



Identomat

COMPLIANCE GUIDE

Banking & Digital Banking Compliance in Estonia

COUNTRY **Estonia**

INDUSTRY **Banking & Digital Banking**

LAST UPDATED **21 October 2026**

KEY REGULATORS **Financial Supervision and Resolution Authority (Finantsinspektsioon) ·
European Central Bank · Financial Intelligence Unit**

Key takeaways

- Only a licensed bank may take deposits from the public in Estonia or call itself a "pank" (bank). A new bank needs at least 5 million euros of paid-in share capital, and the licence decision takes 6 to 12 months.
 - Fully remote account opening is legal. For customers who live outside the European Economic Area (EEA), or whose outgoing payments exceed 15,000 euros a month (individuals) or 25,000 euros a month (companies), the bank must use a government-notified electronic ID, a qualified trust service or a video tool that meets statutory quality rules.
 - Every bank must identify each customer and beneficial owner before opening the account, screen for politically exposed persons and sanctions, and report suspicions to the Financial Intelligence Unit within two working days.
 - AML breaches by a supervised bank can cost up to 5 million euros or 10% of consolidated turnover per offence.
 - The EU Anti-Money Laundering Regulation replaces much of the Estonian rulebook from 10 July 2027, and a fraud-prevention bill letting banks refuse manipulated payments is before Parliament (not yet law).
-

Estonia is open to digital banking, and its national electronic identity infrastructure makes remote onboarding routine. Market access is controlled, though: a credit institution licence is granted by the European Central Bank on a proposal from Finantsinspektsioon, and EEA banks can enter by passport or branch.

Finantsinspektsioon (the Financial Supervision and Resolution Authority) supervises banks for prudential, conduct and AML purposes. The Financial Intelligence Unit receives reports and coordinates financial sanctions, and Eesti Pank is the central bank.

The biggest obstacle for a new entrant is building a remote identification and monitoring setup that meets section 31 of the AML Act and the supervisor's guidelines. This matters most for non-resident customers, whom the national risk assessment treats as a key exposure for Estonian banks.

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
Finantsinspeksioon (Financial Supervision and Resolution Authority)	Bank licensing proposals, prudential and conduct supervision, AML and financial sanctions supervision of banks	National	fi.ee
European Central Bank	Grants and withdraws credit institution licences; supervises banks within the Single Supervisory Mechanism	Supranational (euro area)	via fi.ee
Financial Intelligence Unit (Rahapesu Andmebüroo)	Receives suspicious activity and cash reports; competent authority for financial sanctions	National	fiu.ee
Eesti Pank	Central bank; macroprudential measures and statistical reporting	National (Eurosystem)	eestipank.ee
Ministry of Finance	AML policy, national risk assessment, financial-fraud legislation	National	fin.ee
Data Protection Inspectorate	Supervision of personal and biometric data processing	National	aki.ee

The European Banking Authority issues guidelines that Finantsinspektsioon adopts as advisory guidelines, and the EU Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) will begin direct supervision of 40 entities across the EU from 1 January 2028.

2

Licensing and authorisation

Under the Credit Institutions Act (krediidiasutuste seadus), § 4, credit institutions have the exclusive right to receive deposits or other repayable funds from the public, and § 13 requires a licence for that activity. The licence also covers investment services to the extent stated in it. Only credit institutions may use "pank" or "ühistupank" (association bank) in their business name (§ 12).

Capital

A new bank must have paid-in share capital of at least 5 million euros; an operating company must hold initial capital of the same amount (§ 35).

Application

The management board files the application with a three-year business plan, IT and security systems, internal rules, manager and qualifying-holder information, and a commitment to Guarantee Fund contributions (§§ 13¹–13²). The processing fee is 1,500 euros.

Decision

The decision is due within six months of a complete file and no later than 12 months after the application (§ 14). The European Central Bank decides on a proposal from Finantsinspektsioon.

Seat

An Estonian-licensed bank must have its registered office and head office in Estonia (§ 13(2)).

Banks authorised in another EEA state may operate through a branch or cross-border services under the passport. A bank from outside the EEA must obtain Finantsinspektsioon authorisation for an Estonian branch. That procedure was rewritten on 21 July 2026 to transpose Directive (EU) 2024/1619 (the sixth Capital Requirements Directive), including a description of the branch's activities and governance arrangements.

