



Identomat

COMPLIANCE GUIDE

Crypto & Virtual Assets Compliance in Ukraine

COUNTRY **Ukraine**

INDUSTRY **Crypto & Virtual Assets**

LAST UPDATED **16 October 2026**

KEY REGULATORS **Ministry of Digital Transformation of Ukraine · State Financial Monitoring Service of Ukraine · National Security and Defence Council of Ukraine**

Key takeaways

- Ukraine has no crypto licence or registration you can apply for today. The 2022 Law on Virtual Assets exists on paper but has not taken effect, and its replacement is still a bill in parliament.
 - Crypto businesses are nonetheless named in the anti-money laundering (AML) law as firms that must identify customers, monitor transactions and report suspicions, with the Ministry of Digital Transformation as their designated supervisor. Build to that standard now.
 - Know-your-customer (KYC) checks are required before the customer can transact, and for any one-off crypto transaction of UAH 30,000 or more. The same rules apply online and in person; there is no lighter regime for app-only onboarding.
 - Sanctions are the sharpest live risk: since July 2026 Ukrainian law bans any operation with crypto assets issued in Russia or backed by the rouble, and crypto exchange operators are being added to the national sanctions list.
 - The pending bill (No. 10225-d, not yet law) would require authorisation or registration within 60 days of starting activity and would introduce tax on crypto gains. Watch its second reading.
-

The Ukrainian market is open in practice but unregulated at the licensing level. No statute currently prohibits a virtual asset business, yet none grants an authorisation either, because the Law on Virtual Assets of 2022 takes effect only together with Tax Code amendments that parliament has not yet passed. The State Financial Monitoring Service described the resulting position in December 2025 as an absence of special legislation and of a full licensing and supervision system for virtual asset service providers.

The principal authorities are the Ministry of Digital Transformation (AML supervisor of virtual asset service providers under the AML law), the State Financial Monitoring Service (the financial intelligence unit) and the National Security and Defence Council (sanctions). The National Securities and Stock Market Commission and the National Bank of Ukraine would gain roles only once a virtual asset law is in force.

The biggest obstacle for a new entrant is legal uncertainty: AML duties apply on the face of the statute, but there is no register to join and no supervisor-issued rulebook specific to crypto, while sanctions exposure to Russian-linked flows is severe.

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

Ukraine is a unitary state, so every authority below acts nationally.

Authority	Remit for crypto businesses	Level	Official site
Ministry of Digital Transformation (Mintsyfra)	State financial monitoring entity designated for virtual asset service providers under the AML law	National	thedigital.gov.ua
State Financial Monitoring Service (SFMS)	Financial intelligence unit: receives threshold and suspicious transaction reports, publishes typologies	National	fiu.gov.ua
National Security and Defence Council (NSDC)	Personal and sectoral sanctions, enacted by Presidential decree; State Register of Sanctions	National	rnbo.gov.ua
Verkhovna Rada (parliament)	Virtual asset bill No. 10225-d; approval of sectoral sanctions	National	rada.gov.ua
National Securities and Stock Market Commission (NSSMC)	Market regulator under the 2022 Law on Virtual Assets, which is not in force	National	nssmc.gov.ua
National Bank of Ukraine (NBU)	Supervises the banks and payment providers that crypto firms depend on; proposed regulator of e-money tokens	National	bank.gov.ua

2 Licensing and authorisation

The 2022 Law on Virtual Assets Adopted, effective date not yet set

Law of Ukraine No. 2074-IX «Про віртуальні активи» [On Virtual Assets] was adopted on 17 February 2022 and signed on 16 March 2022. It names the National Securities and Stock Market Commission as market regulator, with the National Bank of Ukraine also given powers, and provides for registration of virtual asset service providers and financial monitoring. It takes effect only on the day that a law amending the Tax Code on the taxation of virtual asset transactions takes effect. No such law has been adopted, so the 2022 Law creates no licence, register or permit that a firm can obtain today.

Bill No. 10225-d Bill, first reading only

The replacement framework is bill No. 10225-d, registered on 24 April 2025, adopted as a basis at first reading on 3 September 2025 and, as of October 2026, being prepared for second reading. Its lead committee describes a new Law «Про ринки віртуальних активів» [On Virtual Asset Markets] replacing the 2022 Law, authorisation or registration of service providers within 60 days of starting activity, annual reporting, and fines of 0.5 to 100 times the minimum wage for breaches. Which authority would authorise providers was one of the main differences between the original drafts (the Securities Commission and National Bank in one, the Ministry of Digital Transformation in the other), and the committee asked for the approaches to be combined. None of this is law.

