



Identomat

COMPLIANCE GUIDE

Crypto & Virtual Assets Compliance in Romania

COUNTRY **Romania**

INDUSTRY **Crypto & Virtual Assets**

LAST UPDATED **21 October 2026**

KEY REGULATORS **Financial Supervisory Authority · National Bank of Romania · National Office
for the Prevention and Combating of Money Laundering**

Key takeaways

- Crypto exchanges, brokers and custodial wallets in Romania need an authorisation under the EU Markets in Crypto-Assets Regulation (MiCA). The old Romanian registration regime has been repealed, and the transition period for firms already operating ended on 1 July 2026.
- Romania has not yet adopted the national law that names the authority granting MiCA licences or sets local penalties (a draft would give this role mainly to the Financial Supervisory Authority). Until it is, providers serve Romanian customers on a licence from another EU country, passported to Romania, or as an already regulated firm (such as a bank or investment firm) adding crypto services.
- Every crypto-asset service provider is covered by Romania's anti-money laundering law: identity must be verified before the account opens, suspicious activity is reported before the transaction goes ahead, and records are kept for five years.
- Fully online onboarding is allowed. Electronic identity, trust services and remote processes approved by the Authority for the Digitalisation of Romania count as reliable evidence, while remote onboarding without such safeguards is treated as a higher-risk factor.
- Every crypto transfer must carry sender and recipient details (the "travel rule"). From 2026, platforms also report users' tax details to the tax agency each year and must block exchange transactions for users who refuse to provide them.

Romania is open to crypto businesses, but on EU terms. Market access is governed by Regulation (EU) 2023/1114 (MiCA), which applies directly, and the anti-money laundering (AML) layer by Law no. 129/2019 as amended in March 2025 to cover all crypto-asset service providers. The tax layer comes from the Fiscal Code and the Fiscal Procedure Code.

The principal authorities are the Financial Supervisory Authority (ASF) and the National Bank of Romania (BNR) as AML supervisors of the financial entities they already regulate, the National Office for the Prevention and Combating of Money Laundering (ONPCSB) as the financial intelligence unit, and the National Agency for Fiscal Administration (ANAF) for tax reporting.

The biggest obstacle for a new entrant is the missing national MiCA implementing act: as of 21 October 2026 no Romanian authority has been designated by law to grant stand-alone crypto-asset service provider licences, so a firm wanting a Romanian licence rather than a passport has to wait.

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 Supervisory Authority (ASF)	AML supervisor of investment firms, market operators, central securities depositories and fund managers providing crypto services under Article 60 MiCA; proposed MiCA competent authority	National	asf.romania.ro
National Bank of Romania (BNR)	AML supervisor of credit institutions and e-money institutions providing crypto services; proposed authority for e-money tokens they issue	National	bnr.ro
National Office for the Prevention and Combating of Money Laundering (ONPCSB)	Financial intelligence unit; receives suspicious transaction and threshold reports; residual AML supervisor	National	onpcsb.ro
National Agency for Fiscal Administration (ANAF)	Crypto tax reporting (DAC8), individual income tax on crypto gains	National	anaf.ro
Authority for the Digitalisation of Romania (ADR)	Approves remote identification processes; endorses video identification providers	National	adr.gov.ro

National Trade Register Office (ONRC)	Central register of beneficial owners	National	onrc.ro
National Supervisory Authority for Personal Data Processing (ANSPDCP)	Data protection, including biometric data used in onboarding	National	dataprotection.ro
European Securities and Markets Authority (ESMA) and European Banking Authority (EBA)	MiCA level 2 rules and registers; AML and travel rule guidelines	EU	esma.europa.eu , eba.europa.eu

Romania is a unitary state, so there are no regional crypto licences. The national MiCA competent authority has not yet been designated by law (see section 2).

2 Licensing and authorisation

MiCA applies directly

[Regulation \(EU\) 2023/1114](#) (MiCA) **In force** applies in Romania without transposition: Titles III and IV (asset-referenced and e-money tokens) from 30 June 2024 and the rest, including crypto-asset service providers (CASPs), from 30 December 2024 (Article 149). Under Article 59, crypto-asset services may be provided only by firms authorised as CASPs under Article 63, or by banks, investment firms, e-money institutions and other listed regulated entities that notify their home authority under Article 60 at least 40 working days before starting. An authorised CASP needs a registered office in a member state where it provides services, effective management in the EU and at least one EU-resident director.

