Identomat

COMPLIANCE GUIDE

Fintech & Digital Payments Compliance in Austria

COUNTRY Austria

INDUSTRY Fintech & Digital Payments

LAST UPDATED 11 November 2026

KEY REGULATORS Financial Market Authority (FMA) · Federal Criminal Police Office, A-FIU · Oesterreichische Nationalbank

Key takeaways

- To offer payments, transfers or wallets in Austria you need a licence from the Financial Market Authority (FMA), either as a payment institution or as an e-money institution, or a licence from another European Economic Area (EEA) country used through passporting. Pure account-information apps only need to be registered.
- Payment and e-money institutions must identify and verify every customer before the business relationship starts, apply anti-money laundering (AML) checks, report suspicions to the Austrian financial intelligence unit and keep identification records for ten years.
- Fully online onboarding is allowed, but only through one of the four safeguards in the anti-money laundering act: video identification under the FMA's rules (including fully automated biometric identification that reads the ID document's chip), ID Austria (the national electronic ID), a qualified electronic signature or registered post with further conditions, or a first payment from the customer's own account at a qualifying bank. Name, date of birth and address must always be known.
- Buy-now-pay-later offered by a third-party lender falls under the new Consumer Credit Act 2026 from 20 November 2026, including a mandatory creditworthiness check.
- The EU Anti-Money Laundering Regulation becomes directly applicable from 10 July 2027; the new EU Payment Services Regulation is agreed but not yet law (November 2026).

Austria is open to non-bank payment and e-money businesses, both through domestic licences and EEA passporting. The FMA licenses and supervises payment and e-money institutions and is also their AML and sanctions supervisor, so one authority sets the rules a new entrant is measured against.

The biggest practical obstacle for a digital entrant is remote identification. Austrian law does not leave the choice of remote method to the firm: the Financial Markets Anti-Money Laundering Act lists the permitted safeguards, and the FMA's Online Identification Regulation prescribes in detail how video and biometric identification must work.

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 fintech and payments	Level	Official site
Financial Market Authority (FMA)	Licenses and supervises payment and e-money institutions; AML supervisor (FM-GwG § 25); monitors sanctions compliance by financial market participants (SanktG 2024 § 12(2)); issues the Online Identification Regulation	National	fma.gv.at
Federal Criminal Police Office, A-FIU (Geldwäschemeldestelle)	Receives suspicious transaction reports through goAML; analyses typologies	National	bundeskriminalamt.at
Oesterreichische Nationalbank (OeNB)	Receives payment service providers' reports under the Instant Payments Regulation (ZaDiG 2018 § 88(9))	National	oenb.at

Federal Ministry of Finance (BMF)	Beneficial owners register authority (WiEReG)	National	bmf.gv.at
Trade authorities (Gewerbebehörden)	Consumer credit enforcement for firms supervised under trade law, alongside the FMA (Consumer Credit Act 2026 § 43)	Regional	Provincial and district authorities
Data Protection Authority (DSB)	Austria's data protection authority under the GDPR, including identity and biometric data	National	dsb.gv.at
Anti-Money Laundering Authority (AMLA)	EU authority drafting the technical standards that will apply under the AML Regulation	Supranational	amla.europa.eu

2 Licensing and authorisation

Under the **Payment Services Act 2018 (ZaDiG 2018)**, § 7(1), providing payment services commercially in Austria requires a licence from the FMA as a payment institution. Account information service providers instead apply for entry in the payment institutions register (§ 15) and must hold professional indemnity insurance; payment initiation services need liability insurance (§ 8). Issuing electronic money requires a separate licence as an e-money institution under the **E-Money Act 2010 (E-Geldgesetz 2010)**, § 3(1); an e-money institution may also provide payment services.

