Identomat

COMPLIANCE GUIDE

Crypto & Virtual Assets Compliance in Lithuania

COUNTRY Lithuania

INDUSTRY Crypto & Virtual Assets

LAST UPDATED 9 November 2026

KEY REGULATORS Bank of Lithuania · Financial Crime Investigation Service

Key takeaways

- Since 1 January 2026, offering crypto exchange, custody or trading in Lithuania requires a licence under the EU Markets in Crypto-Assets Regulation (MiCA) from the Bank of Lithuania, or a MiCA licence from another EU country used across borders. A pre-2026 Lithuanian registration as a virtual currency operator no longer gives any right to operate.
- Unlicensed crypto services are treated as illegal financial activity: the Bank of Lithuania blocks websites (27 in November 2026) and unlicensed provision of financial services can be prosecuted under the Criminal Code.
- Customers can be onboarded fully online, but only by the remote methods the anti-money laundering (AML) law lists: live video identification, an EU electronic ID at substantial or high assurance, a qualified electronic signature, reliance on another firm, or a first payment from the customer's account at an EU (or equivalent) bank, payment or e-money institution plus a certified ID copy. No other remote identification route is permitted.
- Every crypto transfer, whatever its size, must carry sender and recipient details (the EU "Travel Rule"); for transfers above EUR 1,000 to a customer's self-hosted wallet, the provider must assess whether the customer owns or controls it.
- Providers report suspicious activity to the Financial Crime Investigation Service within one working day, report cash or crypto transactions of EUR 15,000 or more within seven working days, keep customer records (including onboarding video recordings) for eight years, and report crypto users to the tax authority every year, with the first report due by 31 May 2027.

Lithuania is open to crypto businesses, but only to licensed ones. The market changed sharply when the national registration regime for virtual currency exchange and wallet operators ended on 31 December 2025, six months earlier than the EU-wide MiCA deadline of 1 July 2026. More than 370 firms had declared crypto activity to the Centre of Registers by mid-2025; three held a Bank of Lithuania licence when the transition closed, and a fourth was licensed in February 2026.

The Bank of Lithuania is the licensing authority for crypto-asset service providers. AML supervision of these firms is shared: the Bank of Lithuania supervises them under Articles 4(1) and 30(1)(2) of the Law on the Prevention of Money Laundering and Terrorist Financing, and the Financial Crime Investigation Service (FNTT), which is also the financial intelligence unit and a competent authority for financial sanctions, supervises all financial institutions under Article 30(1)(1).

The biggest obstacle for a new entrant is the licence itself: the Bank of Lithuania screens applicants hard on shareholder transparency, source of funds and real substance, and refuses shell structures that outsource key functions.

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

Regulator	Remit	Level	Official site
Bank of Lithuania (Lietuvos bankas)	MiCA competent authority: licenses and supervises crypto-asset service providers (CASPs) and token issuers; AML supervisor of CASPs (AML Law Arts. 4(1), 30(1)(2)), issuing their AML instructions in agreement with FNTT; blocks unlicensed websites	National	lb.lt
Financial Crime Investigation Service (FNTT)	Financial intelligence unit: receives suspicious and threshold reports; competent authority for implementing financial sanctions and receives asset freeze notifications; AML supervisor of all financial institutions, including CASPs (AML Law Art. 30(1)(1)); agrees the Bank of Lithuania's AML instructions for CASPs and may fine them for AML breaches	National	fntt.lrv.lt

State Tax Inspectorate (VMI)	Receives annual crypto-asset user reports from CASPs (EU DAC8 rules)	National	vmi.lt
State Data Protection Inspectorate (VDAI)	Data protection supervisor, including for identity and biometric data	National	vdai.lrv.lt
EU Anti-Money Laundering Authority (AMLA)	Will directly supervise a limited number of selected high-risk financial-sector entities, which can include CASPs; first selection to start by 1 July 2027	Supranational	Regulation (EU) 2024/1620
European Securities and Markets Authority (ESMA) and European Banking Authority (EBA)	EU register of authorised CASPs (ESMA); AML, Travel Rule and remote onboarding guidelines (EBA)	Supranational	esma.europa.eu, eba.europa.eu

Lithuania's anti-money laundering and countering the financing of terrorism (AML/CFT) system is evaluated by the Council of Europe's MONEYVAL committee, whose sixth evaluation round of Lithuania began in October 2026.