Deposits are protected by the Guarantee Fund up to 100,000 euros per depositor per bank. Taking deposits from the public without a licence breaches the statutory monopoly in § 4.

Non-bank payment, e-money and consumer credit licences are separate regimes and do not permit deposit-taking.

3

AML, KYC and customer due diligence

Credit institutions, and branches of foreign credit institutions registered in Estonia, are obliged entities under § 2 and § 6 of the Money Laundering and Terrorist Financing Prevention Act (rahapesu ja terrorismi rahastamise tõkestamise seadus, "MLTFPA"). Finantsinspektsioon enforces the Act against the banks it supervises (§ 64(2)).

When due diligence applies

Due diligence applies at the start of every business relationship, for occasional transactions of 15,000 euros or more, and whenever there is suspicion or doubt about earlier data (§ 19). Measures in § 20(1), clauses 1 to 5, must be completed before the account is opened or the transaction made (§ 19(5)). Banks must apply due diligence to occasional money transfers above 1,000 euros (§ 25(1¹)). Anonymous accounts, passbooks, crypto-asset accounts and safe-deposit boxes are prohibited (§ 25(2)).

What must be done

A bank identifies and verifies the customer and any representative, identifies the beneficial owner and understands the ownership and control structure, and establishes the purpose and nature of the relationship. It also checks for politically exposed person (PEP) status and monitors the relationship (§ 20). The beneficial owner of a company is the natural person with ultimate control, with a fallback test of more than 25% ownership and then the senior managing official (§ 9). Where an EU register holds beneficial owner data, the bank must obtain the register extract and report discrepancies to the Estonian registrar (§ 20(2¹), (2⁴)). A bank may not deal with a company whose capital is more than 10% bearer shares (§ 42(2)).

Enhanced due diligence

Enhanced measures are mandatory for PEPs, high-risk third countries, doubts about data authenticity, and countries with weak AML systems or significant corruption where the section 31 remote safeguards are not used (§ 36). PEP relationships need senior management approval, source of wealth and funds checks and enhanced monitoring (§ 41). After enhanced due diligence, the customer's risk profile must be reassessed within six months (§ 38(3)).

Reporting and retention

Suspicious go to the Financial Intelligence Unit without delay and no later than two working days after detection, including for refused or abandoned relationships (§ 49(1)–(2)). For banks, the 32,000-euro cash report applies only to cash foreign exchange with persons who are not customers; other obliged entities report all cash transactions above that amount (§ 49(3)). Identification documents, transaction records and correspondence are kept for at least five years after the relationship ends (§ 47).

4 Identity verification and onboarding

A natural person is identified from an identity document under the Identity Documents Act, a valid foreign travel document, a qualifying driving licence or, for children under seven, a birth certificate (MLTFPA § 21(3)). The bank records the name, personal identification code (or date of birth and residence), and contact details, and verifies name and identity code from a credible and independent source. If the original is not available, the bank may verify identity from notarised copies or from at least two other reliable sources, including electronic identification and trust services (§ 21(4)). Legal persons are verified against the commercial register, which can replace document requests where the bank has access (§ 22).

Finantsinspeksioon's advisory guidelines (amended 8 April 2024) set out the methods. Face-to-face identification compares the person's face with the document photo. IT-based identification compares a facial image captured in the session with the document photo. Where the guidelines allow a "two sources" method, the bank combines an identity document image or strong electronic authentication with a second source such as a population register check, another document or a payment from an account in the customer's name. If the customer's risk is average or higher, the customer must also send a recently taken facial photo.

