



Identomat

COMPLIANCE GUIDE

Crypto & Virtual Assets Compliance in Estonia

COUNTRY **Estonia**

INDUSTRY **Crypto & Virtual Assets**

LAST UPDATED **21 October 2026**

KEY REGULATORS **Financial Supervision and Resolution Authority (Finantsinspektsioon) · Financial Intelligence Unit · Estonian Tax and Customs Board**

Key takeaways

- Since 1 July 2026, only firms authorised under the EU Markets in Crypto-Assets Regulation (MiCA), either by Estonia's Finantsinspektsioon or by another European Economic Area (EEA) supervisor, may provide crypto services in Estonia. The old licences from the Financial Intelligence Unit (FIU) no longer count.
 - An Estonian authorisation means an Estonian-registered limited company, at least two management board members, minimum capital of €50,000 to €150,000 depending on the services, a €3,000 application fee and a review of up to 25 working days for completeness plus 40 for assessment.
 - A crypto firm may only serve customers it has fully onboarded: one-off transactions without an account are banned, and every customer's phone number and email must be collected and verified identity data kept for five years after the relationship ends.
 - Onboarding online is allowed, but non-EEA residents, customers moving more than €15,000 a month (€25,000 for companies) and customers from high-risk countries must be identified through a qualifying electronic ID, a qualified trust service or a tightly specified remote method. Other remote onboarding counts as a higher-risk factor.
 - Every transfer to or from a customer's own (self-hosted) wallet triggers enhanced checks under Estonian law, and from 10 July 2027 the EU Anti-Money Laundering Regulation replaces much of the national rulebook.
-

Estonia is open to crypto businesses, but only under the EU-wide MiCA regime. The FIU-licensed virtual currency sector that once counted hundreds of firms has been closed down: as of October 2026, Finantsinspektsioon lists one Estonian-authorised crypto-asset service provider, while a larger group of providers authorised elsewhere in the EEA serve Estonian customers on a cross-border basis.

Finantsinspektsioon (the Financial Supervision and Resolution Authority) grants and supervises authorisations and enforces anti-money laundering (AML) compliance by authorised firms. The FIU receives suspicious transaction reports. The Tax and Customs Board collects crypto transaction data for tax purposes.

The biggest obstacle for a new entrant is the authorisation itself: a full MiCA application, filed in Estonian through the regulator's portal, backed by Estonian substance and governance.

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 for crypto	Level	Official site
Finantsinspektsioon (Financial Supervision and Resolution Authority)	MiCA authorisation and supervision of crypto-asset service providers and token issuers; AML supervision of the firms it authorises	National	fi.ee
Financial Intelligence Unit (Rahapesu Andmehüroo)	Receives suspicious transaction reports and periodic reports; former licensing authority for virtual currency service providers	National	fiu.ee
Estonian Tax and Customs Board	Crypto-asset tax reporting by service providers (DAC8)	National	emta.ee
Data Protection Inspectorate	Supervision of personal and biometric data processed during onboarding	National	aki.ee
Information System Authority	Runs the national electronic identity (eID) infrastructure used for remote identification	National	ria.ee

European Securities and Markets Authority and European Banking Authority

MiCA technical standards and guidelines, including authorisation forms and AML guidelines referred to in Estonian law

Supranational (EU)

esma.europa.eu,
eba.europa.eu

Estonia is a unitary state, so authorisation and supervision are national.

2 Licensing and authorisation

MiCA ([Regulation \(EU\) 2023/1114](#), Article 59) prohibits providing crypto-asset services in the EU without authorisation. The [Market in Crypto-Assets Act](#) (krüptovaraturu seadus, RT I, 21.06.2024, 3), in force since 1 July 2024, supplements it. Under § 5, a participant in the crypto-asset market needs an authorisation granted and revoked by Finantsinspektsioon. The authorisation has no expiry date and cannot be transferred.

Requirements for an Estonian authorisation

Form and seat

A private or public limited company with its registered office in Estonia (§ 5(4), § 7(1)).

Governance

At least two management board members. A private limited company needs a supervisory board of at least three, unless it provides neither custody nor a trading platform (§ 7(2) and (3)).

Capital

MiCA Annex IV minimums: €50,000 (for example order execution, transfers, advice); €125,000 if custody or exchange services are added; €150,000 to operate a trading platform.