2 Licensing and authorisation

Crypto-asset services in Lithuania are governed by Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA), Title V, and the national Law on Markets in Crypto-Assets (No XIV-2879, consolidated version from 2 July 2026) `In force`. A firm that exchanges, holds, transfers or trades crypto-assets for clients needs a CASP licence from the Bank of Lithuania; financial institutions listed in MiCA Article 60 (such as credit institutions and investment firms) instead notify it at least 40 working days before starting.

Who can apply

Only a public or private limited liability company (AB or UAB) may hold a Lithuanian CASP licence (Law on Markets in Crypto-Assets, Art. 3(2)). MiCA requires a registered office in the EU member state where at least part of the services are provided, effective management in the EU and at least one EU-resident director.

Timeline

The Bank of Lithuania acknowledges an application within 5 working days, checks completeness within 25 working days and decides within 40 working days of receiving a complete application (MiCA Art. 63). The state fee for issuing a CASP licence is EUR 2,425 (Government Resolution No 1458).

Minimum capital

EUR 50,000 for order execution and transmission, placing, transfer services, advice and portfolio management; EUR 125,000 where the firm also provides custody or exchange; EUR 150,000 for operating a trading platform (MiCA Annex IV).

Passporting

A Lithuanian licence can be used across the EU after notifying the Bank of Lithuania of the target member states and services (MiCA Art. 65). Firms licensed elsewhere in the EU may serve Lithuanian clients on the same basis.

What the Bank of Lithuania looks for

Its expectations letter of 22 August 2024 stresses shareholders' repute and finances, origin of funds, managers' qualifications and internal controls, and rules out shell entities that outsource key functions.

The end of the old regime

MiCA allowed existing providers to continue until 1 July 2026 but let member states shorten that period (Art. 143(3)). Lithuania did: virtual currency exchange and depository wallet operators lost the right to operate from 1 January 2026 unless licensed under MiCA (Law on Markets in Crypto-Assets, Art. 22(3), as amended by Law No XV-185). Under Criminal Code Article 202, professional or large-scale financial activity without a required licence is punishable by up to four years' imprisonment, and legal persons are also liable. Firms that carry out e-money token operations qualifying as payment services also need a payment services authorisation: the EBA's no-action transition period ended on 2 March 2026.

3 AML, KYC and customer due diligence

CASPs are "financial institutions" under the Law on the Prevention of Money Laundering and Terrorist Financing (No VIII-275, consolidated version 30 June to 31 December 2026; the AML Law) `In force`. AML supervision is shared: the Bank of Lithuania (Arts. 4(1), 30(1)(2)), which sets CASPs' AML instructions with FNTT, and FNTT (Art. 30(1)(1)). Its Board Resolution No 03-17 of 12 February 2015 (consolidated from 18 March 2025) applies to CASPs, together with the EBA ML/TF Risk Factors Guidelines as amended, which include the crypto-specific Guideline 21.

When due diligence is required

Under Article 9(1), a CASP must identify and verify the customer and beneficial owner before establishing a business relationship; before occasional transactions of EUR 15,000 or more (single or linked); when executing or receiving transfers of funds, in line with Regulation (EU) 2023/1113; where there are doubts about previously obtained data; and whenever money laundering or terrorist financing is suspected. The former EUR 700 threshold for occasional virtual currency operations was repealed from 1 January 2026 (Law No XIV-2883). A beneficial owner is a natural person holding 25% plus one share, or more than 25%, of the customer, or otherwise controlling it (Art. 2).

Enhanced due diligence

Article 14 requires enhanced due diligence in higher-risk situations, including cross-border correspondent relationships involving crypto-asset services with a respondent established outside the EU. Its higher-risk factors include non-face-to-face business outside Article 11 and politically exposed persons.

Self-hosted wallets

Article 29(8) requires CASPs to assess the risk of self-hosted address transfers and apply at least one measure: verifying the originator or beneficiary, asking for information on origin and destination, or continuous monitoring.