Consequence of operating today

Because no authorisation regime is in force, there is no licensing offence specific to crypto. The exposure is instead AML liability under Law No. 361-IX (section 3), sanctions law, and general consumer and criminal law.

Obligated entity status

Law of Ukraine No. 361-IX of 6 December 2019 on prevention and counteraction to legalisation (laundering) of the proceeds of crime lists "virtual assets service providers" among reporting entities (Article 6(2)(8)) and names the Ministry of Digital Transformation as a state financial monitoring entity (Article 6(3)) responsible for them. A provider is any person carrying out, for or on behalf of another, virtual asset exchange; virtual asset transfer; storage or administration of virtual assets or of tools that control them; or financial services connected with an issuer's offer or sale of virtual assets (Article 1(51)). A virtual asset is a digital representation of value that can be digitally traded or transferred and used for payment or investment (Article 1(13)).

The open question: are these duties enforceable now?

Two readings exist. On the text, every listed activity makes a firm a reporting entity today, with the duty to register with the SFMS as a reporting entity (Article 8(2)(1)) and every customer due diligence, reporting and record-keeping obligation. Against that, the Ministry of Digital Transformation stated in December 2020 that the crypto provisions of Law No. 361-IX could not operate without a base law defining the status of virtual assets and service providers, and the SFMS 2025 typology still records the absence of a full licensing and supervision system. A firm that intends to apply for authorisation once bill No. 10225-d passes will be assessed against a track record, so the prudent course is to comply with Law No. 361-IX in full.

When due diligence applies

On establishing a business relationship; on suspicion; on doubts about earlier identification data; and for any virtual asset transaction of UAH 30,000 or more (Article 11(3)).

Data to collect

For a resident individual: full name, date of birth, identity document details, residence address and taxpayer number (Article 11(8)). Non-residents: citizenship and residence or stay in Ukraine (Article 11(9)).

Mandatory high risk

Customers from jurisdictions that do not apply international AML standards, sanctioned persons, foreign politically exposed persons and residents of listed offshore zones (Article 7(5)). Enhanced measures follow (Article 12).

Beneficial owners

Obtain the ownership structure; 25 percent is the direct-control marker (Article 1(30)). Do not rely solely on the Unified State Register, and report discrepancies with it (Articles 8(2)(8)(d), 11(7)).

Reporting and records

Suspicious transactions or attempts are reported to the SFMS immediately, regardless of amount (Article 8(2)(8)©). Threshold transactions are reported within five business days or by the fifth business day of the following month, depending on type (Article 8(2)(8)(a) and (b)); the Ministry of Digital Transformation has stated that the threshold for virtual asset transactions is UAH 400,000. Records of due diligence, refused customers and correspondence must be kept for at least five years after the relationship ends (Article 8(2)(18)). A firm must refuse or end a relationship when it cannot identify or verify the customer or beneficial owner, or when the risk is unacceptably high (Article 15).

4

Identity verification and onboarding

Law No. 361-IX is method-neutral. Verification must rest on official documents or on information from official or reliable sources (Article 11(7)); documents must be valid when presented, and copies other than notarised ones must be certified in the manner the sector supervisor prescribes. The supervisor may also set reliable sources and sector-specific due diligence rules (Article 11(16)). Identification and verification take place before the business relationship begins or the transaction is carried out, although verification may be finished after an account is opened provided it is complete before the first transaction (Article 11(4)).

Politically exposed persons require senior management approval, source of wealth and source of funds checks, and enhanced ongoing monitoring (Article 11(13)). A firm may use an agent under a written agreement, or rely on due diligence by another reporting entity, but stays responsible for the result (Article 11(17)). The law sets no liveness or presentation-attack standard and no identity assurance level for crypto onboarding; these are design choices for the firm's risk-based approach.