Staff competence

Staff giving information or advice must have the knowledge listed in § 8. Finantsinspektsioon guidelines on staff knowledge and skills apply from 28 July 2026.

Process and timeline

According to [Finantsinspektsioon's authorisation page](#) (last edited 27 May 2026):

- **Filing:** applications use the ESMA application form and go through the regulator's application portal, mandatory since 18 March 2026. The application is filed in Estonian; supporting documents may be in English if the application says so.
- **Fee:** €3,000.
- **Review:** Finantsinspektsioon checks completeness within 25 working days, then assesses the application within 40 working days. The assessment can be paused for up to 20 working days for questions.
- **Wind-down plan:** new applicants must also file a plan for winding up their operations (Finantsinspektsioon notice of 23 March 2026).

Credit institutions, e-money institutions and investment firms instead obtain a Finantsinspektsioon decision under MiCA Article 60 (§ 6(1)).

Passporting and third-country firms

A provider authorised in another EEA state may serve Estonia through a branch or cross-border after notifying its home supervisor (MiCA Article 65; § 12 of the Act). The reverse-solicitation exemption in MiCA Article 61 is narrow: any solicitation of EU clients, by any means, takes a third-country firm outside it.

Operating without authorisation

The FIU's virtual currency licences lost effect when the transition ended on 1 July 2026 (§ 48(4) of the Act). Firms whose MiCA applications were still pending on that date may continue to serve existing clients only, with no new client contracts until Finantsinspektsioon decides (§ 48(5)). Section 48(5) links unauthorised activity to the offence in § 372 of the Penal Code.

3 AML, KYC and customer due diligence

Crypto-asset service providers are financial institutions, and therefore obliged entities, under § 6(2) (3¹) of the [Money Laundering and Terrorist Financing Prevention Act](#) (rahapesu ja terrorismi rahastamise tõkestamise seadus, version in force from 21 July 2026). The separate category of "virtual currency service provider" was repealed from 1 July 2026. Finantsinspektsioon enforces the Act for the firms it supervises (§ 64(2)).

Crypto-specific rules

- **No occasional transactions:** crypto-asset service providers may not provide services outside a business relationship (§ 25(1³), from 1 July 2026). The general €15,000 occasional-transaction threshold in § 19 therefore does not help crypto firms.
- **No anonymous accounts:** opening anonymous crypto-asset accounts is prohibited, and any such contract is void (§ 25(2)).
- **Contact data:** identity verification must capture at least the customer's telephone number and email address (§ 25(2²)).
- **Self-hosted wallets:** the firm's risk assessment must define its risk appetite for transfers to and from self-hosted addresses (§ 13(1¹)). Enhanced due diligence (EDD) applies whenever a transfer goes to or comes from one (§ 36(2)(6)), and additional measures include gathering information on the origin and destination of the crypto-assets (§ 38(2)(7)).
- **Crypto correspondent relationships:** a provider must check that a counterparty provider holds an authorisation, or a registration if established in a third country (§ 40(1¹)).

Core customer due diligence

Before the relationship starts (§ 19(5)), § 20 requires identifying and verifying the customer, any representative and the beneficial owner, establishing the purpose of the relationship, checking for politically exposed persons (PEPs), and then ongoing monitoring. Verification may use electronic identification and trust services (§ 20(1)(1)).

EDD always applies to doubts about data or documents, politically exposed persons, high-risk third countries and self-hosted wallet transfers (§ 36(2)), and the customer's risk profile must then be reassessed within six months (§ 38(3)). Corporate customers from EU states need a beneficial ownership register extract (§ 20(2¹)).

Reporting and retention

Suspensions must be reported to the FIU without delay and within two working days (§ 49(1)), including where the relationship is never established (§ 49(2)). Firms also submit periodic reports to the FIU under § 54¹. Identification records are kept for five years after the relationship ends (§ 47(1)), then deleted unless the supervisor orders up to five more years (§ 47(7)).

What must be collected and verified. Section 21 of the AML Act requires each natural-person customer's name and personal identification code. Where the customer has no Estonian code, the date of birth and place of residence are required instead. The data must be verified against a credible and independent source.

Accepted documents. Accepted documents are:

- Estonian identity documents;
- a valid foreign travel document;
- a driving licence meeting the Identity Documents Act standard (§ 21(3)).

