Identomat

COMPLIANCE GUIDE

Crypto & Virtual Assets Compliance in Austria

COUNTRY Austria

INDUSTRY Crypto & Virtual Assets

LAST UPDATED 11 November 2026

KEY REGULATORS Financial Market Authority (FMA) · Financial Intelligence Unit (A-FIU) · Federal Ministry of Finance

Key takeaways

- Any business offering crypto services to people in Austria needs an EU licence under the Markets in Crypto-Assets Regulation (MiCAR). The Financial Market Authority (FMA) grants it in Austria; a licence from another EU country can be used in Austria after a notification.
- The old Austrian registration for virtual-currency providers stopped being enough after 31 December 2025. Firms without a MiCAR licence may not provide crypto services in Austria.
- Customers can be onboarded fully online, but only by the methods Austrian law lists: video identification, the national electronic ID (ID Austria), a qualified electronic signature, or a first payment from the customer's own account at a regulated bank.
- Fully automated selfie-and-document checks are allowed only with identity documents whose chip data is digitally signed by the issuing authority, plus a check that the customer is really present. Recordings and check results must be kept for ten years.
- Every crypto transfer must carry the sender's and recipient's identity data (the "Travel Rule"). For transfers over EUR 1,000 to or from a self-hosted wallet (one not held with a provider), the provider must assess whether its customer owns or controls that wallet. New EU anti-money laundering rules apply from 10 July 2027.

Austria is open to crypto businesses, on EU terms. The national transition window for providers registered under the old anti-money laundering regime closed on 31 December 2025, so every crypto-asset service provider (CASP) serving Austrian customers now needs a MiCAR authorisation, either from the FMA or passported from another member state.

The FMA is the single competent authority for licensing, conduct and anti-money laundering (AML) supervision of CASPs. Suspicious transactions go to the Financial Intelligence Unit at the Federal Criminal Police Office (A-FIU), and tax reporting on crypto users runs through the Ministry of Finance.

The biggest practical obstacle for a new entrant is remote onboarding design. Austria has its own fixed list of remote identification methods and a detailed regulation on video and biometric identification. A fully automated selfie-plus-document flow does not meet it unless it reads the signed chip data of the ID document.

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
Financial Market Authority (FMA)	MiCAR competent authority: CASP authorisation, conduct and market abuse supervision; AML supervisor of CASPs; sanctions authority for financial market participants	National	fma.gv.at
Financial Intelligence Unit (A-FIU), Federal Criminal Police Office	Receives suspicious transaction reports	National	bundeskriminalamt.at
Federal Ministry of Finance	AML policy and national risk assessment; crypto tax reporting (DAC8)	National	bmf.gv.at
Data Protection Authority	GDPR supervision, including biometric identification	National	dsb.gv.at
European Securities and Markets Authority (ESMA) and European Banking Authority (EBA)	MiCAR technical standards and guidelines, EU register of authorised CASPs; EBA Travel Rule guidelines	Supranational	esma.europa.eu

The EU Anti-Money Laundering Authority (AMLA) drafts the technical standards for the EU AML rulebook that applies from July 2027. Tax reporting compliance under the crypto reporting law is checked by the Large Taxpayers Office (Finanzamt für Großbetriebe).

2 Licensing and authorisation

Under Article 59 MiCAR, crypto-asset services may be provided in the EU only by a legal person authorised as a CASP, or by a bank, investment firm, e-money institution or other financial entity listed in Article 60 that has notified its regulator. The **MiCAR Enforcement Act** (MiCA-Verordnung-Vollzugsgesetz, MiCA-VVG) § 1 names the FMA as Austria's competent authority. MiCAR covers asset-referenced tokens, e-money tokens and other crypto-assets; tokens that qualify as financial instruments fall under MiFID II instead.

