Identomat

COMPLIANCE GUIDE

Crypto & Virtual Assets Compliance in Latvia

COUNTRY Latvia

INDUSTRY Crypto & Virtual Assets

LAST UPDATED 5 November 2026

KEY REGULATORS Latvijas Banka · Financial Intelligence Unit of Latvia · State Revenue Service

Key takeaways

- A crypto exchange, custodian, transfer or trading business based in Latvia now needs a Markets in Crypto-Assets (MiCA) licence from Latvijas Banka, the central bank; firms licensed in another EU country can serve Latvian customers under their passport. The old State Revenue Service registration no longer lets a firm operate, and the EU-wide grace period ended on 1 July 2026.
- A Latvian licence can be passported to every other EU country by notification, so Latvia works as an EU entry point. Application review costs EUR 2,500 and supervision costs up to 0.6% of gross crypto revenue a year, with a EUR 3,000 minimum.
- Fully remote onboarding is allowed. If you follow the national rulebook for remote identification (video identification, qualified electronic ID or signature, bank-data checks, or document photo plus selfie comparison), remote customers are not automatically treated as high risk. The central bank also expects proof that the session is live and an assessment of how well the method resists deepfakes.
- Identity must be checked before the account relationship starts, and for one-off crypto transactions from EUR 1,000. Every transfer must carry sender and recipient details (the "Travel Rule"), and transfers to or from customers' own wallets trigger extra checks.
- From 2026, platforms must also collect each user's tax residence for EU crypto tax reporting. Existing users must certify it by 1 January 2027, and the first report is due by 30 June 2027.

Latvia is open to crypto businesses, and actively courts them: Latvijas Banka offers free pre-licensing consultations, and 12 firms held its crypto-asset service provider authorisation by the end of September 2026.

Latvijas Banka is the single licensing, conduct and anti-money laundering supervisor for licensed crypto firms. The Financial Intelligence Unit (Finanšu izlūkošanas dienests) receives suspicious transaction reports, and the State Revenue Service handles crypto tax reporting.

The biggest obstacle for a new entrant is building a MiCA-grade application (governance, capital, custody and AML controls) that also meets Latvia's detailed technical standards for remote identification and evidence retention. Latvia's 2026 national risk assessment rates the sector's money laundering risk as medium-high and notes that Latvijas Banka often finds significant internal control weaknesses during licensing.

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 firms	Level	Official site
Latvijas Banka	Competent authority under MiCA; authorisation and supervision of crypto-asset service providers; anti-money laundering and sanctions supervision of licensed firms	National	bank.lv
Financial Intelligence Unit (Finanšu izlūkošanas dienests)	Suspicious transaction reports, freezing orders, typologies and risk assessments	National	fid.gov.lv
State Revenue Service (Valsts ieņēmumu dienests)	Crypto tax reporting (DAC8); former anti-money laundering supervisor of crypto providers registered before 30 December 2024	National	vid.gov.lv
Data State Inspectorate (Datu valsts inspekcija)	Data protection supervisory authority, including biometric onboarding data	National	dvi.gov.lv
European Banking Authority (EBA)	Travel Rule and risk factor guidelines addressed to crypto-asset service providers	EU	eba.europa.eu

The European Securities and Markets Authority (ESMA) issues MiCA statements and maintains the EU-level list of authorised crypto-asset service providers.

2 Licensing and authorisation

Only an authorised crypto-asset service provider, or a bank, investment firm or other listed financial entity that notifies its supervisor in advance (Article 60), may provide crypto-asset services in the EU (Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA), Article 59). The Kriptoaktīvu pakalpojumu likums [Crypto-Asset Services Law] names Latvijas Banka as competent authority (Section 4) and sets national fees and sanctions.

Who must apply

Exchanges, custodial wallets, transfer services, brokers, trading platforms, advisers and portfolio managers, with a registered office and effective management in the EU and at least one EU-resident director (MiCA Article 59(2)).