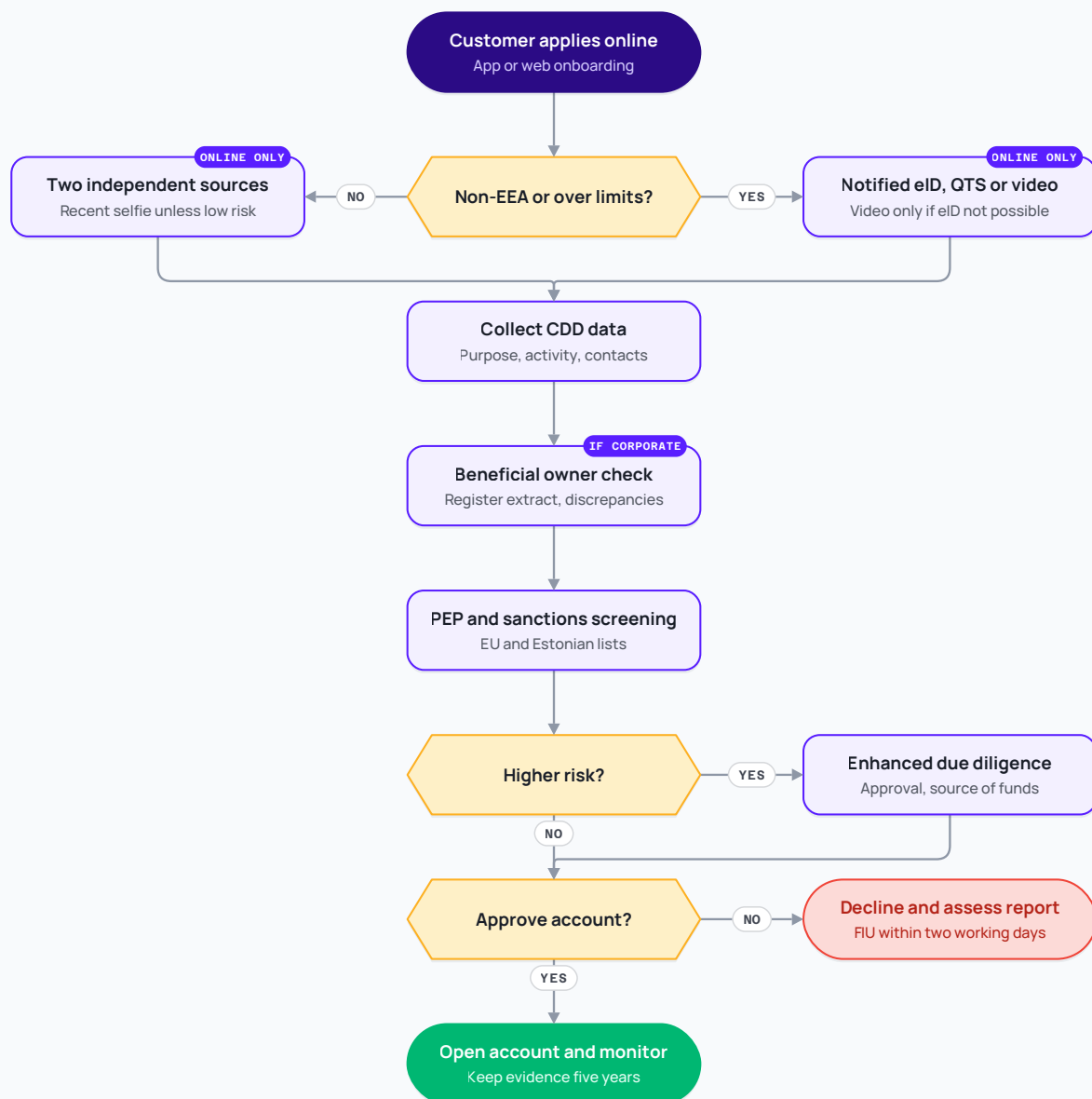


Figure 1. Remote retail and business account opening at an Estonian bank (MLTFPA §§ 20, 31, 36).

A bank may rely on another obliged entity's due diligence, or outsource verification to an identity provider under a written contract that preserves supervisory access and is notified to the supervisor in advance. Nothing may be outsourced to a person in a high-risk third country, and the bank remains fully responsible (§ 24).

Bottom line: remote account opening is fully permitted, but it carries method rules: for non-EEA customers and higher-volume accounts the AML Act fixes which remote tools are acceptable, and remote onboarding without those safeguards is treated as higher risk.