Requirements and timeline

- **Presence:** registered office in a member state where at least part of the services is provided, effective management in the EU and at least one director resident in the EU (Article 59(2) MiCAR).
- **Capital:** the higher of a permanent minimum and one quarter of the previous year's fixed overheads (Article 67): EUR 50,000 for class 1 services (such as order execution, transfer services, advice or portfolio management), EUR 125,000 for class 2 (adding custody and crypto exchange), and EUR 150,000 for class 3 (operating a trading platform) (Annex IV).
- **Process:** applications use the FMA's form and are filed through its Incoming platform. The FMA confirms receipt within five working days, checks completeness within 25 working days, and completes its assessment within 40 (at most 60) working days once the file is complete. On 11 November 2026 the FMA company database listed 13 CASPs authorised in Austria.

Passporting and transition

A CASP authorised elsewhere in the EU may serve Austria after notifying its home regulator under Article 65 MiCAR. Non-EU firms may serve Austrian clients without authorisation only at the client's own exclusive initiative; any solicitation in the EU removes that exemption (Article 61). Providers registered under the Financial Markets Anti-Money Laundering Act (FM-GwG) could continue until 31 December 2025 at the latest (MiCA-VVG § 23). The EU-wide transition ended on 1 July 2026, and the FMA has relayed ESMA's expectation that unauthorised providers stop onboarding and wind down.

3 AML, KYC and customer due diligence

CASPs are financial institutions under the **Financial Markets Anti-Money Laundering Act** (FM-GwG) § 2 no. 2 letter i, and are supervised by the FMA. The definition in § 2 no. 22 covers every MiCAR crypto-asset service except advice on crypto-assets.

When due diligence applies

At the start of every business relationship; for occasional transactions of EUR 15,000 or more; for occasional transfers of funds above EUR 1,000; and whenever there is a suspicion or doubt about earlier data (FM-GwG § 5).

Risk classification and enhanced due diligence

Every customer is placed in a risk class (§ 6(5)). Higher risk triggers enhanced due diligence (§ 9(1)); for high-risk third countries this includes extra source-of-funds information and senior management approval (§ 9a(1)).

Self-hosted wallets

CASPs must assess the money laundering, terrorist financing and sanctions risk of transfers to or from self-hosted addresses. They must apply at least one mitigating measure, such as verifying the counterparty's identity, asking for origin and destination data, or enhanced monitoring (§ 11a).

Timing and beneficial owners

Identity must be established and verified before the relationship begins; verification may be completed during onboarding only where needed to avoid interrupting business and the risk is low (§ 7(1) and (2)). For entity customers covered by the beneficial owners register law (WiEReG), an extract from that register is required at the start (§ 7(1)).

Monitoring, reporting and records

Transaction monitoring may be run or supplemented with artificial intelligence or other advanced technology, if the conditions in FM-GwG § 7a are met. Suspicious transaction reports go to the A-FIU without delay (§ 16(1)), through its goAML application, reached via the Business Service Portal with ID Austria. CASPs filed 2,671 reports in 2025, about 117% more than in 2024, according to the A-FIU's annual report. Copies of due diligence documents, including data from electronic identification and remote identification methods, must be kept for **ten years** after the relationship ends or after the occasional transaction (§ 21(1)).

Travel Rule

Under Regulation (EU) 2023/1113, every crypto transfer must carry the originator's name, ledger address or account number, and address with official document number and customer number (or date and place of birth), plus the beneficiary's details. The originator's CASP must verify the originator's details before the transfer, which counts as done where the customer was identified under AML rules, and may not execute it until it fully complies (Article 14(6) to (8)). There is no minimum amount. Breaches are punishable under FM-GwG § 34(2).

Sanctions

CASPs count as financial market participants under the Sanctions Act 2024 (Sanktionengesetz 2024) § 1(4). They need written sanctions strategies, controls and procedures approved by the management body (§ 7), and the FMA monitors their compliance (§ 12(2)).