Reporting and records

Obligation	Trigger	Deadline	Provision
Suspicious activity report to FNTT	Knowledge or suspicion that property of any value derives from crime or relates to terrorist financing	No later than one working day	AML Law Art. 16(1)
Suspend and report a suspicious transaction	Customer carries out a suspicious transaction, regardless of amount	Within 3 working hours of suspension	AML Law Art. 16(2)
Threshold report to FNTT	Single or linked cash or crypto-asset operations of EUR 15,000 or more	Within 7 working days	AML Law Art. 20(1), (5)
Asset freeze notification to FNTT	Funds or economic resources frozen under international sanctions	Within 2 working days	Government Resolution No 535
Record retention	ID copies, beneficial owner data, live video recordings, account and transaction records	8 years from end of relationship or transaction (correspondence 5 years)	AML Law Art. 19

4 Identity verification and onboarding

Article 11(1) of the AML Law is the exhaustive list of ways a customer may be identified without being physically present. A CASP may use only these:

- **Third-party reliance** under Article 13.
- **EU electronic identification** under a scheme of substantial or high assurance level under the eIDAS Regulation (EU) No 910/2014.
- **Qualified electronic signature** created with a qualified certificate meeting eIDAS (third-country qualified signatures are recognised under eIDAS Article 14).
- **Live video identification**, either (a) capturing the original identity document and confirming identity with at least an advanced electronic signature, or (b) capturing the customer's face together with the original identity document they show.

- **First payment** from an account in the customer's name at a credit, payment or e-money institution in the EU (or an equivalent third country) before services start, plus a paper copy of the identity document certified by a notary, an elder (seniūnas) or a Lithuanian consular officer; copies certified abroad need legalisation or an apostille (FNTT Order No V-131 of 12 September 2017).

Reliance and eID count only if the customer was first identified in person, by live video or by the first-payment method (Art. 11(2)). On every route the firm must use additional data to confirm the identity is genuine (Art. 11(3)) and remains responsible for the result (Art. 11(4)). CASPs must also follow the EBA Guidelines on the use of remote customer onboarding solutions (Art. 11(6)).

FNTT technical requirements for video identification

The FNTT Director's Order No V-314 of 30 November 2016 (consolidated from 12 January 2021) sets the technical rules. Video or photos must be transmitted live; uploading non-real-time photos must be technically impossible. The customer shows the document (both sides of an ID card or residence permit) and tilts it several times. Under method (a), the customer signs the onboarding form with at least an advanced electronic signature within one hour, in the same procedure. Under method (b), face and document are shown together and the customer answers an approved questionnaire. The session must stop if transmission is not live or breaks off, quality is insufficient, more than one person takes part, the form is not signed within the hour (method (a)), or there is reasonable doubt that the customer is the document holder. If the document appears forged, information may be collected only to report the case to FNTT.