Activity	Authorisation	Minimum initial capital
Money remittance only	Payment institution licence (ZaDiG 2018 § 7)	EUR 20,000 (§ 16(1))
Payment initiation only	Payment institution licence plus liability insurance	EUR 50,000 (§ 16(1))

Accounts, transfers, card issuing or acquiring	Payment institution licence	EUR 125,000 (§ 16(1))
Account information only	Registration (§ 15) plus professional indemnity insurance	None
Issuing e-money (wallets, prepaid)	E-money institution licence (E-Geldgesetz 2010 § 3)	EUR 350,000 (§ 11(1))

Stand-alone consumer lending is banking business: granting cash loans commercially requires a bank licence from the FMA (Banking Act, BWG, § 1(1) no. 3 and § 4(1)). A payment institution may grant credit only as an ancillary activity linked to the execution of certain payment services, repayable within 12 months (ZaDiG 2018 § 7(6)).

Agents, distributors and passporting

A payment institution must notify the FMA before using an agent, describing the agent's AML controls (ZaDiG 2018 § 22). E-money institutions may distribute and redeem e-money through third parties but may not issue it through agents or distributors (E-Geldgesetz 2010 § 15(2)). EEA payment and e-money institutions established in Austria other than through a branch may have to appoint a central AML contact point (FM-GwG § 23(7)).

Operating without a licence

Unauthorised payment services are an administrative offence punishable by the FMA with a fine of up to EUR 50,000 (ZaDiG 2018 § 99(1)); unauthorised e-money issuance carries up to EUR 100,000 (E-Geldgesetz 2010 § 29(1)).

3 AML, KYC and customer due diligence

Payment institutions and e-money institutions are obliged entities under the **Financial Markets Anti-Money Laundering Act (FM-GwG)**, supervised by the FMA. The FMA's interpretation is set out in its 01/2022 Circular on due diligence obligations and companion circulars on risk assessment, internal organisation and reporting.

When CDD applies (§ 5)

On establishing a business relationship; for occasional transactions of EUR 15,000 or more, including linked transactions; for occasional transfers of funds of more than EUR 1,000; and whenever there is suspicion of money laundering or terrorist financing.

What must be done (§ 6)

Identify and verify the customer and beneficial owners, ask whether the customer acts on own or third-party account, establish purpose and nature and the source of funds, and monitor the relationship, all before the relationship starts (§ 7(1)). Every customer is placed in a risk class.

Simplified and enhanced (§ 8, § 9)

Simplified measures only where the firm's own risk analysis shows low risk. Enhanced measures where risk is higher; a non-face-to-face relationship without safeguards is a listed higher-risk factor (Annex III), but using a § 6(4) safeguard does not by itself require enhanced measures (FMA Circular 01/2022, MN 247). Politically exposed persons need senior management approval, source of wealth and funds checks and enhanced monitoring (§ 11).

Monitoring and reporting (§ 7a, § 16)

Transaction monitoring may use artificial intelligence under § 7a. Suspicious transaction reports go to the A-FIU without delay.

Firms may rely on third parties for identification and other CDD steps, but final responsibility stays with the relying firm (§ 13(1)). When onboarding a legal entity, firms must obtain an extract from the register under the **Beneficial Owners Register Act (WiEReG)** (§ 7(1)). If the federal government designates a country as a non-cooperative state by regulation, customers resident there may be identified only in person, and transactions of EUR 100,000 or more involving that state must be reported to the A-FIU (§ 12(3) and (4)); no such regulation is in force as of November 2026.

CDD documents, including the data from electronic identification means and remote identification procedures, and transaction records must be kept for ten years after the relationship ends or the occasional transaction (§ 21(1)).

4 Identity verification and onboarding

The default under FM-GwG § 6(2) is personal presentation of an official photo ID: a document issued by a state authority with a non-replaceable facial image, name, date of birth, signature and issuing authority. Where there is no personal contact, § 6(4) allows the photo ID to be replaced by one of four safeguards, and the firm must always know the customer's name, date of birth and address:

1. **Online identification**: the ID is presented in a video-supported electronic procedure, under the FMA's Online Identification Regulation (Online-IDV).
2. **Electronic ID**: a statutory procedure that provides the same information as the photo ID with equal certainty. The E-ID under the E-Government Act (ID Austria) can be used by private-sector firms that set up a suitable technical environment (E-Government-Gesetz § 14) and register as an ID Austria service provider through the Business Service Portal.
3. **Qualified electronic signature** under the eIDAS Regulation, or registered post to the customer's address combined with a copy of the photo ID. For customers resident in a third country, a bank with a lasting relationship with the customer (or an Austrian representation or recognised certification body) must also confirm the identification in writing.
4. **First payment** from an account in the customer's name at a credit institution that qualifies as a third party under § 13, with copies of identification documents or the bank's written confirmation that it identified the customer. The FMA expects the copies or confirmation to be in hand before the first payment (Circular 01/2022, MN 283).

The list is exhaustive (Circular 01/2022, MN 247). Remote identification is not available where the customer acts as a trustee, who must be identified in person (§ 6(3)). Firms may use service providers to run online identification but remain responsible for compliance with the Online-IDV (MN 272).

Video identification under the Online-IDV

The conversation 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 a code, the agent checks holograms and data consistency, and the customer enters a one-time code sent by email or SMS (§ 4(3) to (5)). Agents must be trained and work from a separate room with access control (§ 3). The process must be aborted if checks are not possible or inconsistencies or uncertainties arise (§ 5(1)); if money laundering is suspected, the identification is completed and a suspicious transaction report considered (§ 5(2)).

Fully automated biometric identification

Online-IDV § 4(6) permits purely biometric identification without an agent if it reflects the state of the art and is at least as secure as agent-led identification. Only ID documents electronically signed by the issuing authority may be used, with the chip signature and data integrity verified. A video-based presence check, which may be passive, must confirm the customer is taking part.