4 Identity verification and onboarding

In person, identity is verified by presenting an official photo ID (FM-GwG § 6(2)). Where there is no personal contact, FM-GwG § 6(4) lets the firm replace that with one of four safeguards. In every case the firm must know the customer's name, date of birth and address (for legal entities, the company name and seat):

- **Online identification:** presenting the official photo ID in a video-supported electronic procedure, under the FMA's **Online Identification Regulation** (Online-IDV).
- **Electronic ID:** a statutory procedure that securely provides the same information as an official photo ID, such as ID Austria.
- **Qualified electronic signature:** the customer signs with a qualified electronic signature under eIDAS. Alternatively, the contract can go by registered post to the customer's home address, with further conditions (including a copy of the ID before signing).
- **First payment:** the first payment comes from an account in the customer's name at a credit institution in Austria, another member state or a third country with equivalent AML rules (§ 13(3) and (4)), with document copies or the bank's written confirmation of identification.

Video identification (Online-IDV)

Trained staff run the session (§ 3), which is audio-recorded in full, with screenshots of the face and both sides of the ID (§ 4(2)). The ID needs optical security features at least equal to holograms (§ 2 point 2). The customer moves their head and reads out the ID number or a random code (§ 4(3)), the agent checks security features, laminate, photo and data consistency (§ 4(4)), and the customer enters a one-time code sent by email or SMS (§ 4(5)). Inconsistencies or uncertainties end the session (§ 5(1)).

Automated biometric identification

Under Online-IDV § 4(6), a fully automated process must meet the state of the art, be at least as secure as an agent-led session and **only use photo IDs whose content is electronically signed by the issuing authority** (in practice, read from the chip). The firm verifies the signature, data integrity and that the signing key is not compromised. A presence check based on video captured during the session, which may be passive, replaces the head-movement and code steps. Every step and its result must be documented.