Where the original is not available, a certified copy or other reliable sources, including electronic identification, may be used. In that case at least two different sources are required (§ 21(4)).

Remote identification. Before onboarding anyone remotely under § 31, a firm must adopt rules of procedure that ensure secure identification and manage the risks of not meeting the customer (§ 14(1)). Section 31(3) recognises two remote routes:

- an electronic identification scheme notified under eIDAS (Regulation (EU) No 910/2014) at assurance level "substantial" or "high";
- a qualified trust service.

Where neither can be used, the remote tool must meet three tests in § 31(3¹):

- the data collected must be correct and current;
- images, video, audio and data must be captured and stored securely, in sufficient quality to identify the person unambiguously;
- if the connection drops or a technical fault occurs, the identification must fail.

Estonian eID. The [Information System Authority](#) lists the ID card, Mobile-ID, the e-Resident's digital ID, diplomatic ID and residence cards as valid means of electronic identification. It rates the private Smart-ID at "high" for holders of an Estonian personal code, but notes it cannot distinguish residents from non-residents. An e-Resident's digital ID used remotely must always be combined with another identity document (§ 31(4)).

Reliance and outsourcing. A firm may rely on or outsource CDD under § 24 but stays responsible (§ 24(7)), and never to anyone in a high-risk third country (§ 24(6)).

