



Identomat

COMPLIANCE GUIDE

Fintech & Digital Payments Compliance in Estonia

COUNTRY **Estonia**

INDUSTRY **Fintech & Digital Payments**

LAST UPDATED **21 October 2026**

KEY REGULATORS **Finantsinspektsioon (Financial Supervision and Resolution Authority) ·
Financial Intelligence Unit (Rahapesu Andmebüroo)**

Key takeaways

- A non-bank that offers payment accounts, transfers, card issuing or e-money in Estonia needs an authorisation from Finantsinspektsioon, the Financial Supervision and Resolution Authority, with share capital of between 20,000 and 350,000 euros depending on the service.
 - Payment institutions, e-money institutions and consumer lenders must verify every customer before any money moves, report suspicions to the Financial Intelligence Unit within two working days and keep onboarding records for five years.
 - Fully online onboarding is allowed. For customers living outside the European Economic Area (EEA), or sending more than 15,000 euros a month (25,000 euros for companies), the firm must use a notified electronic ID, a qualified trust service or a remote method that records images and video and fails if the connection drops.
 - An Estonian e-resident's digital ID card is not enough on its own for remote onboarding: a passport or other identity document must be checked at the same time.
 - Buy-now-pay-later products are expected to come under consumer credit rules once a bill now in Parliament is passed, and the EU Anti-Money Laundering Regulation replaces much of the national rulebook from 10 July 2027.
-

Estonia is open to digital payment, e-money and lending businesses, and its national electronic identity (ID card, Mobile-ID and Smart-ID) makes remote onboarding of residents straightforward. The market is not lightly supervised: after the large bank money laundering cases of the last decade, licences are granted slowly, the head office and a compliance officer must be physically in Estonia, and authorisations have been withdrawn for weak anti-money laundering controls.

The principal regulators are Finantsinspektsioon, which licenses and supervises payment, e-money and credit firms including their anti-money laundering compliance, and the Financial Intelligence Unit (Rahapesu Andmehüroo), which receives suspicious transaction reports.

The biggest obstacle for a new entrant is substance: a credible local management board, a compliance officer approved by the Financial Intelligence Unit, safeguarding of client funds and a remote onboarding process that meets the statutory safeguards for non-resident and high-volume customers.

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
Finantsinspektsioon (Financial Supervision and Resolution Authority)	Authorises and supervises payment institutions, e- money institutions, creditors and credit intermediaries; supervises their anti-money laundering and sanctions compliance	National	fi.ee
Rahapesu Andmebüroo (Financial Intelligence Unit)	Receives suspicious and cash transaction reports; approves compliance officers; supervises obliged entities not supervised by Finantsinspektsioon	National	fiu.ee
Eesti Pank (Bank of Estonia)	Payment and settlement systems; consulted by Finantsinspektsioon on authorisations where necessary	National	eestipank.ee
Andmekaitse Inspektsioon (Data Protection Inspectorate)	Personal and biometric data processed during onboarding	National	aki.ee
Centre of Registers and Information Systems	e-Business Register, including beneficial owner data	National	ariregister.rik.ee

European Banking
Authority and Authority
for Anti-Money
Laundering and
Countering the Financing
of Terrorism (AMLA)

EU guidelines, including on
remote customer
onboarding; AMLA takes over
EU-level anti-money
laundering coordination

Supranational eba.europa.eu

The Consumer Protection and Technical Regulatory Authority also has a consumer protection remit that can touch financial advertising; it is not covered in detail here.

2 Licensing and authorisation

The [Payment Institutions and E-money Institutions Act](#) (makseasutuste ja e-raha asutuste seadus, MERAS) requires a company to hold an authorisation from Finantsinspektsioon to operate as a payment institution or e-money institution (§ 14). The eight regulated payment services are listed in § 3, from account services and money remittance to payment initiation and account information.

Activity	Minimum share or initial capital	Legal form
Money remittance only	20,000 euros	Company
Payment initiation service	50,000 euros	Company
Account, transfer, card issuing or acquiring services (§ 3(1) clauses 1 to 5)	125,000 euros	Public limited company
Issuing e-money	350,000 euros	Public limited company if it also provides payment services under clauses 1 to 5; otherwise private or public limited company

Capital figures are from MERAS § 64; legal form rules from §§ 5 and 7 (version in force from 1 March 2026). Finantsinspektsioon decides within three months of receiving a complete application and in any case within six months of filing (§ 18). It may refuse an applicant that appears to have chosen Estonia to avoid stricter rules in the country where it mainly operates (§ 19). The registered office and head office must be in Estonia (§ 46) and the management board must have at least two members meeting fitness and propriety requirements (§ 47).