Authorities have 25 working days to check completeness and 40 working days to decide (Article 63). Minimum capital is EUR 50,000, rising to EUR 125,000 with custody or exchange services and EUR 150,000 for a trading platform (Article 67 and Annex IV).

The Romanian position

Romania's previous regime for exchange and digital wallet providers (Article 30¹ of Law no. 129/2019) was repealed by Government Emergency Ordinance (OUG) no. 10/2025 in favour of the single MiCA authorisation. ESMA's list of transitional periods under Article

143(3) MiCA records 18 months for Romania; the period ended on 1 July 2026 at the latest, so pre-MiCA status no longer gives a basis to operate.

The national act implementing MiCA **Draft, not adopted** had not been published as of 21 October 2026. A Ministry of Finance draft (substantiation note of 23 May 2025) would make the ASF competent for crypto-asset services and for token issuance other than e-money tokens, the BNR competent for e-money tokens issued by credit and e-money institutions, and set the penalty regime. Until then, the routes into the market are:

- **Passporting:** a CASP authorised elsewhere notifies its home authority under Article 65 MiCA and may start once the home authority confirms transmission, or by the 15th calendar day after notifying.
- **Article 60 notification:** a Romanian bank, e-money institution, investment firm or fund manager adds crypto services to its licence, within Article 60's limits.

Firms from other member states established in Romania other than through a branch must appoint a central contact point and notify it to the BNR, the ASF or ONPCSB within 5 days of starting (Law 129/2019 Article 32¹).

3

AML, KYC and customer due diligence

Scope and supervisors

[Law no. 129/2019](#) on preventing and combating money laundering and terrorist financing **In force** treats every crypto-asset service provider as a financial institution (Article 2(g) point 8, added by [OUG 10/2025](#)) and therefore as a reporting entity under Article 5(1)(b). Firms that only give advice on crypto-assets are excluded. OUG 10/2025 has applied since 13 March 2025; its approval bill passed the Senate on 7 April 2025 and is pending in the Chamber of Deputies (PLX 107/2025), which can still amend it.

AML supervision follows the existing licence: the ASF for investment firms, market operators, central securities depositories and fund managers providing crypto services under Article 60 MiCA (Article 28(1)(b)), the BNR for credit and e-money institutions (Article 27(1)(e)). Both supervise the transfer of funds regulation for their entities (Article 29).

Customer due diligence

Standard due diligence applies when a business relationship is established, for occasional transactions of at least EUR 15,000 (single or linked), for transfers of funds of at least EUR 1,000, and whenever money laundering or terrorist financing is suspected (Article 13(1)).

The customer and beneficial owner must be verified before the relationship starts or the occasional transaction is carried out (Article 11(8)), and for corporate customers the firm must obtain proof of registration in, or information from, the beneficial owner register kept by ONRC (Article 11(8¹) and Article 19).

Enhanced due diligence applies to high-risk situations, including politically exposed persons and high-risk third countries (Article 17), and to correspondent relationships with non-EU crypto providers, which need checks on the respondent's authorisation and controls and senior management approval (Article 17²).

Reporting

Suspicious transactions

Report to ONPCSB immediately and before executing any related transaction; the transaction is held for 24 hours from registration, and ONPCSB may suspend it for up to 48 hours (Articles 6 and 8).

Cash transactions

Cash transactions of at least the lei equivalent of EUR 10,000, including linked operations, within 3 working days (Article 7(1) and (7)).

External transfers

Credit and financial institutions report external transfers into and out of accounts of at least EUR 10,000 within 3 working days (Article 7(3) and (7)); the Law does not spell out how this applies to crypto-asset transfers.

Record retention

Customer due diligence records, including electronic identification data, kept for 5 years after the relationship ends or the occasional transaction (Article 21).

From 10 July 2027 the EU AML Regulation (EU) [2024/1624](#) Adopted, applies 10 Jul 2027 will replace much of this, with due diligence for crypto occasional transactions of EUR 1,000 or more (Article 19(3)) and a ban on anonymous crypto-asset accounts (Article 79).

4

Identity verification and onboarding

Law 129/2019 requires verification from reliable and independent sources, including electronic identification means and trust services under the eIDAS Regulation (EU) No 910/2014, or any secure remote or electronic identification process approved or accepted by the Authority for the Digitalisation of Romania (Article 11(1)(a)).