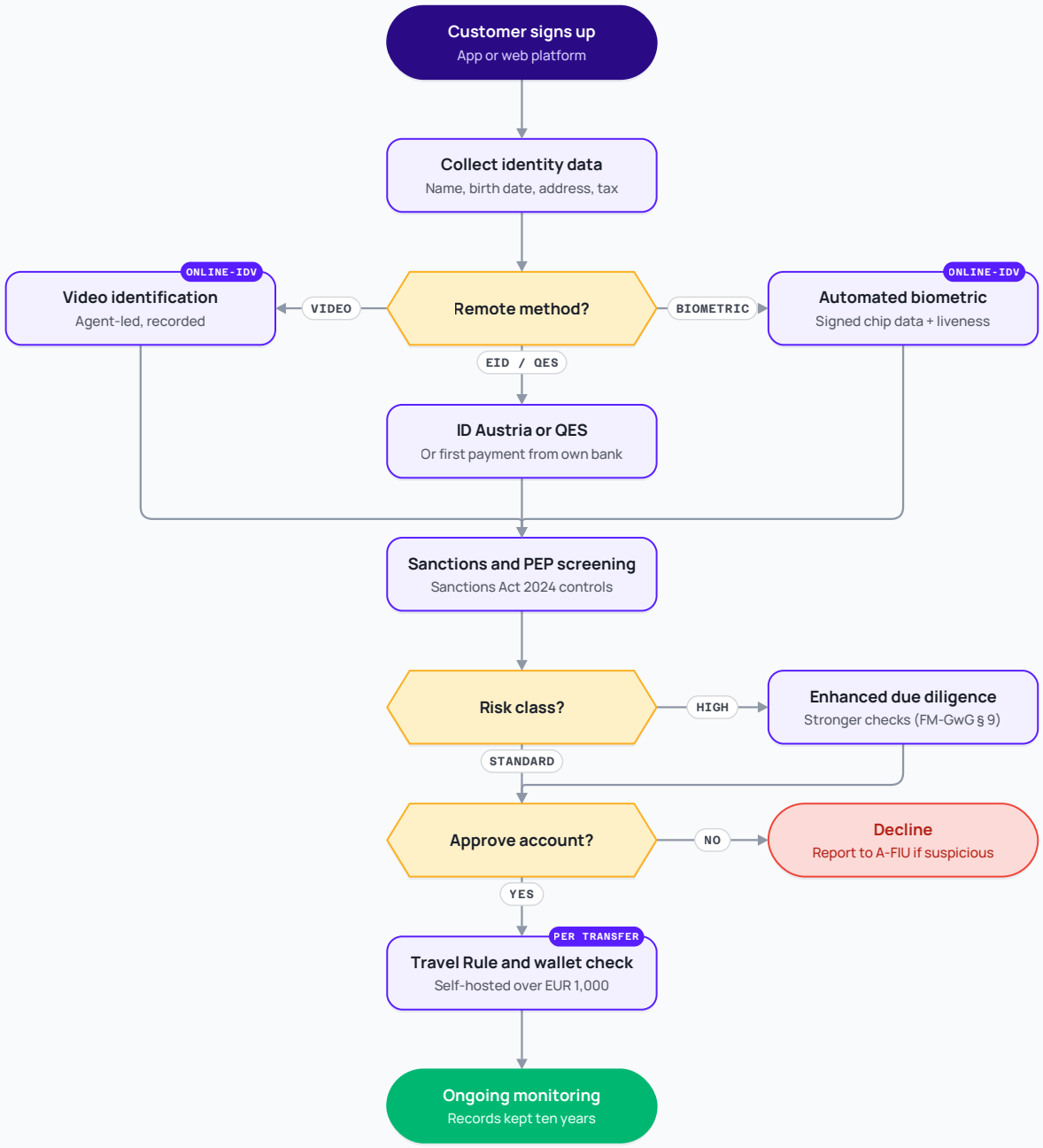


Figure 1. Remote onboarding of a customer by a crypto-asset service provider in Austria.

5 Digital channels: what's different

Bottom line: remote onboarding is fully permitted, but only through four statutory methods. Automated selfie checks must read the issuer-signed chip data of the ID document.

Requirement	In person	Online / remote	Difference
How identity is verified	Official photo ID presented in person	One of four safeguards: video, eID, QES, first payment	Differs
Risk treatment	Standard risk factors	Non-face-to-face without safeguards such as eID is a higher-risk factor	Differs
Document requirements	Official photo ID	Video: hologram-grade security features; biometric: issuer-signed chip data only	Differs
Liveness	Not applicable	Head movement and code (video) or presence check, which may be passive (biometric)	Differs
Evidence captured	Copy of the ID	Full audio recording and screenshots, or recordings and step-by-step results	Differs
Minimum data known	Name, date of birth, address	Name, date of birth, address	Same
Record retention	Ten years	Ten years	Same
Travel Rule data on transfers	Required, no minimum amount	Required, no minimum amount	Same

Remote is not automatically high risk

FM-GwG Annex III treats relationships "without personal contact and without certain safeguards", such as electronic identification, as a higher-risk factor. With a § 6(4) safeguard in place, normal risk classification applies; the Online-IDV controls exist to offset the higher risk of remote identification (§ 1(1)).

Chip reading is the gateway to automation

Video identification accepts any official photo ID with hologram-grade features; automated flows accept only documents with issuer-signed data, verified cryptographically (Online-IDV § 4(6)(5)). Product teams need near-field communication (NFC) chip reading, or an agent-led video fallback.

Outsourced identification

A processor may run online identification to the same standard under a written agreement; final responsibility stays with the CASP (Online-IDV § 6(1)).

Pending

The EU Anti-Money Laundering Regulation `Adopted, applies 10 Jul 2027` lets firms verify identity with an identity document or with electronic identification at eIDAS assurance level "substantial" or "high" (Article 22(6)). AMLA's draft technical standards on due diligence `Final draft, not adopted` would allow other remote document-based tools only where neither route is available, with a recorded justification.