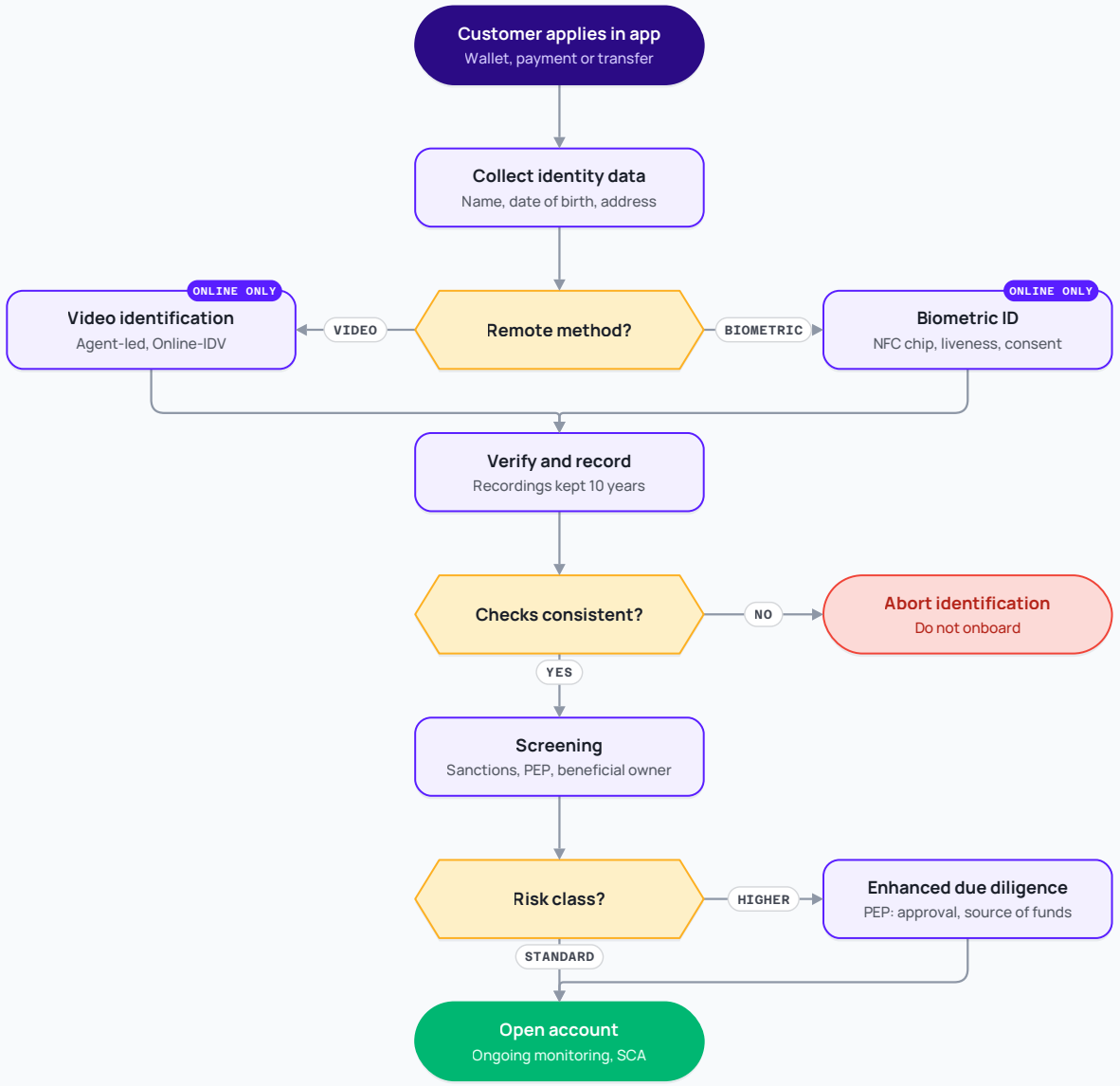


Figure 1. Remote onboarding of a retail customer by an Austrian payment or e-money institution.

5 Digital channels: what's different

Bottom line: the CDD obligations are the same online and in person, but a remote customer can only be verified through one of the methods listed in FM-GwG § 6(4), and video and biometric identification must follow the FMA's detailed procedural rules.

Requirement	In person / branch or agent	Online / remote	Difference
When CDD applies	At start of relationship; occasional transactions from EUR 15,000; occasional transfers over EUR 1,000	Same triggers	Same
How identity is verified	Personal presentation of an official photo ID	Video ident (incl. chip-based biometric), ID Austria, qualified e-signature or registered post, or first payment	Differs
Procedural standard	None beyond the photo ID definition	Online-IDV: recording, security-feature checks, one-time code, liveness	Differs
Risk treatment	Risk-based	Risk-based if a listed safeguard is used; higher-risk factor without one	Differs
Customer acting as trustee	Trustee identified in person	Remote identification not available	Differs
Evidence kept	Copies of documents, 10 years	Audio recording, screenshots or signed chip data, 10 years	Differs
Account access	Not applicable	Strong customer authentication for online access and remote payments	Differs
Reliance on third parties	Permitted; firm keeps responsibility	Permitted; firm keeps responsibility	Same

Chip reading is mandatory for automated flows

Automated flows must read and validate the ID chip (Online-IDV § 4(6)); agent-led video identification relies on visual security-feature checks (§ 4(4)).

Strong customer authentication

ZaDiG 2018 § 87 requires strong customer authentication when a payer accesses a payment account online, initiates an electronic payment or performs any remote action that carries a risk of payment fraud; remote electronic payments must be dynamically linked to amount and payee.

Pending changes

The EU Anti-Money Laundering Regulation `Adopted, applies 10 Jul 2027` lets firms verify identity through eIDAS electronic identification means at assurance level substantial or high and relevant qualified trust services (Article 22(6)); its list of higher-risk factors (Annex III) no longer includes non-face-to-face relationships, and recital 66 states that such electronic identification can reduce risk to standard or low. AMLA's draft standards on customer due diligence `Final draft, not adopted`, covering non-face-to-face verification and electronic identification, were submitted to the Commission on 1 October 2026 and would apply six months after entry into force.