Capital

The higher of a quarter of the previous year's fixed overheads or minimum capital of EUR 50,000 (order execution, transfer, advice and similar), EUR 125,000 (adding custody or exchange) or EUR 150,000 (trading platform) (MiCA Article 67 and Annex IV).

Timeline

Latvijas Banka must check completeness within 25 working days and decide within 40 working days of a complete application (MiCA Article 63). Free pre-licensing consultations come first, with answers within 30 days.

Fees

EUR 2,500 to review an application, then an annual supervision fee of up to 0.6% of gross income from crypto-asset services, at least EUR 3,000 (Crypto-Asset Services Law, Section 6).

Passporting. After notifying Latvijas Banka, the firm may serve other member states from the 15th calendar day at the latest (MiCA Article 65).

Transition. ESMA's list shows a six-month transitional period for Latvia. Providers registered with the State Revenue Service before 30 December 2024 could operate until 30 June 2025. The Crypto-Asset Services Law let firms that had applied by then continue until Latvijas Banka decided (transitional provision 2), while the AML Law ends the right on 30 June 2025 (transitional provision 72). Either way, any such right ended no later than 1 July 2026, the EU-wide end date (MiCA Article 143(3)).

Operating without a licence can be sanctioned under the Crypto-Asset Services Law (Section 8) and the AML Law (Section 78(1.2)).

3 AML, KYC and customer due diligence

Crypto-asset service providers are obliged entities and are classed as financial institutions under the Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likums [Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing] (the AML Law), Section 1(1)(7)(n). Latvijas Banka supervises them (Section 45(1)(1)). A provider that only gives advice on crypto-assets is outside the AML Law's definition (Section 1(1)(21)).

- **When due diligence is required.** Before any business relationship, before occasional crypto transactions (single or linked) of EUR 1,000 or more, on suspicion, and when earlier data is in doubt (Section 11(1)).
- **Limited deferral.** Where a documented risk assessment shows low risk, verification may be completed as soon as possible after first contact, but always before a transaction is executed (Section 11(3)).
- **No due diligence, no service** (Section 11(7)).
- **Enhanced due diligence (EDD).** Mandatory for remote customers unless the Cabinet's remote identification rules are followed, for politically exposed persons on a risk basis, for customers transferring to or from self-hosted addresses, and wherever risk is higher (Section 22(2)).
- **Risk scoring and monitoring.** Latvijas Banka Regulation No. 316 (2024) requires a customer risk model and numerical risk scoring. Latvijas Banka's March 2026 guidelines expect crypto firms to use blockchain analytics and to screen transfers in real time for self-hosted addresses, missing Travel Rule data, mixers and sanctioned addresses before execution.
- **Governance.** A responsible AML officer both in senior management and in the internal control unit (Section 10(2), extended to crypto firms from 6 March 2026) and an independent external audit (Section 7).
- **Reporting.** Every suspicious transaction must be reported to the Financial Intelligence Unit without delay through its online reporting system; requested information must be supplied within three working days where a temporary freeze or urgency applies, otherwise within seven (Section 31.4). Threshold declarations apply to crypto firms only if they also provide cash or cross-border payment services (Cabinet Regulation No. 550, point 14).
- **Retention.** Due diligence data, payments and correspondence are kept five years after the relationship ends (Section 37).

4 Identity verification and onboarding

Data to verify. Section 12 of the AML Law requires an identity document showing, for residents, name, surname and personal identity number; for non-residents, name, surname, date of birth, photograph, document number and issue date, and issuing country and authority. A remotely onboarded non-resident may use a domestic passport or another identity document recognised by their own country (Section 12(3)). Every document must be checked against the Register of Invalid Documents (Section 12(3.1)).

Approved remote methods. Cabinet Regulation No. 392 (2018, as amended 2022) lists four technological solutions (point 7):

- secure electronic signature or qualified increased security electronic identification, including eIDAS schemes;
- live video identification;
- identity data from an EU-regulated bank or payment institution, such as an identification payment;
- a document photo compared with a selfie.