Documents and the new identity card

Some of Romania's new electronic identity cards do not show the holder's address. ONPCSB reminds reporting entities that the address is still mandatory in their reports and points to the Ministry of Internal Affairs' "RO CEI Reader" application, which reads the chip, including the address, with the holder's PIN. An image of the card alone is therefore not enough to capture the address.

Video identification

Remote identification by video is regulated by the norms approved by ADR President's Decision no. 564/2021 (Official Gazette Part I no. 1119 of 24 November 2021). Providers registered in Romania need an ADR endorsement, and ADR publishes the list of endorsed verifiers.

Rules for ASF-supervised entities

For entities the ASF supervises, [ASF Regulation no. 13/2019](#) treats a relationship as remote where identity is verified by video or similar technology (Article 2(2) (k¹)). The entity must assess whether the remote channel calls for enhanced due diligence, consider the risk that the customer is not who they claim or is not a real person, and require its technology provider by contract to combine document checks with checks that the person holds an unaltered document, using more than one data source (Article 27¹).

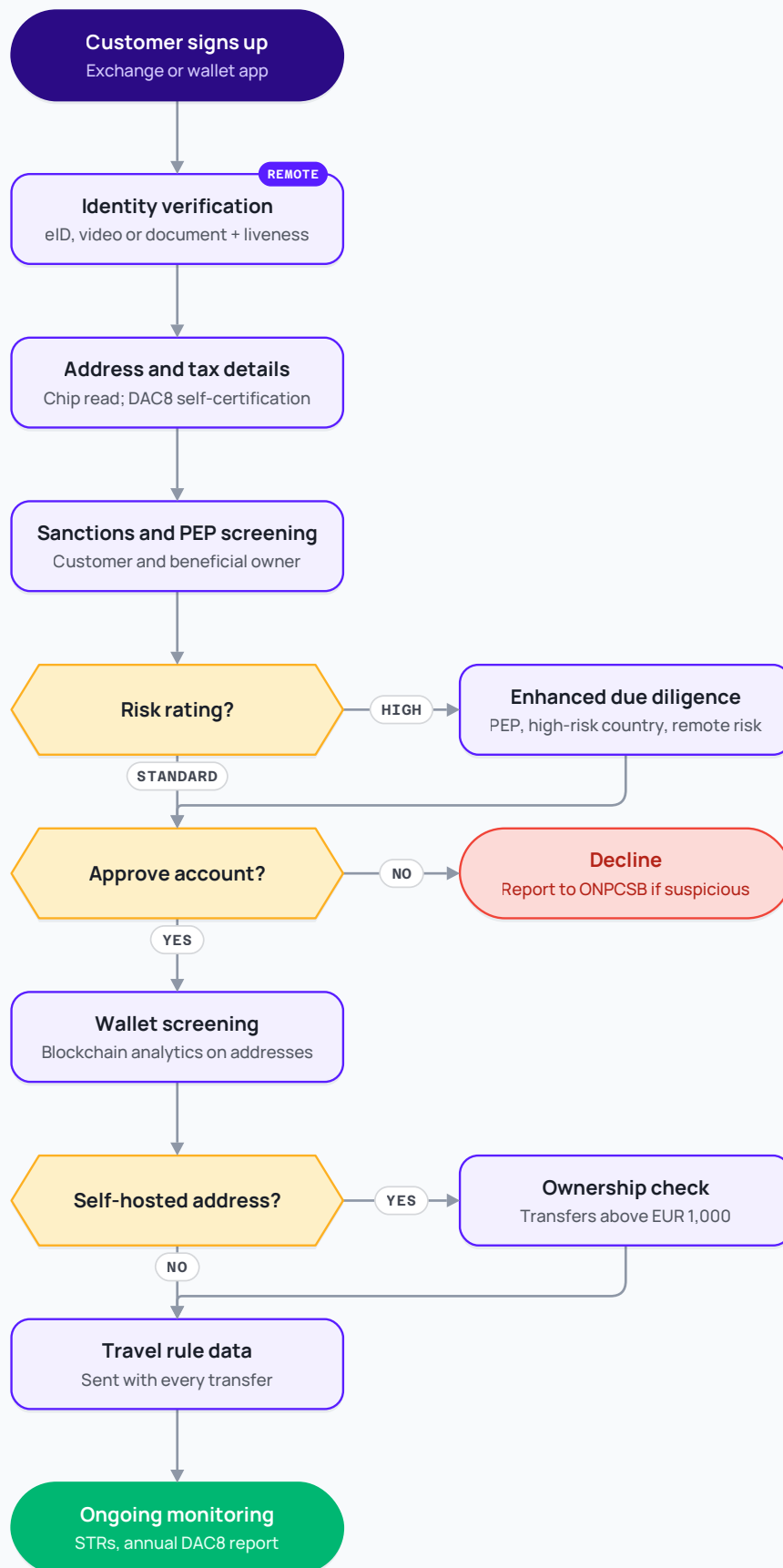


Figure 1. Remote onboarding at a crypto-asset service provider serving Romanian customers.