6 Data protection and biometrics

The General Data Protection Regulation (GDPR) governs identity data generally. For onboarding, Online-IDV § 4(6) permits biometric identification only where lawful under Article 9(2)(a) GDPR (explicit consent) and with security measures appropriate to the risk under Article 32 GDPR. The procedure, its security factors and the result of each check must be documented, and recordings are kept as CDD records for ten years (FM-GwG § 21). The Online-IDV applies without prejudice to data protection law (§ 1(4)).

7 Sector-specific obligations

Consumer credit and buy-now-pay-later

The **Consumer Credit Act 2026 (Verbraucherkreditgesetz 2026)**, enacted by the Consumer Credit Law Amendment Act 2026 (BGBl. I No. 36/2026) to transpose Directive (EU) 2023/2225, applies to contracts concluded from 20 November 2026 (§ 45) and covers

deferred payment (§ 39). Interest- and fee-free deferral granted by the seller itself, with no third party offering credit, is exempt if payment is due within 50 days; for large online sellers the exemption also requires that no third party acquires the claim and that payment is due within 14 days. Buy-now-pay-later provided by a third-party lender is therefore in scope. Lenders must carry out a thorough creditworthiness assessment before concluding a contract (§ 17). The FMA and the trade authorities are the competent authorities (§ 43).

Instant payments and verification of payee

Under the Instant Payments Regulation (Regulation (EU) 2024/886), payment service providers that offer euro credit transfers must offer instant transfers at no extra charge, verify that the payee's name matches the IBAN, and screen their customers against EU sanctions lists at least daily. Euro-area providers have had to offer verification of the payee since 9 October 2025 (Article 5c(9) of Regulation (EU) No 260/2012); euro-area payment and e-money institutions must offer instant euro transfers by 9 April 2027. The FMA enforces these duties under ZaDiG 2018 § 101a, added by the Financial Markets Omnibus Act (BGBl. I No. 5/2026), and providers report annually to the OeNB.

ICT security and outsourced identity checks (DORA)

The Digital Operational Resilience Act (DORA, Regulation (EU) 2022/2554) has applied to payment and e-money institutions since 17 January 2025. Its Article 9 protects the firm's own ICT systems: strong authentication, access rights and identity management for staff and systems (Delegated Regulation (EU) 2024/1774, Articles 20 and 21). It does not govern customer identity verification. For onboarding, DORA bites through Article 28: an external identity verification service is typically an ICT third-party service, and the firm remains fully responsible for compliance. On 14 July 2026 the FMA fined Western Union International Bank EUR 42,000 for late ICT incident reports.

Sanctions

Under the **Sanctions Act 2024 (SanktG 2024)**, § 7, financial market participants must have written, board-approved sanctions compliance controls, applied at entity and group level; the FMA monitors compliance (§ 12(2)).

8 Risk indicators and red flags

PAYMENT AND E-MONEY TYPOLOGIES (A-FIU 2025 REPORT, FM-GWG)

- **Fake IDs in remote onboarding**: forged ID documents bearing data of real, uninvolved people used to pass qualified e-signature or one-cent reference transfer checks.
- **Chained account opening**: a fraudulently opened account used for one-cent reference transfers to open further accounts.
- **Duplicate identities**: a new applicant whose identity already holds an account with the same provider.
- **Money mules and cash-out**: accounts that receive fraud proceeds and pass them on to other money mules or withdraw them in cash in a neighbouring country.
- **Instant payment chains**: transfers that complete in seconds and run through chains of accounts, making funds hard to secure.
- **Fraud proceeds**: fraud is the most common predicate offence identified in suspicious transaction reports (18% in 2025).
- **Non-face-to-face without safeguards**: relationships opened remotely without electronic identification or equivalent controls (FM-GwG Annex III).

9 Enforcement and penalties

Under the FM-GwG, responsible managers face up to EUR 150,000 for due diligence, reporting and organisational breaches (§ 34(1) and (2)), rising to EUR 5 million or twice the benefit derived for serious, repeated or systematic breaches (§ 34(4)). Legal persons face up to EUR 150,000, or EUR 5 million or 10% of annual total turnover for serious, repeated or systematic breaches (§ 35(3)).