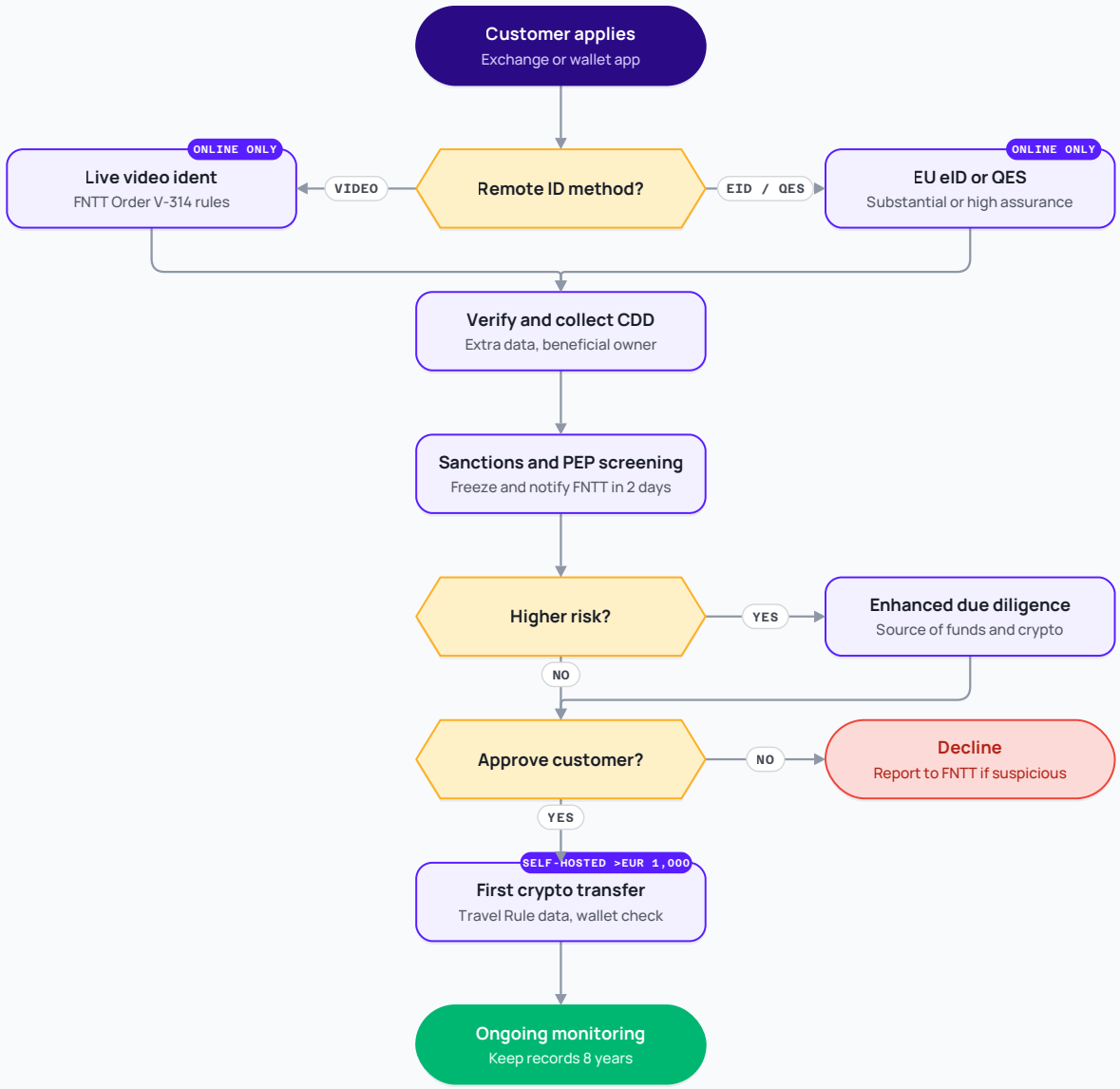


Figure 1. Remote onboarding of a retail customer by a Lithuanian-licensed CASP.

5 Digital channels: what's different

Bottom line: online onboarding is lawful, but only through the five remote methods in AML Law Article 11, and live video has its own FNTT technical rulebook.

Requirement	In person (office, OTC desk)	Online / remote	Difference
Permission to onboard	Identity document checked face to face	Only the five Art. 11(1) methods	Differs
Risk treatment	Risk-based	Other remote routes not permitted; non-face-to-face business outside Art. 11 is a higher-risk factor	Differs
Technical standard	None specific	FNTT Order V-314 for live video	Differs
Extra verification	Standard CDD	Additional data required to confirm authenticity (Art. 11(3))	Differs
When CDD is completed	Before business relationship	Before business relationship	Same
Licence	MiCA CASP licence	MiCA CASP licence	Same
Travel Rule data on transfers	Required, no minimum amount	Required, no minimum amount	Same
Evidence kept	ID copies, 8 years	ID data plus live video recording, 8 years	Differs
Action against unlicensed offers	Criminal and supervisory measures	Also website blocking by the Bank of Lithuania	Differs

A fixed list of methods

Document upload with a selfie and automated liveness is not a listed method; a flow must fit a live video variant under the FNTT order, or use eID, a qualified signature, reliance or the first-payment route.

Website blocking

The Bank of Lithuania can have websites offering illegal financial services blocked; 27 unlicensed crypto websites were blocked by 5 November 2026.

The EU Anti-Money Laundering Regulation (EU) 2024/1624 `Adopted, applies 10 Jul 2027` will set customer due diligence rules directly across the EU from that date, so Lithuania's Article 11 list will need to be aligned with it.

6 Data protection and biometrics

The General Data Protection Regulation (EU) 2016/679 (GDPR) applies, supervised in Lithuania by VDAI, alongside the Law on Legal Protection of Personal Data (No I-1374, consolidated from 30 June 2026).

- **Biometrics.** Facial images processed through specific technical processing to uniquely identify a person are biometric data, a special category under GDPR Article 9(1). A face match during onboarding therefore needs one of the Article 9(2) exceptions, such as explicit consent.
- **Personal code.** The Lithuanian personal identification code may be processed only on a GDPR Article 6(1) legal basis, may not be published and may not be used for direct marketing (Law on Legal Protection of Personal Data, Art. 3).