Document and biometric checks. For video and document-plus-selfie methods the firm must read the machine-readable zone, check optical security features, use forgery detection, and perform biometric recognition and comparison of the person during the session (points 9 and 11). A captured document image or video counts as the copy of the document required by law. Latvijas Banka's guidelines add that firms must show the capture is live, not pre-recorded, treat chip data as most reliable (EBA/GL/2022/15) and assess resilience to deepfakes.

Restrictions. The bank-data and selfie methods may not be used where the customer or beneficial owner is linked to a high-risk third country or a low-tax or no-tax jurisdiction (point 12). Firms must stop remote identification, or apply other measures, if the process seems insecure or data does not match (point 4).

Outsourcing and agents. Remote identification may be outsourced to a provider bound by EU anti-money laundering rules, under the firm's oversight (point 6). A technical vendor meeting Regulation No. 392 is not an "agent" under Latvijas Banka Regulation No. 351, which governs third parties identifying customers on the firm's behalf. The firm stays liable either way.

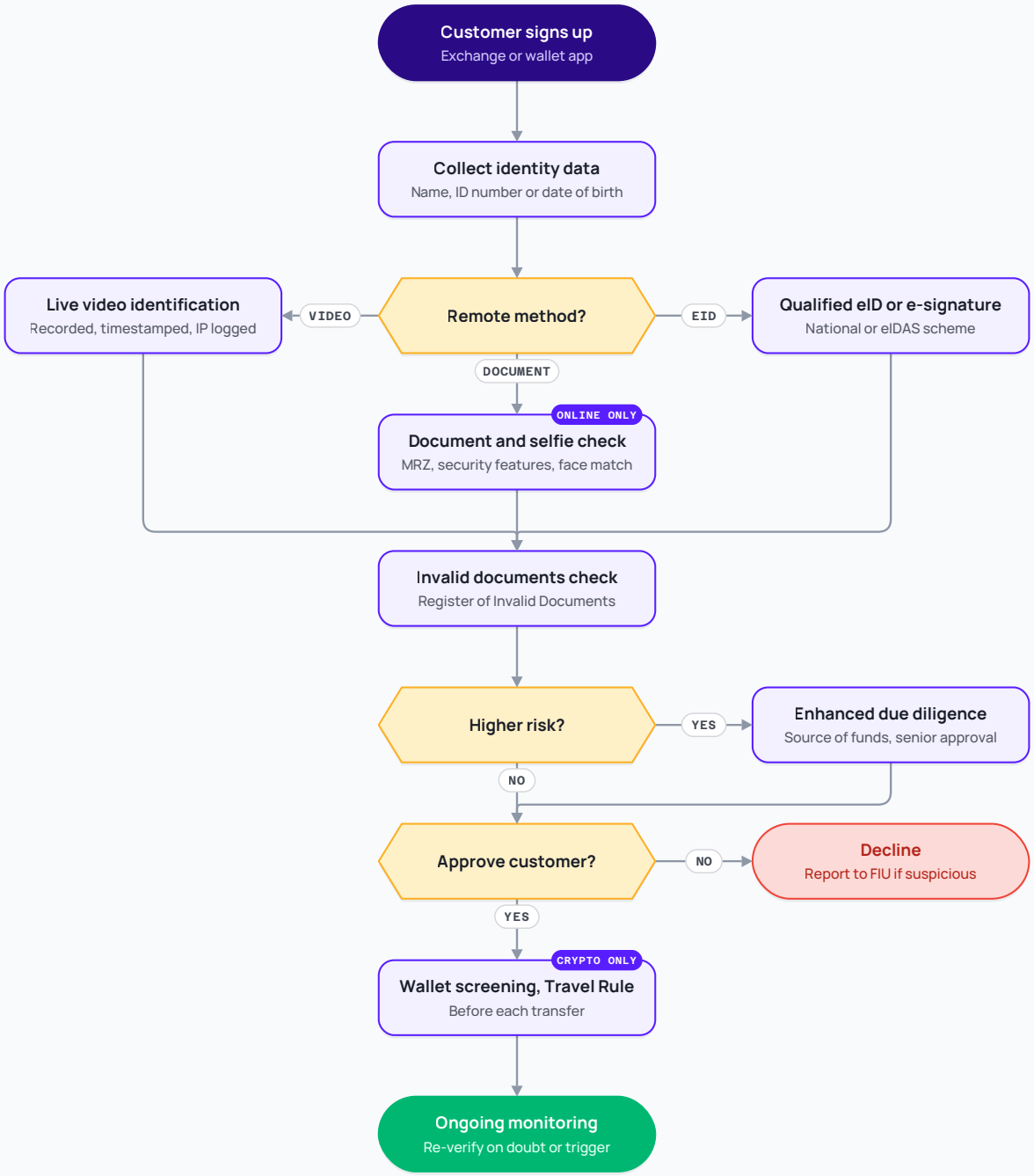


Figure 1. Remote onboarding of a retail customer by a Latvian crypto-asset service provider.

5 Digital channels: what's different

Bottom line: remote onboarding is fully permitted, and it is treated as standard risk only when the firm uses one of the methods in Cabinet Regulation No. 392 and meets its technical and evidence requirements; otherwise every remote customer triggers enhanced due diligence.

Requirement	In person	Online / remote	Difference
Permission to onboard	Permitted	Permitted under Regulation No. 392	Same
Risk treatment	Risk-based	Enhanced due diligence unless Regulation No. 392 is followed	Differs
Accepted identity documents (non-residents)	Document valid for entry into Latvia	Domestic passport or other document recognised in the home country	Differs
Document checks	Document copied (AML Law, Section 14)	Machine-readable zone, optical security features, forgery detection, biometric match	Differs
Proof of a live person	Person present	Firm must show capture is real time, not pre-recorded	Differs
Evidence kept	Copy of the document	Audit trail with immutable timestamp, name and IP address; video and audio where used	Differs
When verification is completed	Before the relationship or a EUR 1,000 occasional transaction	Same	Same