Recent actions: on 29 April 2026 the FMA fined the chief executive of an entity EUR 4,000 for unauthorised money remittance through a clearing system moving funds to and from abroad (ZaDiG 2018 § 99(1)). On 17 March 2026 it fined NOTARTREUHANDBANK AG EUR 127,500 for inadequate ongoing monitoring controls under the FM-GwG; the order is under appeal.

10 Recent changes and what to watch

- **29 October 2026** `In force` BGBl. I No. 94/2026 amended the FM-GwG and the WiEReG, transposing Directive (EU) 2024/1640; all its FM-GwG changes took effect on 30 October 2026 (FM-GwG § 43(8)).
- **29 October 2026** `Adopted, effective 10 Jul 2027` The same law enacted the Beneficial Owners Register Act 2027, replacing the current WiEReG.
- **29 October 2026** `Council position adopted; Parliament approval pending` Payment Services Regulation and Payment Services Directive 3: the agreed Regulation requires an IBAN and name check before every credit transfer, makes providers liable for impersonation ("spoofing") fraud where their controls fail, and lets payment institutions share fraud data. It is to apply 21 months after entry into force.
- **1 October 2026** `Final draft, not adopted` AMLA published and submitted to the Commission its standards on customer due diligence and on business relationships and occasional transactions (final reports dated 30 September 2026).
- **10 June 2026** `Adopted, effective 20 Nov 2026` Consumer Credit Act 2026 published; from 20 November 2026 third-party buy-now-pay-later requires full consumer credit compliance.
- **19 June 2024** `Adopted, applies 10 Jul 2027` EU AML Regulation (2024/1624) published; it becomes the directly applicable CDD rulebook.
- **19 March 2024** `Deadline 9 Apr 2027` Instant Payments Regulation (2024/886) published; euro-area payment and e-money institutions must offer instant euro transfers.

11 What this means for identity verification

- Design remote onboarding around the four § 6(4) safeguards; a selfie and document photo alone does not qualify.
- For automated flows, read and validate the chip of the ID document, run a video-based presence check (passive is allowed) and obtain explicit biometric consent.
- Keep audio recordings, screenshots or signed chip data, and the result of each check, for ten years after the relationship ends.
- Treat the first-payment and qualified-signature routes as fraud-exposed: the A-FIU has seen forged IDs pass them, so add document and duplicate-identity checks.
- Route customers acting as trustees to in-person identification.

- Plan for July 2027: the AML Regulation recognises eIDAS electronic identification at assurance level substantial or high, and AMLA's standards will set the detail of non-face-to-face 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:

- Video KYC that can be configured to the Online-IDV steps: full recording, face and both-sides ID capture, random code and one-time code.
- Automated identity verification with NFC chip reading of e-passports and eID cards, face match and biometric liveness detection.
- AML screening against sanctions, PEP and adverse-media lists at onboarding and through ongoing monitoring.
- KYB and beneficial owner verification for business customers and merchants.
- No-code workflow builder with an audit trail of every 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

- **Zahlungsdienstegesetz 2018 (ZaDiG 2018) [Payment Services Act 2018]**, §§ 7, 8, 15, 16, 22, 87, 88, 99, 101a, consolidated version as of 11 November 2026, RIS, ris.bka.gv.at
- **E-Geldgesetz 2010 [E-Money Act 2010]**, §§ 3, 4, 11, 15, 29, consolidated version as of 11 November 2026, RIS, ris.bka.gv.at