Small-scale exemptions

Finantsinspektsioon can exempt from most prudential chapters a money remitter whose payment transactions average no more than one million euros a month, a limited provider of the clause 1 to 5 services averaging no more than three million euros a month and earning less than half its income from payments, and an e-money issuer whose average outstanding e-money does not exceed 500,000 euros (§§ 11 and 12). Exempt firms cannot open branches or provide services in other EEA states.

Passporting, agents and lending

An Estonian institution notifies Finantsinspektsioon before opening a branch or providing services in another EEA state (§ 29). Paying agents must be notified with a description of their anti-money laundering controls (§ 59) and their managers must meet reputation requirements (§ 61). Consumer lending and credit intermediation require a separate Finantsinspektsioon licence under the Creditors and Credit Intermediaries Act; Finantsinspektsioon regularly withdraws these licences and fines lenders for breaches of responsible lending rules.

3

AML, KYC and customer due diligence

Under the [Money Laundering and Terrorist Financing Prevention Act](#) (rahapesu ja terrorismi rahastamise tõkestamise seadus, RahaPTS), payment service providers (except pure payment initiation and account information providers), e-money institutions, creditors and credit intermediaries, and crowdfunding service providers are financial institutions and therefore obliged entities (§ 6(2)). Finantsinspektsioon enforces the Act for the firms it supervises (§ 64).

When CDD applies

On establishing a business relationship; for occasional transactions of 15,000 euros or more; for occasional money transfers above 1,000 euros; and always on suspicion (§§ 19 and 25). Verification must be completed before the relationship or transaction (§ 19(5)).

What CDD covers

Identity and verification from a reliable independent source, representatives, beneficial owners, purpose of the relationship, politically exposed person (PEP) status and ongoing monitoring (§ 20).

No anonymity

Financial institutions may not offer services usable without identification, except limited-use accounts on which nothing can be done until due diligence is complete (§§ 25 and 27). Payment service providers may not execute a customer's instructions if they cannot meet these duties (§ 42(3)).

Enhanced due diligence

Mandatory for PEPs, high-risk third countries, doubts about documents and certain sanctioned or high-corruption connections (§ 36), with senior management approval and source of funds and wealth checks (§§ 39 and 41).

Beneficial ownership

A beneficial owner is the natural person with ultimate control, with a fallback test of more than 25 per cent shareholding (§ 9). For customers whose beneficial owners must be registered in an EU state, the firm must obtain the registry extract (§ 20(2¹)) and report discrepancies with the Estonian e-Business Register (§ 20(2⁴)). Business relationships with companies whose capital is more than 10 per cent bearer shares are prohibited (§ 42(2)).

Reporting and retention

Suspensions go to the Financial Intelligence Unit without delay and no later than two working days after they arise, including for refused or abandoned relationships (§ 49(1) and (2)). Obligated entities other than credit institutions must also report every cash transaction above 32,000 euros within two working days (§ 49(3)). Reports are filed through the unit's online form or the X-road service (§ 50). Tipping off is prohibited (§ 51). Identification documents and records are kept for at least five years after the relationship ends, extendable by a supervisory compliance notice for up to five more years (§ 47). A management board member must be responsible for compliance, and the compliance officer must work permanently in Estonia and be approved in coordination with the Financial Intelligence Unit (§ 17).

4

Identity verification and onboarding

A natural person is identified from an Estonian identity document, a valid foreign travel document, a compliant driving licence or, for children under seven, a birth certificate (RahaPTS § 21(3)). The firm records name, personal identification code (or date of birth and residence), any authority to represent and contact details (§ 21(1)). Where the original document is not seen, identity may be verified from a certified copy or from other reliable

independent information, including electronic identification and trust services, using at least two different sources (§ 21(4)). Companies are identified from the commercial register, which the firm may consult directly instead of asking for documents (§ 22).

Firms may rely on another obliged entity's due diligence or outsource it under a written contract, but they remain responsible, must notify Finantsinspeksioon of outsourcing in advance and may not rely on or outsource to anyone in a high-risk third country (§ 24).

Finantsinspeksioon's advisory guideline on anti-money laundering (amended 8 April 2024) explains how it expects the two-source method to work: one source is always a colour copy of a photo identity document, the same data from an official database, or, for lower-risk customers, a strong authentication with a digital ID; for medium or higher risk the customer sends a freshly taken photograph that the firm confirms is recent. The guideline also applies, with stated exceptions, the European Banking Authority's guidelines on remote customer onboarding.