Retention period	Five years after the relationship ends	Five years after the relationship ends	Same
Sanctions risk controls	Required	Required	Same

Video identification is a defined procedure

Video identification must be a live, encrypted audio and video interview with the face uncovered, the document legible and verification questions asked; if the stream breaks, it restarts (Regulation No. 392, point 10).

What is changing: from 10 July 2027 the EU Anti-Money Laundering Regulation (AMLR) `Adopted, applies 10 Jul 2027` allows identity verification by electronic identification means at eIDAS assurance level "substantial" or "high" as an alternative to document submission (Article 22(6)).

6 Data protection and biometrics

The General Data Protection Regulation applies, supervised by the Data State Inspectorate under the Fizisko personu datu apstrādes likums [Personal Data Processing Law]. Facial images processed to uniquely identify a person are biometric data (GDPR Article 4(14)), and their processing is prohibited unless an Article 9(2) condition applies, so a face-match step needs a documented Article 9 basis. The Data State Inspectorate's guidance says facial recognition performing a task set by law may rely on the public-interest exception, otherwise on consent, after a data protection impact assessment. The AML Law treats such processing as public interest (Section 5.2).

Remote identification evidence, including video and audio, must be stored unaltered; video need not be kept where qualified eID is combined with video identification and images are retained (Regulation No. 392, point 16). After the five-year retention period, the data must be destroyed (AML Law, Section 37(2.1)).

7 Sector-specific obligations

Travel Rule

Regulation (EU) 2023/1113, applying since 30 December 2024, requires every crypto transfer to carry the originator's name, ledger address or account, and address, document number and customer number (or date and place of birth), plus the beneficiary's name and ledger address or account (Article 14(1) and (2)). There is no minimum amount. The sending firm must verify originator data before transfer and may not execute a transfer until it complies (Article 14(6) and (8)). EBA Guidelines EBA/GL/2024/11 set the operational detail, and Latvijas Banka expects firms to validate data, hold back or return non-compliant transfers, and report counterparties that repeatedly fail the Travel Rule.