7 Sector-specific obligations

Travel Rule

Regulation (EU) 2023/1113 has applied since 30 December 2024 `In force`. Every crypto transfer, with no minimum amount, must carry the originator's name, ledger address or account number, and address with official document and customer number (or date and place of birth), plus the beneficiary's name and ledger address or account number (Art. 14(1) and (2)). The originator's data must be verified before the transfer (Art. 14(6)). For a transfer of more than EUR 1,000 to a self-hosted address, the originator's CASP must take adequate measures to assess whether the originator owns or controls that address (Art. 14(5)); the beneficiary's CASP has the mirror obligation for incoming transfers from self-hosted addresses (Art. 16(2)).

Wallet and sanctions screening

The Law on International Sanctions (No IX-2160, consolidated from 30 June 2026) names FNTT, with the Ministry of Finance and the Customs Department, among the competent authorities ensuring implementation of financial sanctions (Art. 11). Government Resolution No 535 of 25 May 2022 (consolidated from 9 December 2025) requires anyone

who freezes funds or economic resources, or learns of assets that should have been frozen, to inform FNTT within two working days.

Tax reporting of user identity (DAC8)

Amendments approved by the Seimas on 19 June 2025 transpose the EU directive on administrative cooperation in tax matters (DAC8) `In force from 1 Jan 2026`. CASPs must collect information on reportable crypto-asset users resident in the EU, including Lithuania, and in third countries, and report it to the State Tax Inspectorate by 31 May for the previous calendar year; the first report, for 2026, is due by 31 May 2027 (State Tax Inspectorate Order No VA-119, consolidated from 25 September 2026). Data must be kept for at least five years. Users who withhold the required data for 60 days after a first reminder must be blocked from reportable transactions. Reporting failures carry fines of EUR 200 to EUR 6,000.

8 Risk indicators and red flags

CRYPTO-ASSET TYPOLOGIES (EBA ML/TF RISK FACTORS GUIDELINES, GUIDELINE 21; BANK OF LITHUANIA AND FNTT)

- **Anonymising access**: IP addresses linked to the darknet, anonymous email or VPNs, or one device or IP shared by many customers.
- **Threshold avoidance**: repeated self-hosted transfers just below EUR 1,000.
- **Pass-through activity**: crypto-assets withdrawn to a self-hosted address immediately after deposit or exchange.
- **Privacy tools**: funds from mixers, tumblers or privacy coins, or links to darknet markets.
- **Money mule profile**: a customer with little understanding of crypto-assets making frequent or high-value transactions.
- **Funding mismatch**: multiple cards or accounts, or accounts in another person's name, used to fund the crypto account.
- **Sanctions exposure**: customer transfers routed through EU-sanctioned banks, as found in the FNTT's 2024 Payeer case.

9 Enforcement and penalties

MiCA breaches

Under Article 15 of the Law on Markets in Crypto-Assets, the Bank of Lithuania may fine legal persons up to EUR 5,000,000 or 10% of total annual income, whichever is higher, and managers and other individuals up to EUR 700,000. For market abuse breaches (MiCA Articles 88 to 92) the caps are EUR 15,000,000 or 15% for legal persons and EUR 5,000,000 for individuals.

AML breaches

Under AML Law Article 39, the Bank of Lithuania and FNTT may fine a financial institution 0.5% to 5% of total annual income; for systematic, serious or repeated breaches, 0.5% to 10% of annual income, or EUR 2,000 to EUR 5,100,000 where 10% of income would be below EUR 5,100,000.

Recent action

In July 2024 FNTT fined Payeer UAB, a Lithuanian-registered virtual currency exchange and wallet operator, more than EUR 8.23 million for international sanctions breaches (serving mainly Russian customers through EU-sanctioned Russian banks) and EUR 1.06 million for AML breaches, including deliberately weak identity verification and failure to report crypto transactions of EUR 15,000 or more. FNTT noted that the decisions could be appealed. In April 2025 FNTT fined UAB "Koncika", a virtual currency operator, for AML breaches that included failures under FNTT Order V-314: image quality, a mismatch between the customer and the document holder, and more than one person taking part in a video session.