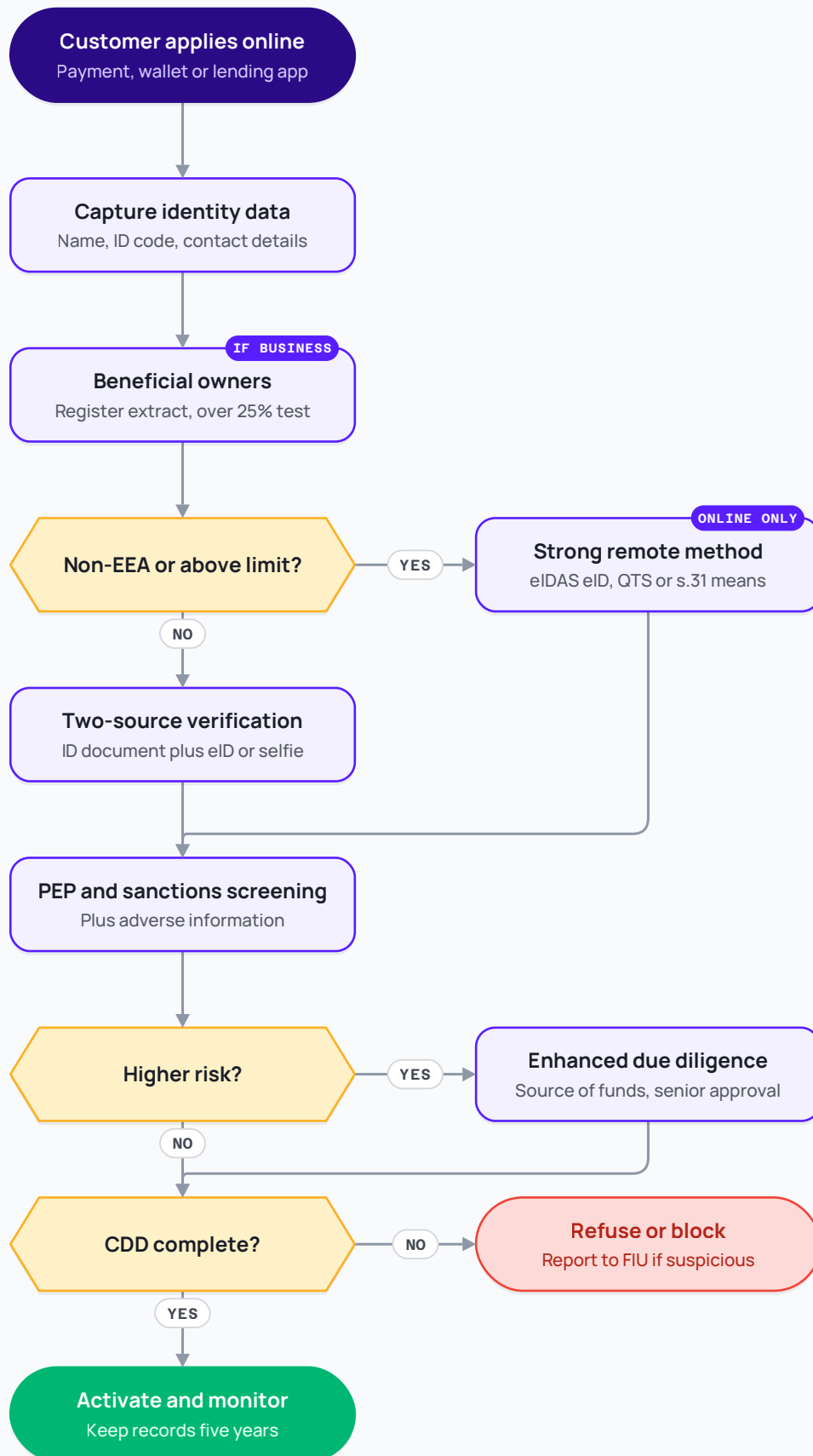


Figure 1. Remote onboarding of a payment or e-money customer in Estonia.

Bottom line: remote onboarding is fully permitted, but once a customer lives outside the EEA, comes from a high-risk third country or sends more than 15,000 euros a month (25,000 euros for a legal person), RahaPTS § 31 dictates which remote methods may be used.

Requirement	In person	Online / remote	Difference
Accepted identity documents	§ 21(3) list	Same list, seen remotely or via official databases	Same
Internal rules before onboarding	General CDD procedures	Additional rules ensuring secure remote identification (§ 14(1 ¹))	Differs
Non-EEA residents or above 15,000 / 25,000 euros a month	Face-to-face check of the document	Notified eID (substantial or high), qualified trust service or a § 31(3 ¹) method	Differs
Residents of high-risk third countries	Face-to-face with enhanced due diligence	Only a notified eID or qualified trust service	Differs
E-resident digital ID	Not an identity document on its own for this purpose	Must be combined with another § 21(3) document	Differs
Risk rating	No channel factor	Remote onboarding without § 31 safeguards is a higher-risk factor (§ 37(3))	Differs
Evidence kept	Copies of documents for five years	Digital ID data, database queries and time-stamped identification data for five years (§ 47(6)); document copies not needed if e-identification was used	Differs
Suspicion reporting and screening	Two working days to the FIU	Two working days to the FIU	Same