Self-hosted wallets

For a transfer of more than EUR 1,000 to a self-hosted address, the firm must assess whether the customer owns or controls that address (Regulation 2023/1113, Article 14(5)). Latvian law adds enhanced due diligence for customers using self-hosted addresses and requires one or more of: risk-based identification of the counterparty, information on the origin and destination of the assets, or enhanced monitoring (AML Law, Sections 22(2)(4.1) and 25.2).

Custody and client funds

Custodians need a client agreement, a register of each client's positions, a custody policy and segregation of client holdings, and are liable for losses attributable to them (MiCA Article 75). Client funds may be held at a credit institution or Latvijas Banka (Crypto-Asset Services Law, Section 5(2)).

Crypto tax reporting (DAC8)

Cabinet Regulation No. 751, in force 1 January 2026, requires reporting crypto-asset service providers to collect and validate each user's tax residence through self-certification, and report exchange transactions and transfers to the State Revenue Service. For users onboarded before 2026, the self-certification is due by 1 January 2027 (points 55 and 56); the first report covers 2026 and is due by 30 June 2027 (point 54). Users who ignore two reminders must be blocked from reportable transactions (point 42).

Sanctions

Firms must document a sanctions risk assessment and run sanctions controls (Law on International Sanctions and National Sanctions of the Republic of Latvia, Section 13.1); Latvijas Banka expects these to include screening of wallet addresses.

8 Risk indicators and red flags

CRYPTO-ASSET TYPOLOGIES FLAGGED BY LATVIAN AND EU AUTHORITIES

- **High-risk counterparties**: conversion through a provider registered in a high-risk third country (FIU indicator J1).
- **Tainted addresses**: wallets linked to platforms with adverse information, such as gambling sites, malware or reported thefts (J2).
- **Hidden location**: masked IP addresses or IP addresses in high-risk jurisdictions (J3).
- **Unregistered exchanges**: transfers to or from an exchange that is not registered in the jurisdiction where the customer or the exchange is located (J4).
- **Obfuscation**: use of mixers, tumblers or privacy-enhancing technology (EBA Guideline 21).
- **Pass-through accounts**: deposits soon after onboarding followed by rapid withdrawal without economic rationale (EBA Guideline 21).
- **Fraud and proxies**: transactions out of line with the customer's income or knowledge, or a customer guided by a third party (State Revenue Service sector assessment, 2023 to 2025); suspected fraud is the most common reason for the sector's suspicious transaction reports (National Risk Assessment 2023 to 2025).
- **Sector risk drivers**: self-hosted transfers, occasional transactions, high-risk jurisdictions and exchange services linked to decentralised finance (National Risk Assessment 2023 to 2025).

9 Enforcement and penalties

Anti-money laundering and Travel Rule breaches (AML Law, Section 78): because crypto firms are financial institutions, Latvijas Banka may fine a legal person up to 10% of total annual turnover, or up to EUR 5,000,000 where 10% would be lower, and responsible individuals up to EUR 5,000,000. It may also suspend or revoke a licence, halt the firm's settlements and require removal of managers; sanctions are published for five years.

MiCA breaches (Crypto-Asset Services Law, Sections 8 and 10): legal persons face up to EUR 5,000,000, 5% of the previous year's turnover or twice the profit gained for service-provider breaches, and up to EUR 15,000,000 or 15% for market abuse; individuals up to

EUR 700,000 to EUR 5,000,000. Authorisation can be withdrawn, and cases opened up to five years after the breach.