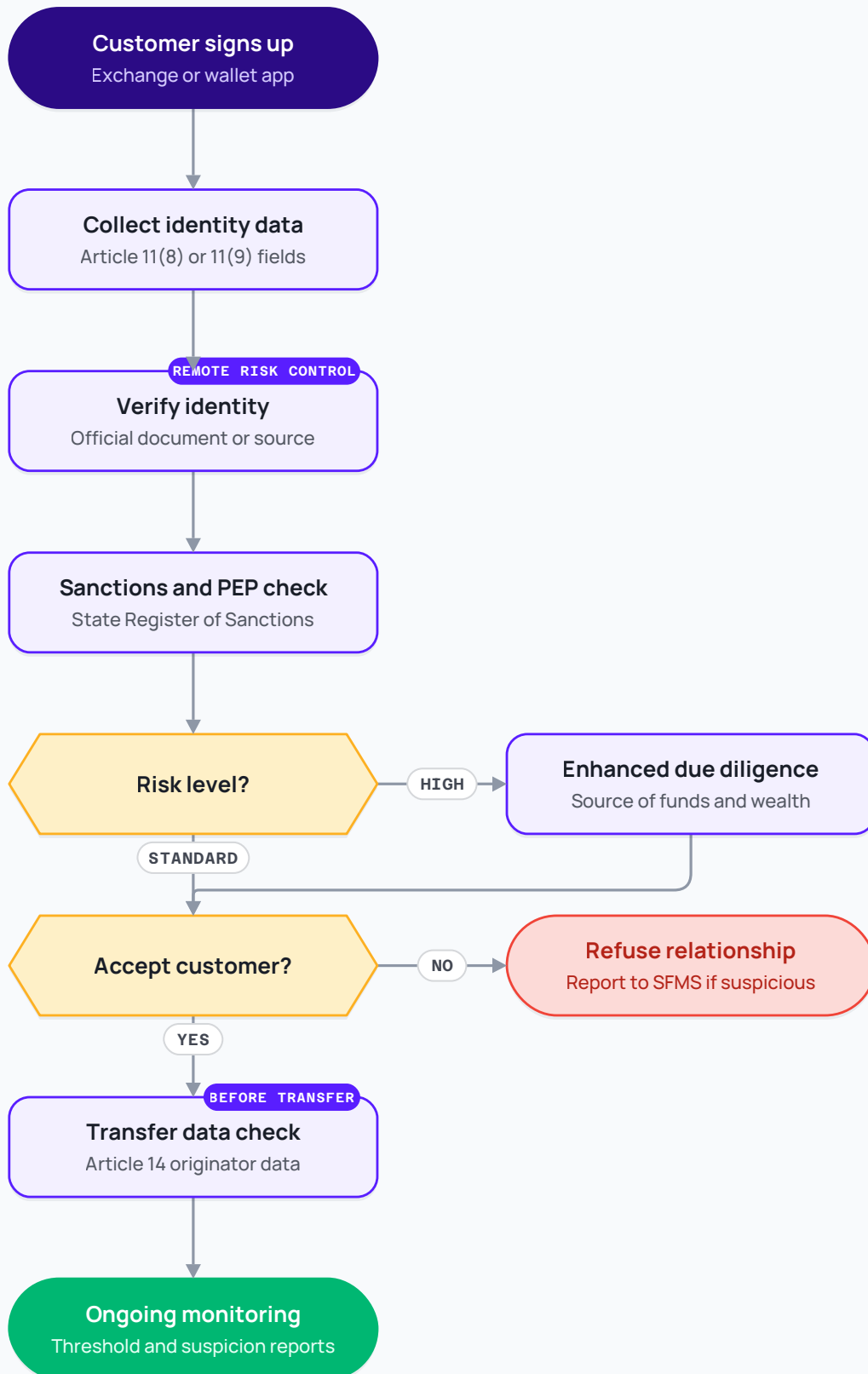


Figure 1. Remote onboarding and first transfer on a Ukrainian crypto platform under Law No. 361-IX.

Bottom line: the rules are channel-neutral, but a firm onboarding without face-to-face contact must specifically manage the risks of that technology, and the delivery channel is one of the risk criteria it must weigh.

Requirement	In person	Online / remote	Difference
Permission to onboard	Due diligence under Article 11	Same, plus a duty to manage risks of technologies used without direct contact	Differs
Risk treatment	Risk-based	Channel is a risk criterion; not on the mandatory high-risk list	Same
When verification is complete	Before first transaction	Before first transaction	Same
Data collected	Article 11(8) and 11(9)	Article 11(8) and 11(9)	Same
Evidence base	Official documents or reliable sources	Official documents or reliable sources; certified copies	Same
Agents and reliance	Written agreement; firm stays liable	Written agreement; firm stays liable	Same
Transfer information	Article 14 applies	Article 14 applies	Same
Record retention	Five years minimum	Five years minimum	Same

Non-face-to-face risk management

Article 8(2) (25) of Law No. 361-IX requires every reporting entity to manage the risks of new and existing products, practices and technologies, expressly including those that allow financial transactions without direct contact with the customer. Article 7(1) lists the way services are provided as a risk criterion. The law does not make remote onboarding automatically high risk: it is absent from the mandatory list in Article 7(5).

