfaked identities used to open accounts through video identification or qualified electronic signatures.
- **Account chaining**: a fraudulently "verified" account used for one-cent verification transfers to open further accounts at other banks.
- **Forged documents in online identification**: flagged by the FMA as a practical problem, together with weak selection of identification providers.
- **Shell and straw-man companies**: nominee directors and sham firms used for tax and social security fraud.
- **Non-resident, offshore and PEP relationships**: elevated risk for banks, with continuing exposure to foreign corruption proceeds.
- **Proliferation and sanctions evasion**: front companies and straw men acting for listed persons or between buyers and sellers of sanctioned goods, including in trade finance.

9 Enforcement and penalties

FM-GwG penalties are administrative fines imposed by the FMA, set on two tiers:

Breach	Responsible person (§ 34)	Legal person (§ 35)
Due diligence, reliance, reporting, retention, internal organisation, sanctions controls, transfer-of-funds data	Up to EUR 150,000	Up to EUR 150,000
Serious, repeated or systematic breaches of the core duties	Up to EUR 5 million or twice the benefit gained	Up to EUR 5 million or 10% of annual total turnover
Trustee failing to disclose a trust relationship	Up to EUR 60,000	Not applicable

In 2024 the FMA imposed fines of about EUR 4.33 million under the FM-GwG, including EUR 2,070,000 against a correspondent bank that failed to assess two third-country respondents' controls, and EUR 791,000 in a second correspondent banking case. In May 2026 the FMA fined Sparkasse Oberösterreich Bank AG EUR 60,000 for weak written policies on ownership structures and data updating (final). In March 2026 it fined NOTARTREUHANDBANK AG EUR 127,500 for inadequate ongoing monitoring controls; the penalty is not final because the bank has appealed to the Federal Administrative Court.

10 Recent changes and what to watch

- **10 July 2027**: the EU Anti-Money Laundering Regulation (Regulation (EU) 2024/1624) applies `Adopted, applies 10 Jul 2027`. It lowers the occasional transaction threshold from EUR 15,000 to EUR 10,000 and sets a five-year retention period, against ten years under the FM-GwG today. On the same day a new Beneficial Owners Register Act 2027 (Federal Law Gazette I No. 94/2026, published 29 October 2026) replaces the WiEReG.
- **11 January 2027**: Banking Act rules on branches of foreign credit institutions (Federal Law Gazette I No. 93/2026) take effect `Adopted, effective 11 Jan 2027`.
- **24 December 2026**: deadline for member states to provide European Digital Identity Wallets `Adopted, due 24 Dec 2026`. Austria will roll out its wallet in stages from the ID Austria app; most banks must accept wallets on request by 24 December 2027.
- **30 October 2026**: amendments to the FM-GwG made by Federal Law Gazette I No. 94/2026 (published 29 October 2026; the law transposes Directive (EU) 2024/1640) took effect (§ 43(8)) `In force`. For banks, fines for transfer-of-funds data breaches now cap at EUR 150,000 unless serious, repeated or systematic.
- **1 October 2026**: AMLA published its final draft due diligence standards (final report dated 30 September 2026) and submitted them to the European Commission `Final draft, not adopted`. Proposed to apply six months after entry into force.
- **30 April 2026**: FATF published Austria's mutual evaluation report `Published`. Supervision was rated substantial, preventive measures only moderate; Austria is in enhanced follow-up with key actions due within three years.
- **1 January 2026**: the FMA took over pending sanctions matters from the OeNB under the Sanctions Act 2024 `In force`. Sanctions supervision of banks, including pending authorisations, now sits with the FMA.

11 What this means for identity verification

- **Offer a fallback route.** Biometric onboarding needs explicit consent and chip-signed documents, so provide agent-led video, the E-ID, a qualified signature or a reference payment as alternatives.
- **Defend against deepfakes and forged IDs.** The national risk assessment and the FMA flag both.
- **Keep evidence for ten years**, including recordings, signed chip data and each check result, and block transactions until due diligence is complete.
- **Plan for 2027.** EU rules and wallets will reset remote verification.

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:

- Remote onboarding with ID document capture and NFC chip verification, face match and biometric liveness detection.
- Agent-led video KYC with recorded sessions and an audit trail for each check.
- KYB and beneficial owner verification for corporate customers.
- AML screening against sanctions, PEP and adverse-media lists at onboarding and through ongoing monitoring.
- No-code workflow builder to offer alternative identification routes and adapt flows as EU rules change.