Requirement	In person / branch	Online / remote	Difference
Permission	Face-to-face meeting with original document	Allowed under § 31 rules of procedure for secure remote identification (§ 14(1 ¹))	Differs
Non-EEA or high-volume customers	Any § 21(3) identity document	Notified eIDAS scheme (substantial or high), qualified trust service, or compliant video tool (§ 31(1), (3), (3 ¹))	Differs
High-risk third country residents	Enhanced due diligence	Enhanced due diligence plus notified eID scheme or qualified trust service only (§ 31(1 ¹))	Differs
Risk classification	Standard risk-based approach	Remote onboarding without § 31 safeguards is a higher-risk factor (§ 37(3) clause 4)	Differs
E-resident digital ID	Not used for identification	Must be combined with a second § 21(3) document (§ 31(4))	Differs
Evidence kept	Copies of documents, five years (§ 47(1))	Document data, identity database query and timestamped session data, five years (§ 47(6))	Differs
CDD content, PEP and beneficial owner checks	§ 20 measures	§ 20 measures	Same
Suspicious activity reporting	Two working days (§ 49)	Two working days (§ 49)	Same

The section 31 thresholds

Section 31 of the MLTFPA (as rewritten from 1 July 2024) applies when due diligence is not done in the same location. It requires a notified eIDAS scheme at "substantial" or "high" assurance, a qualified trust service, or a means meeting § 31(3¹). This applies where the customer lives outside the EEA, or where monthly outgoing payments exceed 15,000 euros for a natural person or 25,000 euros for a legal person. A § 31(3¹) tool, used only where an eIDAS scheme or trust service is not possible, must keep data correct and current and capture images, video and audio securely and in unambiguous quality. It must also treat a dropped connection or technical fault as a failed identification. Banks may query the state identity documents database.

Below the thresholds

For EEA residents below those payment levels, Finantsinspektsioon's guidelines allow the two-source method instead of face-to-face or IT-based identification. Banks must also follow the European Banking Authority's guidelines on remote customer onboarding, which Finantsinspektsioon adopted in part from 2 October 2023. Under that adoption, use of an eIDAS-notified "substantial" scheme together with § 31 satisfies several of the European Banking Authority's evidence and liveness criteria.

What is changing

Regulation (EU) 2024/1624 **Adopted, applies 10 Jul 2027** will set EU-wide customer due diligence rules, so the Estonian section 31 regime is expected to be revised. A government fraud bill **Bill, not enacted** would let banks refuse payments where the customer appears to have been manipulated, even if strongly authenticated.

6 Data protection and biometrics

The General Data Protection Regulation applies directly, supervised by the Data Protection Inspectorate. For AML, MLTFPA § 48(2) declares that processing personal data to prevent money laundering and terrorist financing is in the public interest. Data collected for AML may not be reused for other purposes such as marketing. Customers must be informed about AML processing before the relationship begins (§ 48(3)).

Facial images captured for remote identification are biometric data and a special category of personal data under the General Data Protection Regulation, so the bank needs a lawful basis for that processing in addition to the AML purpose. Retention is set by the MLTFPA rather than chosen freely. Remote identification records are kept for five years after the

relationship ends (§ 47(6)) and then deleted, unless the supervisor orders retention for up to five more years (§ 47(7)). Where the customer was identified with electronic identification or the document is in a state database, the bank need not retain document copies (§ 47(1¹)).

7 Sector-specific obligations

Correspondent banking

For cross-border correspondent relationships with third-country or higher-risk respondents, a bank must assess the respondent's reputation, supervision and AML controls, obtain senior management approval, and document both institutions' responsibilities. For payable-through accounts, it must be satisfied about the respondent's due diligence on customers with direct access (§ 40). Relationships with shell banks, and with institutions that knowingly let shell banks use their accounts, are prohibited and void (§ 18).

Basic payment services

Since 15 July 2025, credit institutions and Estonian branches of foreign credit institutions must provide basic payment services under the Law of Obligations Act (Credit Institutions Act § 88¹). Finantsinspektsioon may grant an exemption, and the decision must be made within four months. Banks that did not provide these services before 15 July 2025 are covered only if Finantsinspektsioon so orders (§ 141¹⁸). Breaches are punishable by fines of up to 400,000 euros for a legal person (§ 134²⁷).