6 Data protection and biometrics

The Online-IDV sets the legal basis for video identification data as FM-GwG § 6(4), processed to prevent money laundering and terrorist financing (Online-IDV § 4(1)). For automated biometric procedures, it requires that processing be permissible under **Article 9(2)(a) GDPR**, which means the customer's explicit consent. The firm must also take technical and organisational measures that give a level of security appropriate to the risk under Article 32 GDPR (Online-IDV § 4(6)). Customers who refuse biometric processing need another route, such as agent-led video or ID Austria. Recordings are kept as AML records for ten years (FM-GwG § 21), and Travel Rule data must be sent securely and in line with the GDPR (Regulation (EU) 2023/1113, Article 14(4)).

7 Sector-specific obligations

Self-hosted wallets

For transfers to a self-hosted address, the originator's CASP must obtain and hold the originator and beneficiary information. Above **EUR 1,000** it must assess whether the address is owned or controlled by its own customer (Regulation (EU) 2023/1113, Article 14(5)); the beneficiary's CASP has the same duty for incoming transfers (Article 16(2)). FM-GwG § 11a adds risk-based measures, and the FMA publishes the EBA's Travel Rule guidelines.

Tax reporting on crypto users (DAC8)

The **Crypto Reporting Obligation Act** (Krypto-Meldepflichtgesetz, Krypto-MPfG), in force since 1 January 2026, implements Directive (EU) 2023/2226. When a new relationship begins, a reporting CASP must obtain a tax self-certification from which it can determine the user's tax residence, and confirm that it is reasonable using the AML/KYC data it holds. A relationship may be opened only once a valid self-certification is in place (§ 28(1) and (3)). For existing users the deadline is **1 January 2027** (§ 28(2)). Reports cover the calendar year, are due by 31 July of the following year (§ 19) and are filed through FinanzOnline (Krypto-MPfG Implementing Regulation § 4).

Capital gains tax withholding

CASPs with their seat or management in Austria, and Austrian branches of foreign CASPs, are the withholding agents for capital gains tax on their customers' realised gains from cryptocurrencies, and on current crypto income where there is no domestic debtor (Income Tax Act 1988 § 95(2)).

8 Risk indicators and red flags

CRYPTO TYPOLOGIES (A-FIU 2025 REPORT AND FATF)

- **Cyber-trading fraud**: fake trading platforms; fraudsters use remote-access software on victims' computers, move funds through crypto and demand "fees" before any payout.
- **Exchange impersonation**: fraudsters posing as crypto exchanges induce "security transfers" to their own wallets.
- **Deepfakes**: manipulated video and audio used to defeat online identification.
- **Scam-centre and "pig-butchering" proceeds**: often moved through stablecoins and peer-to-peer transfers via unhosted wallets.
- **Profile mismatch**: a new user makes a large initial deposit inconsistent with their profile.
- **Rapid layering**: assets moved immediately to several providers, offshore VASPs or cross-chain tools.
- **Anonymity tools**: funds linked to mixers, privacy coins or peer-to-peer platforms.

9 Enforcement and penalties

Breach	Responsible individuals	Legal persons
Providing crypto-asset services without authorisation (MiCA-VVG § 11 no. 3)	Up to EUR 700,000 or twice the benefit gained	Up to EUR 5 million, 5% of annual turnover, or twice the benefit (§ 15(3))
AML duties, including due diligence, reporting and Travel Rule breaches (FM-GwG § 34(1) and (2))	Up to EUR 150,000	Up to EUR 150,000 (§ 35(3))
Serious, repeated or systematic AML breaches (FM-GwG § 34(4))	Up to EUR 5 million or twice the benefit	Up to EUR 5 million or 10% of annual turnover (§ 35(3))

Turnover is taken from the last approved annual accounts. An FMA decision of 31 July 2026, announced on 29 October 2026, ordered Senta Tech Limited Liability Company (ultima.io, utrading.com), based in Georgia, to stop unauthorised portfolio management of crypto-assets in Austria under MiCA-VVG § 11 no. 3. An earlier order (September 2025) targeted another unlicensed crypto portfolio manager. On the AML side, the FMA fined Coinfinity GmbH, now an FMA-authorised CASP, EUR 105,000 in October 2025 for weaknesses in its company-wide risk assessment, staff training and due diligence procedures for occasional transactions. The penal order is final.