Before MiCA, the State Revenue Service sanctioned registered crypto providers in 2023 (one suspension with a EUR 800 fine) and 2025 (one suspension with a fine, and one fine), mainly for outdated internal controls, missing identification and monitoring, and no sanctions risk assessment. Latvijas Banka has suspended other non-bank firms, such as currency exchanger DIKAS SIA in June 2025, over transactions by unidentified persons.

10 Recent changes and what to watch

- **10 July 2027** `Adopted, applies 10 Jul 2027` EU Anti-Money Laundering Regulation applies: customer due diligence for every occasional crypto transaction of EUR 1,000 or more, identification and verification of the customer below that amount (Article 20(1)(a)), and a ban on anonymous crypto accounts and anonymity-enhancing coins (Articles 19(3) and 79).
- **30 June 2027** `Adopted, first report due 30 Jun 2027` First DAC8 crypto tax report for 2026; self-certifications from existing users are due by 1 January 2027.
- **15 October 2026** `In force` Positive cash balances of non-resident or corporate clients off-boarded by a financial institution pass to the state if unclaimed for five years; institutions must run their first check within six to nine months (AML Law, Section 43(2.1)).
- **1 October 2026** `Final draft, not adopted` AMLA submitted its final draft standards on customer due diligence (Article 28(1) AMLR; report of 30 September 2026). Draft Article 7 allows remote document-based checks only where the customer cannot reasonably present an identity document in person and has no eIDAS "substantial" or "high" means or relevant qualified trust service; the firm must justify it and meet listed safeguards. Proposed to apply six months after entry into force.
- **2026** `Published` National Risk Assessment 2023 to 2025 raises crypto-asset service providers from medium to medium-high money laundering risk; firms must reflect it in their own risk assessments (AML Law, Section 6(1.1)).
- **1 July 2026** `In force` MiCA transitional period ended across the EU; ESMA told unauthorised providers to stop onboarding and wind down.
- **March 2026** `In force` AML Law amendments align the crypto definitions with MiCA and require a two-level AML officer structure (from 6 March); Latvijas Banka's updated guidelines add a crypto chapter on analytics, monitoring and the Travel Rule.

11 What this means for identity verification

- **Use a listed method and route by country.** Build on the four Regulation No. 392 methods, and send customers linked to high-risk or low-tax jurisdictions to video identification or qualified eID.
- **Check the document and the person.** Read the machine-readable zone (chip data where available), check security features, detect forgeries, match the face and prove the capture is live.
- **Keep a tamper-proof trail** with timestamp, name and IP address, plus video and audio where used, for five years after the relationship ends.
- **Capture Travel Rule, wallet and tax data at onboarding**, including proof of control for self-hosted addresses and DAC8 tax residence.

IDENTOMAT

How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- Remote onboarding with ID document capture and verification, including machine-readable zone reading and NFC, plus face match and biometric liveness.
- Video KYC for customers who must be identified by live video, with recorded sessions and an audit trail.
- AML screening against sanctions, PEP and adverse-media lists at onboarding and through ongoing monitoring.
- KYB and beneficial owner verification for corporate clients, with KYC questionnaires to collect tax residence and source of funds.
- No-code workflow builder to route customers by country and risk to the right verification method.