Information sharing and banking secrecy

Banks may exchange information needed for due diligence regardless of banking secrecy (MLTFPA § 16(2)), and may share information on high-risk customers and suspected criminal transactions with each other (§ 51(5)). Records of these exchanges are kept for five years. Tipping off a customer about a report is prohibited (§ 51(1)).

Investment services and ICT resilience

A bank licence covers investment services to the extent authorised, and the same due diligence rules apply to securities accounts. Breaches of the EU Digital Operational Resilience Act (Regulation (EU) 2022/2554), including its third-party ICT risk rules, carry fines of up to 5 million euros or 10% of consolidated turnover (Credit Institutions Act § 134²⁶).

8 Risk indicators and red flags

Estonia's national risk assessment for 2020 to 2024 (approved 30 September 2025) rates the threat level for credit institutions as above average and their vulnerability as medium.

BANKING TYPOLOGIES FROM THE NATIONAL RISK ASSESSMENT

- **Correspondent services to foreign fintechs:** nested payment flows from respondents layering cross-border proceeds.
- **Virtual IBANs:** fraud proceeds routed through virtual account numbers that are not stand-alone accounts.
- **Account and credential handover:** nominees register companies, open accounts and pass ID cards and passwords to third parties.
- **Sanctions evasion:** evasion cases concentrated in credit institutions.
- **Companies with no Estonian link:** entities used for foreign predicate crime, sometimes via e-resident structures.
- **Identity fraud in remote onboarding:** deepfakes and processes that do not fully follow the guidelines.
- **Cash through payment services:** rising cash reports linked to cross-border transfer and currency exchange.

MLTFPA § 37 adds statutory higher-risk factors, including private banking, nominee shareholders and unusually complex ownership.

9 Enforcement and penalties

Finantsinspektsioon and the Financial Intelligence Unit are the out-of-court authorities for AML misdemeanours, with a three-year limitation period (MLTFPA § 97). Fines are set per offence, and the tier depends on whether the obliged entity is subject to Finantsinspektsioon supervision.

Breach (MLTFPA)	Supervised bank, legal person	Other obliged entities, legal person
-----------------	-------------------------------	--------------------------------------

Risk assessment and internal rules (§ 82)	Up to 5,000,000 euros, twice the benefit or harm, or 10% of consolidated turnover	Up to 1,000,000 euros or twice the benefit or harm
Customer identification (§ 84), beneficial owner (§ 85)	Up to 5,000,000 euros, twice the benefit or harm, or 10% of consolidated turnover	Up to 1,000,000 euros or twice the benefit or harm
Reporting to the Financial Intelligence Unit (§ 92)	Up to 5,000,000 euros, twice the benefit or harm, or 10% of consolidated turnover	Up to 1,000,000 euros or twice the benefit or harm
Anonymous accounts (§ 83), correspondent relationships (§ 91), payer data (§ 96)	Up to 5,000,000 euros, twice the benefit or harm, or 10% of consolidated turnover	

Separately, non-compliance levies enforcing an administrative order against a credit institution run up to 32,000 euros on the first occasion and 100,000 euros thereafter, capped at the higher of 5 million euros or 10% of annual turnover (§ 65(2)). On 19 October 2023 Finantsinspeksioon fined AS LHV Pank 900,000 euros and issued a precept over AML failings in correspondent banking, business relationship monitoring and data retention. In 2025 the Finantsinspeksioon board issued four precepts and fines totalling 416,800 euros across all supervised sectors.

10 Recent changes and what to watch

- **1 January 2028** Adopted, from 1 Jan 2028 AMLA begins direct supervision of 40 entities; large cross-border banking groups should expect EU-level AML oversight.
- **10 July 2027** Adopted, applies 10 Jul 2027 The EU Anti-Money Laundering Regulation (2024/1624) applies, together with a 10,000-euro EU cap on cash payments; onboarding procedures will need re-mapping to the new rulebook.
- **October 2026** Bill, not enacted A Law of Obligations Act amendment on financial fraud is before the Riigikogu; it would let banks refuse manipulated payments and share fraud data, including information covered by banking secrecy.
- **21 July 2026** In force Credit Institutions Act amendments transposing Directive (EU) 2024/1619 change third-country branch authorisation and management appointment notifications.
- **1 July 2026** In force The ban on anonymous accounts expressly covers crypto-asset accounts (MLTFPA § 25(2)).