10 Recent changes and what to watch

- **10 July 2027** `Adopted, applies 10 Jul 2027` : the EU Anti-Money Laundering Regulation starts to apply directly; remote onboarding procedures built on AML Law Article 11 will need review. AMLA starts selecting entities for direct supervision by 1 July 2027.
- **31 May 2027** `Adopted, first report due 31 May 2027` : CASPs file their first DAC8 report on 2026 users with the State Tax Inspectorate.
- **5 November 2026** `In force` : the Bank of Lithuania announced that 27 websites offering crypto services without a MiCA licence had been blocked.

- **13 October 2026** `Under way, visit autumn 2027`: Lithuania's sixth-round MONEYVAL evaluation began; the technical compliance questionnaire is due in March 2027 and the on-site visit is expected in autumn 2027.
- **1 July 2026** `In force`: the MiCA transitional period ended across the EU; unlicensed providers may no longer serve EU clients.
- **2 March 2026** `In force`: the EBA transition period ended; CASPs providing e-money token services that qualify as payment services need a payment services authorisation.
- **1 January 2026** `In force`: the national virtual currency operator regime ended; the EUR 700 occasional-transaction threshold was repealed; DAC8 data collection for tax reporting began.

11 What this means for identity verification

- Map every remote onboarding path to one of the five Article 11(1) methods; a path that fits none cannot be used to identify the customer.
- For video identification, design to FNTT Order V-314: real-time capture, document tilting, face shown with the document (or an advanced e-signature within one hour), a questionnaire, and the session stops listed in point 22.
- Collect Travel Rule data and tax residence at onboarding to avoid re-contacting customers.
- For self-hosted wallets, assess ownership or control for transfers above EUR 1,000 and apply at least one Article 29(8) risk measure to all such transfers.

IDENTOMAT

How Identomat helps

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

- Video KYC and remote identity verification flows built around Lithuania's permitted remote identification methods, with recordings kept for audit.
- ID document capture and verification, including NFC chip reading, with face match and biometric liveness.
- AML screening against sanctions, PEP and adverse-media lists at onboarding and through ongoing monitoring.
- KYB and beneficial owner verification for corporate clients, plus KYC questionnaires for source-of-funds and tax residence data.
- No-code workflow builder to route customers to enhanced due diligence when risk factors appear.

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

- **Lietuvos Respublikos kriptoturto rinkų įstatymas Nr. XIV-2879 [Law on Markets in Crypto-Assets]**, consolidated version from 2 July 2026, Arts. 2, 3, 15, 22, e-seimas, e-seimas.lrs.lt
- **Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymas Nr. VIII-275 [Law on the Prevention of Money Laundering and Terrorist Financing]**, consolidated version 30 June to 31 December 2026, Arts. 2, 4, 9, 11, 14, 16, 19, 20, 29, 30, 36, 39, e-seimas, e-seimas.lrs.lt
- **FNTT Director's Order No V-314 of 30 November 2016, Techniniai reikalavimai kliento tapatybės nustatymo procesui ... tiesioginio vaizdo perdavimą [Technical requirements for remote customer identification using live video]**, consolidated from 12 January 2021, e-seimas, e-seimas.lrs.lt