Bottom line: crypto services are online by nature and remote onboarding is permitted, but Romanian law treats remote onboarding without electronic identification, trust services or an ADR-approved process as a higher-risk factor, and self-hosted wallets bring extra checks that have no in-person equivalent.

Requirement	In person	Online / remote	Difference
Permission to onboard	Permitted	Permitted (Law 129/2019 Art. 11(1) (a))	Same
Risk treatment	Standard risk assessment	Remote without eID or trust services is a higher-risk factor (Art. 17(14))	Differs
Accepted evidence	Original identity document	eID, trust services, ADR-approved remote processes, video with ADR endorsement	Differs
Timing of verification	Before the relationship starts	Before the relationship starts (Art. 11(8))	Same
Address on new eID card	Can be read from the chip at the counter	Needs chip reading or a separate address step	Differs
Transfers to self-hosted wallets	Not applicable	Risk assessment; ownership check above EUR 1,000	Differs
Travel rule data	Every transfer	Every transfer, no minimum amount	Same
Record retention	5 years	5 years, including electronic identification data (Art. 21)	Same

Safeguards decide the risk level

Law 129/2019 lists remote relationships "without certain safeguards, such as electronic identification means or relevant trust services" as a higher-risk factor (Article 17(14)). The EBA's risk factor guidelines for crypto-asset service providers (EBA/GL/2024/01, from 30

December 2024) add remote onboarding that does not follow its remote onboarding guidelines (EBA/GL/2022/15) (Guideline 21.9(a)).

Self-hosted wallets

Providers must assess the risk of transfers to and from self-hosted addresses and mitigate it, for example by verifying the counterparty's identity, asking about the origin and destination of the assets or monitoring more closely, including against sanctions evasion (Law 129/2019 Article 25(5)-(7)). For transfers above EUR 1,000 they must also assess whether the customer owns or controls the address.

What is changing

The national MiCA act **Draft, not adopted** would create a domestic licensing route, and the AML Regulation **Adopted, applies 10 Jul 2027** sets a EUR 1,000 threshold for occasional crypto transactions.

6 Data protection and biometrics

The [General Data Protection Regulation](#) applies directly, supplemented by [Law no. 190/2018](#) (Official Gazette Part I no. 651 of 26 July 2018), which sets special rules for biometric data and conditions for processing the personal numeric code (CNP). Face matching and liveness checks process biometric data, a special category under the GDPR, so providers need a documented legal basis, starting from the AML obligation in Law 129/2019.

AML and travel rule records are kept for 5 years, after which travel rule personal data must be deleted unless national law provides otherwise (Law 129/2019 Article 21; Regulation 2023/1113 Article 26). DAC8 records are kept for 5 to 10 years (Fiscal Procedure Code Article 291⁶(7)).

7 Sector-specific obligations

Travel rule

[Regulation \(EU\) 2023/1113](#) **In force** has applied since 30 December 2024. The originator's provider must send names and distributed ledger addresses or account numbers of both parties, plus further originator details, with every transfer regardless of amount, and verify the originator's data first (Article 14). The beneficiary's provider must

detect missing data and reject, return or hold the transfer until it is supplied, and report providers that repeatedly fail (Articles 16 and 17). The EBA's [Travel Rule Guidelines](#) (EBA/GL/2024/11) apply from the same date.

Tax reporting (DAC8)

OUG no. 71/2025 (Official Gazette Part I no. 1146 of 10 December 2025) In force transposes Directive (EU) 2023/2226 into the Fiscal Procedure Code. Reporting providers apply the Annex 6 due diligence for periods from 1 January 2026 and report to ANAF by 15 March for the previous year (Article 291⁶). Users who still do not provide the required information after two reminders and at least 60 days must be blocked from exchange transactions (Article 291⁶(6)). [ANAF Order no. 750/2026](#) (Official Gazette Part I no. 554 of 6 July 2026) approves form F8000, which must be filed even with nothing to report.