Transfer information (the travel rule)

Article 14 applies the information that must accompany a transfer to virtual asset transfers. Domestic transfers below UAH 30,000, and transfers abroad below UAH 30,000, carry a reduced data set where there is no sign of linked transactions; above that, full originator and recipient data travel with the transfer, and the originator is verified before the transfer (Article 14(2) to (4)). A provider may not send a transfer that lacks the required information (Article 14(5)).

Pending changes

Bill No. 10225-d **Bill, first reading only** would add authorisation, client protection and verification of parties to transfers; its details may change before second reading.

6 Data protection and biometrics

Law No. 361-IX states that processing personal data for AML purposes is not a breach of the Law on Personal Data Protection and takes place without the data subject's consent, but the firm must inform the customer, at identification, of its AML processing obligations (Article 2(2)). Retention beyond the five-year AML minimum needs its own justification. Supervision of the current 2010 Law on Personal Data Protection sits with the Ukrainian Parliament Commissioner for Human Rights. Bill No. 8153 **Bill, first reading only**, a new data protection law presented as part of EU integration, would, together with bill No. 6177, move supervision to a separate independent authority; in December 2025 it was transferred to the Committee on Legal Policy for second reading. Selfie, liveness and face-matching data collected during onboarding should be treated as sensitive pending that reform.

7 Sector-specific obligations

Sanctions on Russian-linked assets and services

By decision of 9 June 2026, enacted by Presidential Decree No. 561/2026 and approved by the Verkhovna Rada in July 2026, Ukraine's sectoral sanctions on Russian financial institutions now extend to financial platforms and payment systems that issue or circulate Russia's digital financial assets, and ban any operation with virtual assets issued in Russia or backed by the rouble, and with infrastructure providers that enable such operations **In force**. Personal sanctions in February and October 2026 targeted the A7 crypto

network and operators of crypto exchanges and exchange services. Screening must therefore cover token issuers and counterparty platforms as well as customers.

Token classification

Law No. 361-IX uses a single, broad definition of virtual asset for AML purposes and does not distinguish securities-like tokens. The 2022 Law on Virtual Assets would split financial virtual assets (supervised by the Securities Commission or National Bank) from others, and the drafts behind bill No. 10225-d instead classify e-money tokens, asset-linked tokens and unique virtual assets, with e-money tokens the only category usable for payment, by agreement of the parties. Neither classification applies yet.

Stablecoins and taxation

No stablecoin issuance regime and no tax on crypto gains is in force. Under bill No. 10225-d, proceeds from selling virtual assets would be taxed as investment profit, with record-keeping and declaration duties for taxpayers.

8

Risk indicators and red flags

VIRTUAL ASSET TYPOLOGIES FROM THE SFMS 2025 STUDY

- **Telegram and P2P donations:** direct crypto collections used to finance terrorist activity.
- **OTC desks:** large exchanges through over-the-counter desks with minimal identification.
- **Mixers and DeFi:** flows fragmented to hide sources and recipients.
- **Rouble-linked stablecoins:** use of A7A5 and the Garantex or Grinex exchange to evade sanctions.
- **Deepfake verification:** synthetic video used to pass remote identity checks.
- **Crypto-to-IBAN cash-out:** proceeds of unknown origin received from crypto sales via bank accounts.
- **Young money mules:** minors recruited for crypto exchanges, pseudo-trading or mixer transfers.
- **Fake trading projects:** investment fraud presented as crypto trading.

Enforcement and penalties

Under Law No. 361-IX the Ministry of Digital Transformation supervises virtual asset service providers, including through scheduled and unscheduled inspections, and the head of a reporting entity and its compliance officer are personally responsible for inadequate financial monitoring (Article 8(6)). Firms must also prevent persons with unexpunged convictions for mercenary offences or terrorism from management roles (Article 8(2)(29)).