- **Finanzmarkt-Geldwäschegesetz (FM-GwG) [Financial Markets Anti-Money Laundering Act]**, §§ 2, 5 to 9, 11, 12, 13, 16, 21, 23, 25, 34, 35, 43 and Annex III, consolidated version as of 11 November 2026, RIS, ris.bka.gv.at
- **Online-Identifikationsverordnung (Online-IDV) [Online Identification Regulation]**, BGBl. II No. 5/2017 as last amended by BGBl. II No. 470/2022, §§ 1, 3, 4, 5, RIS, ris.bka.gv.at
- **BGBl. I No. 94/2026** (Beneficial Owners Register Act 2027 and amendments to the WiEReG and FM-GwG), published 29 October 2026, RIS, ris.bka.gv.at
- **BGBl. I No. 36/2026, Verbraucherkreditrechts-Änderungsgesetz 2026 [Consumer Credit Law Amendment Act 2026]**, Article 2 (Verbraucherkreditgesetz 2026), §§ 17, 39, 43, 45, published 10 June 2026, RIS, ris.bka.gv.at
- **Sanktionengesetz 2024 (SanktG 2024) [Sanctions Act 2024]**, §§ 7, 12, consolidated version as of 11 November 2026, RIS, ris.bka.gv.at
- **E-Government-Gesetz [E-Government Act]**, §§ 4, 14, consolidated version as of 11 November 2026, RIS, ris.bka.gv.at
- **Bankwesengesetz (BWG) [Banking Act]**, §§ 1(1), 4(1), consolidated version as of 11 November 2026, RIS, ris.bka.gv.at
- **BGBl. I No. 5/2026, Finanzmarktsammelgesetz [Financial Markets Omnibus Act]**, amendments to ZaDiG 2018 (§§ 88(9), 101a), published 18 February 2026, RIS, ris.bka.gv.at
- **FMA Circular 01/2022 on Due Diligence Obligations for the Prevention of Money Laundering and Terrorist Financing**, 23 February 2022, MN 246 to 283 and 309 to 316, fma.gv.at
- **Business Service Portal, ID Austria für Unternehmen und behördliche Einrichtungen [ID Austria for businesses and public bodies]**, last updated 28 April 2026, usp.gv.at
- **FMA, The legal basis under national and European law** (AML regulations and circulars), fma.gv.at
- **FMA, Payment Institutions** (Instant Payments Regulation summary), fma.gv.at
- **FMA, Announcement: sanction for unauthorised money remittance business**, 29 April 2026, fma.gv.at
- **FMA, Announcement: sanction against NOTARTREUHANDBANK AG**, 17 March 2026, updated 13 April 2026, fma.gv.at
- **A-FIU, Lagebericht Geldwäsche 2025 [Money Laundering Situation Report 2025]**, September 2026, pp. 14, 17 to 18, 31, 39 to 41, bundeskriminalamt.at
- **Regulation (EU) 2024/1624 (Anti-Money Laundering Regulation)**, OJ L 2024/1624, 19 June 2024, recital 66, Articles 22 and 90, Annex III, EUR-Lex, eur-lex.europa.eu
- **Regulation (EU) 2022/2554 (Digital Operational Resilience Act, DORA)**, Articles 2, 9, 28 and 64, EUR-Lex, eur-lex.europa.eu
- **Commission Delegated Regulation (EU) 2024/1774 (RTS on ICT risk management framework)**, Articles 20 and 21, EUR-Lex, eur-lex.europa.eu
- **FMA, Announcement: sanction on Western Union International Bank GmbH for breaches of DORA notification obligations**, 14 July 2026, fma.gv.at

- **Regulation (EU) 2024/886 (Instant Payments Regulation)**, OJ L 2024/886, 19 March 2024, Article 1 (new Articles 5a and 5c of Regulation (EU) No 260/2012), EUR-Lex, eur-lex.europa.eu
- **Council of the EU, Statement of the Council's reasons, Position at first reading on the Payment Services Regulation**, 8543/1/26 REV 1 ADD 1, 29 October 2026, consilium.europa.eu
- **Council of the EU, Position of the Council at first reading on the Payment Services Regulation**, 8543/1/26 REV 1, 4 November 2026, Article 124, consilium.europa.eu
- **AMLA, Press release: AMLA finalises key standards for the private sector**, 1 October 2026, amla.europa.eu
- **AMLA, Final Report: Draft Regulatory Technical Standards under Article 28(1) of Regulation (EU) 2024/1624**, 30 September 2026, amla.europa.eu