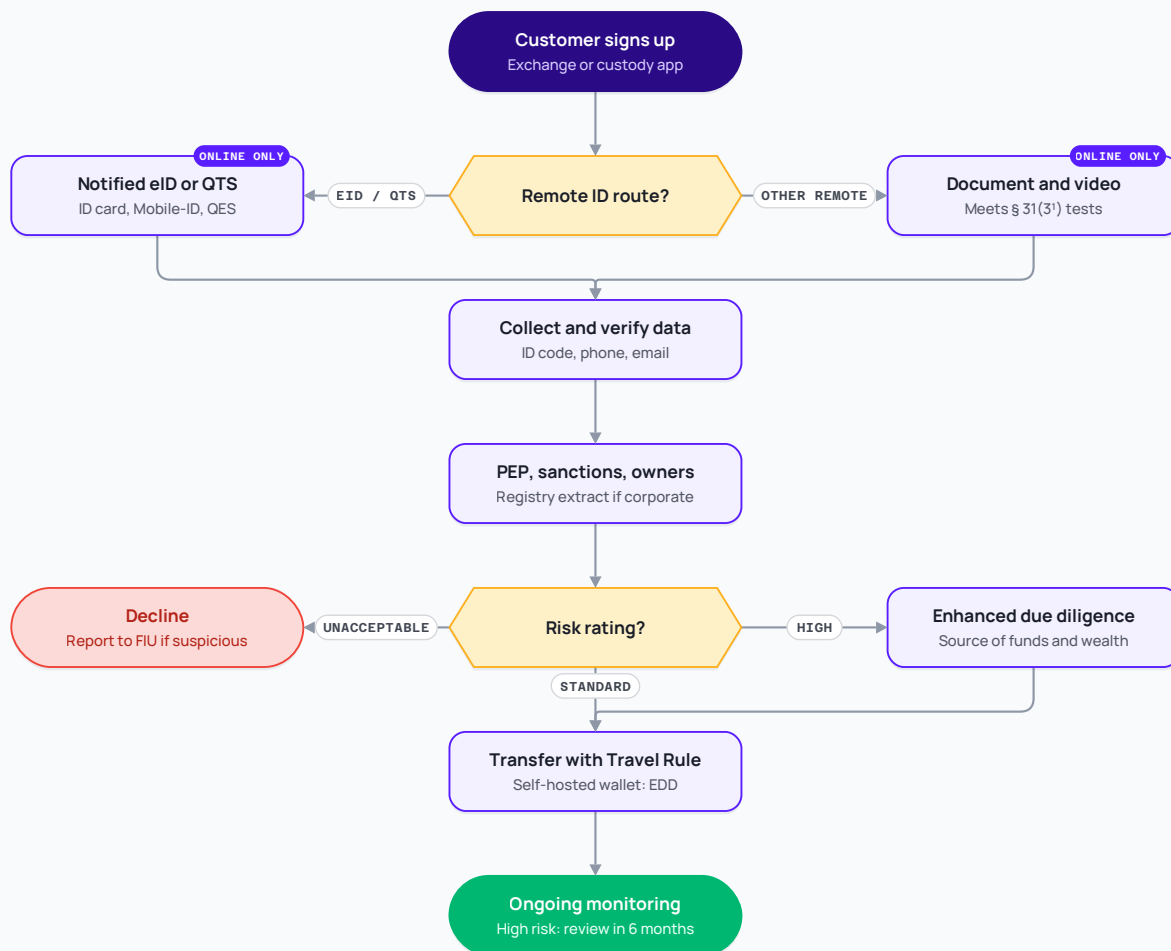


Figure 1. Remote onboarding and first transfer at a crypto-asset service provider serving Estonian customers.

5 Digital channels: what's different

Bottom line: the due diligence obligations are the same online and in person. However, the AML Act prescribes which remote identification methods may be used for higher-risk customers, treats other remote onboarding as a higher-risk factor, and adds evidence retention rules for remote checks.

Requirement	In person	Online / remote	Difference
Due diligence measures	Full CDD under § 20 before the relationship	Full CDD under § 20 before the relationship	Same

Identity evidence	Original document under § 21(3)	eID scheme at substantial or high, qualified trust service, or a method meeting § 31(3 ¹)	Differs
Mandatory method	None beyond § 21	§ 31 route required for non-EEA residents and above €15,000 (natural) or €25,000 (legal) monthly outgoing payments; eID or qualified trust service for high-risk third countries	Differs
Risk treatment	Standard, risk-based	Remote onboarding without § 31 safeguards is a higher-risk factor (§ 37(3)(4))	Differs
e-Resident digital ID	Not applicable	Must be combined with another identity document (§ 31(4))	Differs
Evidence retained	Documents or copies for five years (§ 47(1))	Also document data, the identity database query and the time-stamped procedure record for five years (§ 47(6))	Differs
Contact data and account type	Phone and email; no anonymous accounts	Phone and email; no anonymous accounts	Same
Travel Rule and self-hosted wallets	Regulation (EU) 2023/1113 and § 36(2)(6) EDD	Regulation (EU) 2023/1113 and § 36(2)(6) EDD	Same

When the § 31 route becomes mandatory

When the customer is not met in person, § 31(1) requires a notified eID scheme, a qualified trust service or a tool meeting § 31(3¹) in either of two situations:

- the customer lives or is seated outside the EEA;
- monthly outgoing payments exceed €15,000 for a natural person or €25,000 for a legal person.

For customers in a high-risk third country, only the eID scheme or qualified trust service will do (§ 31(1¹)).

Remote onboarding outside § 31 raises the risk rating

For lower-value EEA customers, § 31 is optional, but remote onboarding without it is a higher-risk factor (§ 37(3)(4)), so the method chosen feeds the risk profile.

Remote evidence and failed sessions

For remote checks, § 47(6) requires keeping the identity document data, the identity database query record and the time-stamped procedure data for five years after the relationship ends. An interrupted session must end in a failed identification (§ 31(3¹)(3)). Where eID or a qualified trust service was used, document copies need not be kept (§ 47(1¹)).

What is changing

Adopted, applies 10 Jul 2027 The EU Anti-Money Laundering Regulation ([Regulation \(EU\) 2024/1624](#)) will allow remote verification through eID means at assurance level "substantial" or "high" and relevant qualified trust services (Article 22(6)).

6 Data protection and biometrics

The General Data Protection Regulation (GDPR, [Regulation \(EU\) 2016/679](#)) applies directly, supervised by the Data Protection Inspectorate. Two features bite on crypto onboarding.

- **Purpose limitation:** under § 48(2) of the AML Act, data gathered for due diligence may be processed only for AML purposes, treated as a matter of public interest under the GDPR. It may not be reused, for example, for marketing. Customers must receive information on this processing before the relationship begins (§ 48(3)).
- **Biometric data:** face images processed to uniquely identify a person, such as a face match in remote onboarding, are special-category data under GDPR Article 9. Their processing is prohibited unless an Article 9(2) condition applies, such as explicit consent.

The Act sets the retention clock for identity records at five years after the relationship ends, followed by deletion (§ 47(7)).