The most visible enforcement against the sector is through sanctions. On 7 February 2026 the NSDC sanctioned 42 individuals and 35 legal entities for helping Russia evade financial sanctions, including the A7 crypto network ecosystem (Decree No. 103). On 12 October 2026 sanctions were applied to 28 individuals and 27 legal entities including crypto exchange operators, crypto exchange services and their managers and owners.

Bill No. 10225-d **Bill, first reading only** would add a sector penalty regime of 0.5 to 100 times the minimum wage per breach, alongside inspections, investigations and withdrawal of authorisation.

Recent changes and what to watch

- **12 October 2026** **In force** : NSDC sanctions on crypto exchange operators and A7 network managers. Re-screen customers and counterparties.
- **1 September 2026** **Bill, first reading only** : bill No. 10225-d placed on the agenda of the current parliamentary session. A second reading would start the authorisation clock.
- **July 2026** **In force** : ban on operations with virtual assets issued in Russia or backed by the rouble. Block these tokens and the platforms that issue them.
- **22 December 2025** **Published** : SFMS typology study with crypto indicators. Map its indicators into monitoring rules.
- **3 December 2025** **Bill, first reading only** : data protection bill No. 8153 moved to a new lead committee. Biometric rules may tighten.
- **3 September 2025** **Bill, first reading only** : bill No. 10225-d adopted as a basis. Not law until second reading, signature and publication.

What this means for identity verification

Collect the Article 11(8) data set in full for Ukrainian residents, including the taxpayer number or the passport mark recording refusal of one, and the Unified State Demographic Register entry number where the document carries it; non-residents need citizenship and residence or stay data. Accept only documents valid at presentation, and keep evidence that shows verification against an official document or a reliable source. Complete verification before the first transfer, and set a UAH 30,000 trigger for one-off transactions by unverified users. Because the law demands management of non-face-to-face risk but sets no technical standard, document liveness and presentation-attack controls in the risk assessment, particularly given SFMS reports of deepfakes at verification. Re-verify when earlier data is in doubt, apply politically exposed person checks to beneficial owners, and keep images and logs for at least five years after the relationship ends.

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 that captures the identification data Ukrainian AML law requires, with ID document capture and verification including NFC.
- Biometric liveness and face match to manage the non-face-to-face risks the law requires firms to control, including deepfake attempts.
- AML screening against sanctions, PEP and adverse-media lists at onboarding and through ongoing monitoring.
- KYB and beneficial owner verification for corporate clients, with transaction monitoring and an audit trail for every 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

- Law of Ukraine No. 361-IX of 6 December 2019 «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [On Prevention and Counteraction to Legalisation (Laundering) of the Proceeds of Crime, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction], Articles 1, 2, 6 to 8, 11 to 15, English text published by the State Financial Monitoring Service, fiu.gov.ua
- Bill No. 10225-d on amendments to the Tax Code and other acts on regulating the circulation of virtual assets, bill card and status, Verkhovna Rada, itd.rada.gov.ua
- Conclusion of the Verkhovna Rada Committee on Finance, Tax and Customs Policy on bills No. 10225 and No. 10225-1, 24 April 2025, protocol No. 195, komfinbank.rada.gov.ua
- Ministry of Digital Transformation: President signs the Law on Virtual Assets, 16 March 2022, thedigital.gov.ua
- Ministry of Digital Transformation: Law No. 361-IX enters into force, 29 April 2020, thedigital.gov.ua
- Ministry of Digital Transformation: myths about the draft Law on Virtual Assets, 21 December 2020, thedigital.gov.ua
- State Financial Monitoring Service typology study 2025, approved by Order No. 116 of 22 December 2025, sections 1.2, 1.4, 2.1 and 4.8, fiu.gov.ua
- Presidential Decree No. 561/2026 of 29 June 2026 enacting the NSDC decision of 9 June 2026 amending sectoral sanctions on Russian financial institutions, rnbo.gov.ua
- NSDC: Verkhovna Rada approves stronger sanctions on Russia's financial sector, 15 July 2026, rnbo.gov.ua
- NSDC: sanctions on persons linked to Russia's defence industry and financial sector (Decrees No. 102 and No. 103), 9 February 2026, rnbo.gov.ua
- NSDC: new sanctions including crypto exchange operators, 12 October 2026, rnbo.gov.ua
- Transcript of the Verkhovna Rada Committee on Human Rights on bill No. 8153, 3 December 2025, kompravlud.rada.gov.ua