Taxation of users

Since 1 January 2026, individuals pay 16% income tax on virtual currency gains, self-assessed in the single tax return; gains below 200 lei per transaction are exempt if annual gains do not exceed 600 lei (Fiscal Code Article 116(2¹), added by Law no. 239/2025, Official Gazette Part I no. 1160 of 15 December 2025).

CRYPTO-ASSET RISK FACTORS (EBA/GL/2024/01, GUIDELINE 21)

- **Anonymity-enhancing products:** services offering a higher degree of anonymity (21.3(a)).
- **Mixers and peer-to-peer:** transactions involving self-hosted addresses, mixers or tumblers, DeFi or peer-to-peer platforms (21.3(d)).
- **Crypto ATMs:** cash-based exchange hardware and relationships established through it (21.3(d), 21.9(f)).
- **Masked connections:** IP addresses linked to the darknet, anonymising software or VPNs (21.5(a) (vi)).
- **Illicit sources:** crypto-assets received from or sent to the darknet or illegal activity (21.5(b) (xiii)).
- **Implausible rewards:** claimed mining or staking income out of line with the activity (21.5(b) (xvii)).
- **Mule accounts:** vulnerable persons used as money mules, multiple accounts without rationale (21.5(a), 21.5(b)).
- **High-risk geography:** addresses linked to higher-risk or sanctioned jurisdictions (21.7(b)).

Under Article 43 of Law 129/2019, natural persons face a warning or fines of 25,000 to 150,000 lei for breaches of due diligence, reporting or the transfer of funds regulation, 20,000 to 120,000 lei for breaches of Article 25 (including the self-hosted address duties) and 10,000 to 90,000 lei for threshold reporting and other listed breaches. For legal persons the maximum rises by 10% of total revenues for the last closed fiscal period, and managers can also be sanctioned. Complementary sanctions include suspension or withdrawal of authorisation and a public statement (Article 44).

DAC8 failures (no, late or incorrect reports, or no due diligence) carry fines of 50,000 to 150,000 lei, and record-keeping breaches 20,000 to 100,000 lei (Fiscal Procedure Code Article 336).

MiCA requires maximum fines of at least EUR 5,000,000 or 5% of turnover for legal persons and EUR 700,000 for natural persons for CASP breaches (Article 111); Romania's amounts await the national implementing act.

10 Recent changes and what to watch

- **6 July 2026:** ANAF Order 750/2026 approves the DAC8 reporting form F8000 **In force**. Providers must file it each year, including nil returns.
- **1 July 2026:** the MiCA transitional period under Article 143(3) ended **In force**. Firms without a MiCA authorisation, a valid passport or an Article 60 notification must stop serving Romanian clients.
- **1 January 2026:** 16% tax on individuals' crypto gains and DAC8 due diligence periods begin **In force**. Onboarding must now collect tax residence information.
- **10 December 2025:** OUG 71/2025 transposes DAC8 **In force**. Sets reporting, blocking and record-keeping duties for providers.
- **23 May 2025:** Ministry of Finance draft emergency ordinance implementing MiCA **Draft, not adopted**. Would designate the ASF and the BNR and set penalties; its adoption opens a domestic licensing route.
- **13 March 2025:** OUG 10/2025 brings all crypto-asset service providers under Law 129/2019 **In force**. Parliamentary approval is pending in the Chamber of Deputies, which may amend it.
- **10 July 2027:** EU AML Regulation 2024/1624 applies **Adopted, applies 10 Jul 2027**. Introduces a EUR 1,000 due diligence threshold for occasional crypto transactions.

11 What this means for identity verification

- **Verify before activation.** Identity and beneficial ownership must be verified before the account opens; there is no deferred verification window under Law 129/2019.
- **Prefer recognised remote methods.** eID, qualified trust services and ADR-approved processes keep remote onboarding out of the higher-risk category; video identification needs an ADR-endorsed provider.
- **Plan for the new identity card.** Capture the address through chip reading or a separate step, because the card face may not show it.

- **Check document and person together.** For ASF-supervised entities, a document check alone is not enough remotely; it must be combined with checks that the person is real and is the holder, using more than one data source.
- **Collect tax data at onboarding.** DAC8 requires tax residence information, and users who do not provide it within the statutory window must be blocked from exchange transactions.
- **Extend KYC to wallets.** Screen addresses, attach travel rule data to every transfer and assess ownership of self-hosted addresses for transfers above EUR 1,000.
- **Retain evidence.** Keep identification data, including electronic identification results, for 5 years; DAC8 records for 5 to 10 years.