- **1 March 2026** **In force** Savings and loan associations can no longer apply for Financial Intelligence Unit authorisation; existing authorisations lapse by 31 December 2028 at the latest.
- **15 July 2025** **In force** Credit institutions must provide basic payment services unless exempted by Finantsinspeksioon.

11 What this means for identity verification

Route each applicant at the start of onboarding by residence and expected monthly outgoing payments, because those two facts decide which remote method is lawful. EEA residents below 15,000 euros (individuals) or 25,000 euros (companies) can be verified with two independent sources. Non-EEA residents and higher-volume customers need a notified eIDAS scheme, a qualified trust service or a compliant video session. Residents of high-risk third countries need an eIDAS scheme or trust service only.

Treat expected volume as a re-verification trigger. A customer onboarded under the lower-tier method who later exceeds the monthly payment limits falls within § 31(1) and must be identified again with an approved method.

Design video and biometric tools around § 31(3¹). That means:

- capture images, video and audio in unambiguous quality;
- fail the session on any interruption;
- compare the live face with the document or database photo;
- store timestamped session data and the identity database query for five years after account closure.

Pair e-resident digital IDs with a second identity document, and expect the 2027 EU rulebook to change data fields and remote-identification evidence.

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 chip reading, face match and biometric liveness detection.
- Video KYC sessions that record images, video and audio for an audit trail, for customers who cannot use a notified electronic ID.
- KYB and beneficial owner verification for business accounts, with configurable risk-based workflows.
- AML screening against sanctions, PEP and adverse-media lists at onboarding and through ongoing monitoring.
- No-code workflow builder to route customers by residence and expected payment volume, with cloud, on-premises or hybrid deployment.

[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

- **Rahapesu ja terrorismi rahastamise tõkestamise seadus [Money Laundering and Terrorist Financing Prevention Act]**, consolidated text in force from 21.07.2026, §§ 2, 6, 9, 14, 16, 18–25, 31, 36–42, 47–49, 51, 64–65, 82–97, Riigi Teataja, riigiteataja.ee (Estonian text: riigiteataja.ee)
- **Krediidasutuste seadus [Credit Institutions Act]**, §§ 4, 12, 13–15, 21, 35, 88¹, 134²⁶, 134²⁷, 141¹⁸, Riigi Teataja, English translation riigiteataja.ee; Estonian text including amendments of RT I, 11.07.2026, 7 riigiteataja.ee
- **Rahvusvahelise sanktsiooni seadus [International Sanctions Act]**, §§ 19 and 30, Riigi Teataja, riigiteataja.ee

- Finantsinspektsioon, The operating licence for a credit institution, [fi.ee](#)
- Finantsinspektsioon advisory guidelines "Organisational approaches and preventive measures of credit and financial institutions for prevention of money laundering and terrorist financing", Resolution 11-7/172 of 26.11.2018 as amended by Resolution 11-7/58 of 8.04.2024, points 4.3.1.14 to 4.3.1.24, [fi.ee \(PDF\)](#)
- Finantsinspektsioon, "Finantsinspektsioon fined AS LHV Pank almost a million euros", 19.10.2023, [fi.ee](#)
- Finantsinspektsioon, "SEB got permission to merge in the Baltics", 22.05.2026, [fi.ee](#)
- Finantsinspektsioon Yearbook 2025, published June 2026, management board statistics and international cooperation, [fi.ee \(PDF\)](#)
- Eesti riikliku riskihinnangu aruanne rahapesu tõkestamise valdkonnas 2020–2024 [National money laundering risk assessment 2020–2024], Ministry of Finance, October 2025, sections 4.2–4.3, [fin.ee \(PDF\)](#)
- Ministry of Finance, Finantspettuste ennetamine: poliitika ja õigusaktid [Financial fraud prevention: policy and legislation], updated 08.10.2026, [fin.ee](#)
- Riigikogu, "Riigikogu passed legislative amendments increasing protection of deposits" (Guarantee Fund Act amendments, 119 SE), [riigikogu.ee](#)