10 Recent changes and what to watch

- **10 July 2027:** `Adopted, applies 10 Jul 2027` The Anti-Money Laundering Regulation (EU) 2024/1624 applies directly. CASPs must apply full due diligence to occasional transactions of EUR 1,000 or more, and at least identify the customer below that amount (Article 19(3)).
- **10 July 2027:** `Adopted, effective 10 Jul 2027` A new Beneficial Owners Register Act 2027 (BGBl. I No. 94/2026) replaces the current Beneficial Owners Register Act, which is repealed on that date.
- **1 January 2027:** `In force, deadline 1 Jan 2027` Tax self-certifications must be collected from all existing users under the Krypto-MPfG. The first annual DAC8 report is due by 31 July 2027.

- **30 October 2026:** `In force` BGBl. I No. 94/2026 (published 29 October 2026), focused on the beneficial owners register, amended the FM-GwG with effect from the following day.
- **1 October 2026:** `Final draft, not adopted` AMLA published its final draft standards on due diligence and submitted them to the European Commission. Selfie and video tools would become a justified fallback where an ID document or eIDAS "substantial" or "high" electronic identification cannot be used.
- **1 July 2026:** `In force` The EU-wide MiCAR transition period ended. Unauthorised providers must stop onboarding and wind down.
- **30 April 2026:** `Published` The FATF mutual evaluation of Austria found that the virtual asset sector presents high money laundering and terrorist financing risks, and rated Recommendations 15 (new technologies) and 16 (wire transfers) largely compliant.

11 What this means for identity verification

- **Documents:** agent-led video needs an official photo ID with hologram-grade optical features. Fully automated flows accept only IDs with issuer-signed chip data, so plan NFC reading and certificate checks.
- **Methods:** offer at least two of the four statutory routes. ID Austria or a qualified electronic signature is a natural fallback for customers who decline biometric processing.
- **Liveness:** automated flows need a video-based presence check, which may be passive. Agent-led video uses head movement, a spoken code and a one-time code.
- **Data set:** name, date of birth, address and a tax self-certification before the account opens.
- **Evidence:** keep audio recordings, screenshots or biometric session recordings, and each step's result for ten years after the relationship ends.
- **Re-verification triggers:** doubts about earlier data, changes that make a tax self-certification unreliable, and transfers above EUR 1,000 to or from self-hosted wallets (ownership check).
- **2027 changes:** from 10 July 2027 the EU AML Regulation favours ID documents and eIDAS "substantial" or "high" electronic identification; keep chip-based and video flows, but expect to justify them if AMLA's draft standards are adopted.

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 KYC onboarding with ID document capture and NFC chip verification, face match and biometric liveness.
- Agent-led video KYC as a fallback for customers whose documents cannot be read by chip.
- AML screening against sanctions, PEP and adverse-media lists at onboarding and through ongoing monitoring.
- KYC questionnaires for source of funds and tax self-certification data, configured in a no-code workflow builder.
- Audit trail of each verification step to support long-term record retention.