- **Lietuvos Respublikos tarptautinių sankcijų įstatymas Nr. IX-2160 [Law on International Sanctions]**, consolidated from 30 June 2026, Art. 11, e-seimas, e-seimas.lrs.lt
- **Government Resolution No 535 of 25 May 2022 on implementing the Law on International Sanctions**, consolidated from 9 December 2025, e-seimas, e-seimas.lrs.lt
- **Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas Nr. I-1374 [Law on Legal Protection of Personal Data]**, consolidated from 30 June 2026, Arts. 3, 7, e-seimas, e-seimas.lrs.lt
- **Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA)**, Arts. 59, 60, 63, 65, 143, Annex IV, EUR-Lex, eur-lex.europa.eu
- **Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets**, Arts. 14, 16, EUR-Lex, eur-lex.europa.eu
- **Regulation (EU) 2024/1624 on the prevention of the use of the financial system for money laundering or terrorist financing**, Art. 90, EUR-Lex, eur-lex.europa.eu
- **Regulation (EU) 2024/1620 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism**, Art. 13, EUR-Lex, eur-lex.europa.eu
- **Lietuvos Respublikos baudžiamasis kodeksas [Criminal Code]**, consolidated from 3 July 2026, Art. 202, e-seimas, e-seimas.lrs.lt
- **Bank of Lithuania Board Resolution No 03-17 of 12 February 2015, Finansų rinkos dalyviams skirti nurodymai, kuriais siekiama užkirsti kelią pinigų plovimui ir (arba) teroristų finansavimui [Instructions to financial market participants on preventing money laundering and terrorist financing]**, consolidated from 18 March 2025, e-tar, e-tar.lt
- **FNTT Director's Order No V-131 of 12 September 2017, Asmens tapatybės dokumento kopijos tvirtinimo ir pateikimo tvarkos aprašas [Procedure for certifying and submitting copies of identity documents]**, e-tar, e-tar.lt
- **Government Resolution No 1458 of 15 December 2000, list of state fee amounts**, consolidated from 3 October 2026, item 3.157, e-seimas, e-seimas.lrs.lt
- **State Tax Inspectorate Order No VA-119 of 10 December 2025, Duomenų apie praneštinus kriptoturto naudotojus teikimo Valstybinei mokesčių inspekcijai tvarkos aprašas [Procedure for reporting data on reportable crypto-asset users]**, consolidated from 25 September 2026, points 21, 41, e-tar, e-tar.lt
- **Regulation (EU) 2016/679 (General Data Protection Regulation)**, Arts. 4(14), 9, EUR-Lex, eur-lex.europa.eu
- **Bank of Lithuania, Authorisation of crypto-asset service providers**, last updated 5 April 2024, lb.lt
- **Bank of Lithuania, Kriptoturto paslaugų teikėjų licencijavimas [Licensing of crypto-asset service providers]**, lb.lt
- **Bank of Lithuania, FAQ: expectations regarding entities seeking a CASP licence** (letter of 22 August 2024), lb.lt
- **Bank of Lithuania, Crypto-asset service providers that do not intend to continue their operations must ensure smooth winding down**, 18 July 2025, lb.lt

- **Bank of Lithuania, Lietuvoje baigiasi kriptoturto paslaugų pereinamasis laikotarpis [Transitional period for crypto-asset services ends in Lithuania]**, 31 December 2025, lb.lt
- **Bank of Lithuania, MiCA reglamento pereinamojo laikotarpio pabaiga [End of the MiCA transitional period]**, 2 July 2026, lb.lt
- **Bank of Lithuania, Blokuota prieiga prie beveik 30 interneto svetainių [Access blocked to almost 30 websites illegally offering crypto services]**, 5 November 2026, lb.lt
- **Bank of Lithuania, Operacijoms su EMT reikės mokėjimo paslaugų licencijos [E-money token operations will require a payment services licence]**, 11 June 2025, lb.lt
- **Bank of Lithuania, Lietuvos bankas and FCIS step up cooperation on supervision of crypto-asset services**, 25 November 2024, lb.lt
- **Bank of Lithuania, Prasideda Lietuvos 6-asis MONEYVAL tarpusavio vertinimo turas [Lithuania's sixth MONEYVAL evaluation round begins]**, 13 October 2026, lb.lt
- **FNTT, The FCIS fines virtual currency operator a record fine of almost EUR 9.3 million**, 11 July 2024, fntt.lrv.lt
- **FNTT, Sprendimai dėl poveikio priemonių [Decisions on sanctions imposed]**, 2025 decisions, fntt.lrv.lt
- **Ministry of Finance, Fines imposed for infringements of delivery of information on crypto-asset users**, 12 September 2025, finmin.lrv.lt
- **Bank of Lithuania, Licences issued (register)**, lb.lt
- **Ministry of Finance, Kriptoturto paslaugų teikėjai privalės teikti informaciją apie kriptoturto naudotojus [CASPs will have to report information on crypto-asset users]**, 19 June 2025, finmin.lrv.lt
- **EBA, Guidelines amending the ML/TF Risk Factors Guidelines (EBA/GL/2024/01)**, 16 January 2024, Guideline 21, eba.europa.eu
- **EBA, Guidelines on the use of remote customer onboarding solutions**, press release 22 November 2022, eba.europa.eu
- **EBA, EBA advises national authorities on actions to take at the end of the transition period under its No-Action Letter on the interplay between PSD2 and MiCA**, 12 February 2026, eba.europa.eu
- **EBA, Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113**, eba.europa.eu