Travel Rule

[Regulation \(EU\) 2023/1113](#), applying since 30 December 2024 and expressly referenced in § 7(5) of the Market in Crypto-Assets Act, sets no minimum amount for transfers between providers. The originator's provider must send the following with each transfer, before or at the same time as it (Article 14):

- the originator's name, address and account details;
- the originator's official personal document number and customer identification number, or alternatively date and place of birth;
- the beneficiary's name and wallet address or account number.

Both sides verify their own customer's data before the assets move (Articles 14(6) and 16(3)).

Self-hosted wallets

For transfers to or from a self-hosted address, the provider must obtain and hold the originator and beneficiary information. For amounts above €1,000, it must take adequate measures to assess whether the address is owned or controlled by its customer (Articles 14(5) and 16(2)). Estonian law goes further than the EU baseline: § 36(2)(6) of the AML Act applies EDD to every such transfer, whatever the amount.

Custody and token classification

Custodians must segregate client crypto-assets legally and operationally (MiCA Article 75(7)). MiCA does not cover tokens that are financial instruments or deposits (Article 2(4)), and only credit and e-money institutions may issue e-money tokens (§ 6(3)).

Tax reporting of users

Under the EU's DAC8 directive, the [Tax and Customs Board](#) requires reporting crypto-asset service providers to collect identity and transaction data on Estonian and foreign users from 1 January 2026, including tax residence and tax identification number, with the first annual report, for 2026, due in 2027.

Article 23 of Regulation (EU) 2023/1113 also requires internal controls to implement EU and national sanctions when making transfers, which in practice includes screening wallet counterparties.

CRYPTO TYPOLOGIES IDENTIFIED BY ESTONIAN AUTHORITIES

- **Fiat in, crypto out:** large incoming fiat transfers converted at once to stablecoins and withdrawn to a cold wallet (FIU Yearbook 2024).
- **Profile mismatch:** transaction volumes exceeding the wealth the customer declared at onboarding.
- **Location mismatch:** logins from countries that do not match the customer's country of residence.
- **Adverse media:** links to investment platforms under foreign regulator warnings.
- **Crypto casinos:** serving crypto casinos or related companies, identified by the FIU as the main concentration of sector risk.
- **Nested services:** customers that are themselves service providers to their own clients, creating correspondent-type exposure (FIU action against B2BX, February 2025).
- **Self-hosted and anonymity:** transfers to or from self-hosted wallets, and any product favouring anonymity (§§ 36 and 37 of the AML Act).

Penalties are maximum misdemeanour fines; for legal persons the cap is the highest of a fixed amount, a multiple of the gain, or a share of turnover.

Breach	Natural person	Legal person	Provision
MiCA service-provider requirements (Articles 59, 60, 64 to 83)	€700,000 or 2x gain	€5,000,000, 2x gain or 5% of turnover	Market in Crypto-Assets Act § 37
Market abuse (MiCA Articles 89 to 92)	€5,000,000 or 3x gain	€15,000,000, 3x gain or 15% of turnover	Market in Crypto-Assets Act § 42

Failure to identify and verify customers (firms under Finantsinspeksioon supervision)	€5,000,000 or 2x benefit	€5,000,000, 2x benefit or 10% of consolidated turnover	AML Act § 84
Travel Rule breaches (Regulation (EU) 2023/1113)	€5,000,000 or 2x benefit	€5,000,000, 2x benefit or 10% of consolidated turnover	AML Act § 96 ²
Opening anonymous crypto-asset accounts	€5,000,000 or 2x benefit	€5,000,000, 2x benefit or 10% of consolidated turnover	AML Act § 83

Finantsinspeksioon conducts the extra-judicial proceedings for misdemeanours under the Market in Crypto-Assets Act, with a three-year limitation period (§ 47). Non-compliance levies on a legal person reach €32,000 on the first occasion and €100,000 later, capped at €5,000,000 or 10% of turnover (§ 36).

Recent action. In February 2025, the [FIU reported](#) that B2BX Digital Exchange OÜ gave up its virtual currency licence during supervision proceedings that would have led to revocation. The firm's total revenue exceeded €1 billion. The FIU found weak due diligence on correspondent-type clients, no internal control policy, no source-of-funds checks and late suspicious transaction reports.