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

- **MiCA-Verordnung-Vollzugsgesetz (MiCAR Enforcement Act, MiCA-VVG), BGBl. I No. 111/2024 as amended**, §§ 1, 11, 15, 23, 28, RIS consolidated version of 11 November 2026, ris.bka.gv.at
- **Finanzmarkt-Geldwäschegesetz (Financial Markets Anti-Money Laundering Act, FM-GwG), BGBl. I No. 118/2016 as amended**, §§ 2, 5, 6, 7, 7a, 9, 9a, 11a, 13, 16, 21, 34, 35 and Annex III, RIS consolidated version of 11 November 2026, ris.bka.gv.at
- **Online-Identifikationsverordnung (Online Identification Regulation, Online-IDV), BGBl. II No. 5/2017 as amended**, §§ 1 to 6, RIS consolidated version of 11 November 2026, ris.bka.gv.at
- **Sanktionengesetz 2024 (Sanctions Act 2024)**, §§ 1(4), 7, 12, RIS consolidated version of 11 November 2026, ris.bka.gv.at

- **Krypto-Meldepflichtgesetz (Crypto Reporting Obligation Act, Krypto-MPfG), BGBl. I No. 96/2025**, §§ 3, 19, 28, 29, 46, RIS consolidated version of 11 November 2026, ris.bka.gv.at
- **BGBl. I No. 94/2026** (Beneficial Owners Register Act 2027 and amendments to the FM-GwG), published 29 October 2026, ris.bka.gv.at
- **Regulation (EU) 2023/1114 on markets in crypto-assets (MiCAR)**, Articles 59 to 61, 65, 67 and Annex IV, eur-lex.europa.eu
- **Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets**, Articles 14 and 16, eur-lex.europa.eu
- **Regulation (EU) 2024/1624 (Anti-Money Laundering Regulation)**, Articles 19(3) and 22(6) and date of application, eur-lex.europa.eu
- **FMA, Markets in Crypto-Assets Regulation (MiCAR)**, fma.gv.at
- **FMA, Informationen für CASP-Zulassungswerber (information for CASP applicants)**, fma.gv.at
- **FMA, End of the MiCAR Transition Period: ESMA states clear rules for unauthorised providers**, 23 June 2026, fma.gv.at
- **FMA, Announcement: FMA imposes sanction on Senta Tech Limited Liability Company**, 29 October 2026, fma.gv.at
- **Einkommensteuergesetz 1988 (Income Tax Act 1988)**, § 95(2), RIS consolidated version of 11 November 2026, ris.bka.gv.at
- **Krypto-MPfG-Durchführungsverordnung (Krypto-MPfG Implementing Regulation), BGBl. II No. 331/2025**, § 4, ris.bka.gv.at
- **AMLA, Final Report: Draft Regulatory Technical Standards under Article 28(1) of Regulation (EU) 2024/1624**, 30 September 2026, Article 7 of the draft, amla.europa.eu
- **AMLA, Press Release: AMLA finalises key standards for the private sector**, 1 October 2026, amla.europa.eu
- **Federal Criminal Police Office, Geldwäscherei (A-FIU reporting via goAML)**, bundeskriminalamt.at; **Lagebericht Geldwäsche 2025 (Money Laundering Situation Report 2025)**, September 2026, pp. 29 to 30, 41 to 42, 47 to 51, bundeskriminalamt.at
- **FMA, Announcement: FMA imposes sanction against Coinfinity GmbH for breaches of due diligence obligations**, 6 October 2025, fma.gv.at
- **FMA, Announcement: FMA imposes sanction against Quantum Data Analytics e.U. for unauthorised offering of portfolio management of crypto-assets**, 30 September 2025, fma.gv.at
- **FMA, sanctions archive**, fma.gv.at
- **FMA company database, category "CASP - Crypto-Asset Service Provider (AT)"**, searched 11 November 2026, fma.gv.at
- **FATF, Mutual Evaluation Report of Austria, 2026**, overview and technical compliance annex (Recommendations 15 and 16), fatf-gafi.org
- **FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs**, July 2026, Key Findings, fatf-gafi.org

- **FATF, Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (handout for VASPs)**, September 2020, fatf-gafi.org