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

- **Finanzmarkt-Geldwäschegesetz (FM-GwG) [Financial Markets Anti-Money Laundering Act]**, §§ 1, 2, 5 to 13, 16, 17, 21, 23a, 34, 35, 43 and Annex III, RIS consolidated version of 11 November 2026, ris.bka.gv.at
- **Online-Identifikationsverordnung (Online-IDV) [Online Identification Regulation]**, §§ 1 to 6, RIS consolidated version of 11 November 2026, ris.bka.gv.at
- **Bankwesengesetz (BWG) [Banking Act]**, §§ 1, 4, 5, 94, 98, 99, 107, RIS consolidated version of 11 November 2026, ris.bka.gv.at
- **Wirtschaftliche Eigentümer Registergesetz (WiEReG) [Beneficial Owners Register Act]**, § 2, RIS consolidated version of 11 November 2026, ris.bka.gv.at
- **Sanktionengesetz 2024 [Sanctions Act 2024]**, §§ 2, 6, 7, 12 and transitional provisions, RIS consolidated version of 11 November 2026, ris.bka.gv.at
- **Zahlungsdienstegesetz 2018 (ZaDiG 2018) [Payment Services Act 2018]**, § 87, RIS consolidated version of 11 November 2026, ris.bka.gv.at
- **E-Government-Gesetz [E-Government Act]**, § 4 (the E-ID function, including § 4(6)), RIS consolidated version of 11 November 2026, ris.bka.gv.at
- **Einlagensicherungs- und Anlegerentschädigungsgesetz (ESAEG) [Deposit Guarantee Schemes and Investor Compensation Act]**, §§ 7, 12, 13, RIS consolidated version of 11 November 2026, ris.bka.gv.at
- **Federal Law Gazette I No. 94/2026** (Beneficial Owners Register Act 2027 and amendments to the FM-GwG, Article 5, in force under FM-GwG § 43(8)), published 29 October 2026, ris.bka.gv.at
- **FMA Circular 01/2022 on Due Diligence Obligations for the Prevention of Money Laundering and Terrorist Financing**, version February 2022, published 23 February 2022, marginal numbers 247 to 283, fma.gv.at
- **FMA, Priorities and Trends in the Prevention of ML/TF 2024**, 2025, sections 1 and 3, fma.gv.at
- **FATF Mutual Evaluation Report of Austria - 2026**, 30 April 2026, key findings and ratings, fatf-gafi.org
- **ECB Banking Supervision, Authorisation** (licensing timeframe), bankingsupervision.europa.eu
- **FMA, Deposit protection**, fma.gv.at
- **Commission Implementing Regulations (EU) 2024/2977, 2024/2979, 2024/2980, 2024/2981 and 2024/2982** (European Digital Identity Wallets), published 4 December 2024, eur-lex.europa.eu
- **oesterreich.gv.at, ID Austria**, oesterreich.gv.at
- **FMA, Licensing & Notification (banks)**, including ECB competence and the licensing procedure, fma.gv.at
- **FMA, The legal basis under national and European law (prevention of money laundering)**, fma.gv.at
- **FMA, Announcement: sanction upon Sparkasse Oberösterreich Bank AG**, 5 May 2026, fma.gv.at

- **FMA, Announcement: sanction against NOTARTREUHANDBANK AG**, 17 March 2026, updated 13 April 2026, fma.gv.at
- **Federal Ministry of Finance, Nationale Risikoanalyse 2025 [National Risk Assessment 2025]**, pp. 17 to 18, 44 and 138 to 145, bmf.gv.at
- **Federal Chancellor, Parliamentary answer 5451/AB (XXVIII. GP) on the EUDI Wallet**, 7 July 2026, parlament.gv.at
- **Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No 910/2014**, OJ C/2025/2448, 25 April 2025, eur-lex.europa.eu
- **Regulation (EU) 2024/1624 (Anti-Money Laundering Regulation)**, Articles 19, 22, 23, 77 and 90, eur-lex.europa.eu
- **Regulation (EU) 2024/1183 (European Digital Identity Framework)**, Articles 5a and 5f, eur-lex.europa.eu
- **AMLA, Final Report: Draft Regulatory Technical Standards under Article 28(1) of Regulation (EU) 2024/1624**, 30 September 2026, amla.europa.eu
- **AMLA, Press release: AMLA finalises key standards for the private sector**, 1 October 2026, amla.europa.eu