10 Recent changes and what to watch

- **Adopted, applies 10 Jul 2027** **EU Anti-Money Laundering Regulation:** Regulation (EU) 2024/1624 replaces much of the national AML rulebook. It adds self-hosted wallet risk measures (Article 40) and bans accounts using anonymity-enhancing coins (Article 79).
- **In force 28 Jul 2026** **Finantsinspeksioon competence guidelines:** staff giving advice need more knowledge than staff giving information, and firms must assess staff competence at least annually.
- **In force 1 Jul 2026** **End of the transition:** FIU virtual currency licences lost effect. Crypto firms may no longer serve customers outside a business relationship, must collect phone and email, and may not open anonymous crypto-asset accounts.
- **In force 18 Mar 2026** **Application portal:** authorisation applications must be filed through Finantsinspeksioon's portal.
- **In force 1 Jan 2026** **DAC8 data collection:** reporting providers collect user identity and transaction data for tax reporting in 2027.

- **In force 30 Dec 2024** Travel Rule and self-hosted EDD: Regulation (EU) 2023/1113 and the Estonian EDD trigger for self-hosted transfers apply.

11 What this means for identity verification

- **Two remote routes:** notified eID or a qualified trust service (mandatory for high-risk third countries), and a document-and-video route meeting § 31(3¹), with a hard fail on interrupted sessions.
- **Route by risk:** residence and expected monthly outgoing payments above €15,000 or €25,000 decide whether the § 31 route is required; watch for customers who cross the threshold later.
- **Data set:** personal code (or date of birth and residence), phone, email, and the address and document data Travel Rule messages need. e-Residents using their digital ID also need a second document.
- **Evidence and biometrics:** keep remote session records for five years after the relationship ends, then delete; settle the GDPR Article 9 basis for face match and liveness before go-live.
- **Transfers:** build self-hosted wallet ownership checks into the transfer flow and send every self-hosted transfer to enhanced review.

How Identomat helps

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

- Remote KYC onboarding with ID document capture and verification (including NFC), face match and biometric liveness, with the full session recorded for audit.
- Video KYC for customers whose residence or payment volumes call for a stronger remote identification route.
- AML screening against sanctions, PEP and adverse-media lists at onboarding and on an ongoing basis.
- KYB and beneficial owner verification for corporate crypto customers.
- No-code workflow builder to route customers by residence, risk and expected volumes, with configurable data retention.

[Request a meeting](#)

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- Krüptovaraturu seadus [Market in Crypto-Assets Act], RT I, 21.06.2024, 3, Riigi Teataja, English translation riigiteataja.ee; Estonian text riigiteataja.ee
- Rahapesu ja terrorismi rahastamise tõkestamise seadus [Money Laundering and Terrorist Financing Prevention Act], version in force from 21 July 2026, Riigi Teataja, English translation riigiteataja.ee; Estonian text riigiteataja.ee
- Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA), Articles 2, 59 to 61, 65, 75 and Annex IV, EUR-Lex, eur-lex.europa.eu

- Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets, Articles 14, 16, 23 and 26, EUR-Lex, eur-lex.europa.eu
- Regulation (EU) 2024/1624 (Anti-Money Laundering Regulation), Articles 19, 22, 40 and 79, EUR-Lex, eur-lex.europa.eu
- Regulation (EU) 2016/679 (General Data Protection Regulation), Article 9, EUR-Lex, eur-lex.europa.eu
- The operating license in markets of crypto assets, Finantsinspektsioon, page last edited 27 May 2026, fi.ee
- Crypto asset service providers in Estonia (register of supervised entities), Finantsinspektsioon, fi.ee; Cross-border crypto asset service providers, fi.ee
- The transition period for crypto companies ends in summer, Finantsinspektsioon, 23 March 2026, fi.ee
- Finantsinspektsioon is clarifying the competence requirements for staff of crypto companies, Finantsinspektsioon, 26 March 2026, fi.ee
- The transitional period for providers of crypto asset services is ending, Financial Intelligence Unit, 30 June 2026, fiu.ee
- B2BX Digital Exchange OÜ renounced their license of virtual asset services during supervision proceeding, Financial Intelligence Unit, 11 February 2025, fiu.ee
- Estonian Financial Intelligence Unit Yearbook 2024, published June 2025, sections on vulnerability of market participants and best report of the year, fiu.ee
- Crypto-asset tax reporting (DAC8/CARF), Estonian Tax and Customs Board, last updated 5 November 2025, emta.ee
- Electronic Identity eID, Information System Authority, last updated 20 July 2026, ria.ee