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

- **Kriptoaktīvu pakalpojumu likums** [Crypto-Asset Services Law], adopted 13 June 2024, in force 30 June 2024, Sections 4 to 10 and transitional provisions, likumi.lv
- **Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likums** [Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing], consolidated version including amendments in force 15 October 2026, Sections 1, 5.2, 6, 7, 10 to 12, 14, 22, 25.2, 31.4, 37, 43, 45, 78 and transitional provision 72, likumi.lv
- **Grozījumi Noziedzīgi iegūtu līdzekļu legalizācijas ... novēršanas likumā** [Amendments to the AML Law], adopted 5 February 2026, in force 6 March 2026, likumi.lv
- **Cabinet Regulation No. 550** (17 August 2021), suspicious transaction reports and threshold declarations, point 14, likumi.lv
- **Cabinet Regulation No. 392** (3 July 2018, as amended by Regulation No. 331 of 7 June 2022), Procedure for remote customer identification, likumi.lv
- **Latvijas Banka Regulation No. 316** (17 September 2024), customer risk, due diligence, enhanced due diligence and IT requirements, likumi.lv
- **Latvijas Banka Regulation No. 351** (25 November 2024, in force 1 January 2025), cooperation with third parties for customer identification and due diligence, likumi.lv
- **Cabinet Regulation No. 751** (9 December 2025, in force 1 January 2026), automatic exchange of information on crypto-asset transactions, points 2, 42 and 54 to 56, likumi.lv
- **Starptautisko un Latvijas Republikas nacionālo sankciju likums** [Law on International Sanctions and National Sanctions of the Republic of Latvia], Sections 13 and 13.1, likumi.lv
- **Fizisko personu datu apstrādes likums** [Personal Data Processing Law], Section 3, likumi.lv
- **Regulation (EU) 2023/1114 on markets in crypto-assets**, Articles 3, 59, 60, 63, 65, 67, 75 and 143 and Annex IV, eur-lex.europa.eu
- **Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets**, Articles 14 and 40, eur-lex.europa.eu
- **Regulation (EU) 2024/1624 (Anti-Money Laundering Regulation)**, Articles 19, 20, 22, 79 and 90, eur-lex.europa.eu
- **Regulation (EU) 2016/679 (General Data Protection Regulation)**, Articles 4(14) and 9, eur-lex.europa.eu
- **AMLA, Final Report: Draft Regulatory Technical Standards under Article 28(1) of Regulation (EU) 2024/1624**, 30 September 2026, Article 7 and Article 29, amla.europa.eu

- **AMLA, Press release "AMLA finalises key standards for the private sector"**, 1 October 2026, amla.europa.eu
- **EBA Guidelines on information requirements for transfers of funds and crypto-assets (EBA/GL/2024/11)**, 4 July 2024, applying from 30 December 2024, eba.europa.eu
- **EBA Guidelines amending the ML/TF Risk Factors Guidelines (EBA/GL/2024/01)**, 16 January 2024, Guideline 21 for crypto-asset service providers, eba.europa.eu
- **Finanšu izlūkošanas dienests, Noziedzīgi iegūtu līdzekļu legalizācijas tipoloģijas un pazīmes** [Money laundering typologies and indicators], 3rd edition, 2024, section J, fid.gov.lv
- **Finanšu izlūkošanas dienests, Nacionālais NILLTPF risku novērtēšanas ziņojums 2023–2025** [National ML/TF/PF Risk Assessment 2023 to 2025], 2026, section 5.11, fid.gov.lv
- **Valsts ieņēmumu dienests, sector risk assessment: Kriptoaktīvu pakalpojumu sniedzēji** [Crypto-asset service providers], 2023 to 2025, vid.gov.lv
- **Latvijas Banka, Vadlīnijas NILLTPF novēršanas un sankciju riska pārvaldīšanas iekšējās kontroles sistēmas izveidei un klientu izpētei** [AML/CFT and sanctions risk guidelines], March 2026, sections 5.10 and 14, latvijasbanka.lv
- **Datu valsts inspekcija, "#DVIskaidro: Biometrijas datu apstrāde mazumtirdzniecībā"** [Biometric data processing], dvi.gov.lv
- **Latvijas Banka, Financial market participant register: crypto-asset market** (consulted 5 November 2026), bank.lv
- **Latvijas Banka, Crypto-asset service providers: how to obtain authorisation** (updated 1 October 2026), bank.lv
- **ESMA, Public Statement on the end of the MiCA transitional period** (ESMA75-113276571-1710), 23 June 2026, esma.europa.eu
- **ESMA, List of grandfathering periods decided by Member States under Article 143 of MiCA**, esma.europa.eu
- **Latvijas Banka, Sanctions register** (entry of 18 June 2025), bank.lv