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 identity verification before account activation, with ID document capture and verification (including NFC chip reading of Romanian electronic identity cards), face match and biometric liveness.
- Video KYC for flows that rely on agent-led remote identification.
- AML screening against sanctions, PEP and adverse-media lists at onboarding, with ongoing monitoring of the customer base.
- Proof of address and KYC questionnaires to capture address and tax-residence details the identity card does not show.
- KYB and beneficial owner verification for corporate customers, in a no-code workflow builder with an audit trail for each check.

[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

- Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA), EUR-Lex, eur-lex.europa.eu; Articles 59, 60, 63, 65, 67, 111, 143, 149 and Annex IV via ESMA Interactive Single Rulebook, esma.europa.eu
- List of grandfathering periods decided by Member States under Article 143 of MiCA, ESMA, esma.europa.eu
- Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets, Articles 14, 16, 17, 26 and 40, EUR-Lex, eur-lex.europa.eu
- Regulation (EU) 2024/1624 (AML Regulation), Articles 19, 79 and 90, EUR-Lex, eur-lex.europa.eu
- Legea nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului [Law no. 129/2019 on preventing and combating money laundering and terrorist financing], Official Gazette Part I no. 589 of 18 July 2019, consolidated form, Articles 2, 5, 7, 8, 11, 13, 17, 17², 19, 21, 25, 27-29, 32¹, 43, 44, Legislative Portal, legislatie.just.ro
- Ordonanța de urgență nr. 10/2025 [Emergency Ordinance no. 10/2025 amending Law 129/2019], Official Gazette Part I no. 225 of 13 March 2025, Legislative Portal, legislatie.just.ro
- Bill L56/2025 approving OUG 10/2025, legislative record, Senate of Romania, senat.ro
- Notă de fundamentare, proiect de ordonanță de urgență privind stabilirea unor măsuri de punere în aplicare a Regulamentului (UE) 2023/1114 [Substantiation note, draft emergency ordinance implementing MiCA], 23 May 2025, Ministry of Finance, mfinante.gov.ro
- Ordonanța de urgență nr. 71/2025 pentru modificarea și completarea Legii nr. 207/2015 privind Codul de procedură fiscală [Emergency Ordinance no. 71/2025 amending the Fiscal Procedure Code], Official Gazette Part I no. 1146 of 10 December 2025, Article 291⁶, Article 336 and Annex 6, Legislative Portal, legislatie.just.ro
- Ordinul președintelui ANAF nr. 750/2026 [ANAF President's Order no. 750/2026 approving form F8000], Official Gazette Part I no. 554 of 6 July 2026, Legislative Portal, legislatie.just.ro
- Legea nr. 227/2015 privind Codul fiscal [Law no. 227/2015 on the Fiscal Code], consolidated form, Article 114(2)(m) and Article 116(2¹) as added by Law no. 239/2025, Legislative Portal, legislatie.just.ro
- Regulamentul ASF nr. 13/2019 [ASF Regulation no. 13/2019 on AML/CFT measures in the sectors supervised by the ASF], consolidated form, Articles 2(2)(k¹) and 27¹, Legislative Portal, legislatie.just.ro
- Obligations of the reporting entities (notice on new electronic identity cards and RO CEI Reader), ONPCSB, onpcsb.ro
- Identificarea la distanță prin mijloace video [Remote identification by video means], ADR President's Decision no. 564/2021, Authority for the Digitalisation of Romania, adr.gov.ro
- Final report on amending Guidelines on ML/TF risk factors (EBA/GL/2024/01), Guidelines 4.29 and 21, EBA, 16 January 2024, eba.europa.eu
- Travel Rule Guidelines (EBA/GL/2024/11), EBA press release of 4 July 2024, eba.europa.eu

- Guidelines on the use of remote customer onboarding solutions (EBA/GL/2022/15), EBA, eba.europa.eu
- Regulation (EU) 2016/679 (General Data Protection Regulation), EUR-Lex, eur-lex.europa.eu
- Legea nr. 190/2018 [Law no. 190/2018 on measures implementing the GDPR], Official Gazette Part I no. 651 of 26 July 2018, ANSPDCP, dataprotection.ro