Which remote method, when

Section 31(1) requires credit and financial institutions to use a scheme listed in § 31(3) or a compliant alternative whenever due diligence is not done in person and the customer resides outside the EEA or monthly outgoing payments exceed the thresholds. The listed schemes are an electronic identification scheme notified under Article 9 of Regulation (EU) No 910/2014 (eIDAS) at assurance level substantial or high, and a qualified trust service. Where neither can be used, the alternative must keep data accurate and current, store images, video, audio and data securely at a quality that identifies the person unambiguously, and fail if the connection breaks or another technical defect occurs (§ 31(3¹)). For residents of high-risk third countries the alternative is not available (§ 31(1¹)). Institutions may check data against the identity documents database (§ 31(5)).

Below the thresholds

For EEA-resident customers below the monthly limits, § 21(4) applies: verification from at least two reliable independent sources, which in practice can be a document image combined with a national digital ID login, a selfie or a database check.

E-residents

When an e-resident's digital identity card is used for remote identification, another identity document listed in § 21(3) must be used at the same time (§ 31(4)). A firm may terminate the relationship without notice if that card is refused, suspended or invalidated on certain statutory grounds (§ 43(2)).

6 Data protection and biometrics

The General Data Protection Regulation (Regulation (EU) 2016/679) applies directly and is supervised by the Data Protection Inspectorate. RahaPTS § 48 treats processing for anti-money laundering as a matter of public interest, forbids reusing that data for other purposes such as marketing and requires customers to be told how their data is processed before onboarding. Certain data subject rights (restriction, portability, objection) may be limited where honouring them would undermine due diligence.

Face matching against an identity document photo is biometric processing of special category data. The Inspectorate's published explanations state that biometric data cannot be processed on the basis of contract performance and needs an exception under GDPR Article 9(2), such as explicit consent or a legal basis. Firms should document which basis they rely on for liveness and face matching, and run a data protection impact assessment.

Retention is fixed by RahaPTS § 47: five years after the relationship ends for identification data, then deletion, unless a compliance notice extends retention by up to five years.

7 Sector-specific obligations

Safeguarding and internal control

MERAS §§ 78 to 80 require client funds to be safeguarded; breaches carry fines of up to 5,000,000 euros or 10 per cent of consolidated turnover for a legal person (§ 114). Internal rules must cover, among other things, ICT risk under the Digital Operational Resilience Act and the handling of sensitive payment data (§ 50).

Prepaid instruments and e-money

A payment service provider may accept a payment made with an anonymous prepaid card only if the card is not reloadable, holds no more than 150 euros, is used only for goods and services, cannot be funded with anonymous e-money, is monitored by its issuer and the payment does not exceed 50 euros (RahaPTS § 25(2¹)).

Consumer credit and buy-now-pay-later

Creditors must assess creditworthiness and keep compliant internal rules under the Creditors and Credit Intermediaries Act. Finantsinspektsioon fined Svea Finance AS a total of 200,000 euros in June 2025 and Bondora AS 200,000 euros in April 2025 for responsible lending failures.

EEA providers operating through agents

An e-money institution or payment service provider headquartered in another EU state that operates in Estonia other than through a branch can be ordered to appoint a central contact point in Estonia to ensure compliance with RahaPTS (§ 15(6)).

Risk indicators and red flags

PAYMENT AND E-MONEY RED FLAGS (FINANCIAL INTELLIGENCE UNIT AND FINANTSINSPEKTSIOON)

- **Remote control:** the applicant appears to act for someone else or is directed or watched by a third party during onboarding.
- **Document tampering:** formats inconsistent with the issuing country, identical or pasted signatures.
- **Name mismatch:** an incoming payment above 1,000 euros where the payee name clearly differs from the account holder.
- **Transit account:** large inflows from abroad passed straight on to foreign accounts with implausible payment descriptions.
- **Account farming:** an unreasonable number of accounts or virtual card accounts, or sudden unexplained limit increases.
- **Funnel pattern:** many unrelated payers into one account followed by rapid withdrawal or onward transfer.
- **Card misuse:** a card used by someone unrelated to its holder.
- **Virtual IBANs and cross-border services:** named by Finantsinspektsioon as the main sector risks alongside sanctions evasion.

Enforcement and penalties

RahaPTS sets misdemeanour fines per breach. For an obliged entity supervised by Finantsinspektsioon, failing to identify and verify a customer, or breaching risk assessment and internal control rules, carries a fine of up to 5,000,000 euros or twice the benefit gained or harm prevented, rising for a legal person to 10 per cent of consolidated turnover (§§ 82 and 84). Breaches of the EU transfer of funds rules carry the same maximum (§ 96). Non-compliance levies to enforce an order can reach 32,000 euros for a first and 100,000 euros for each subsequent occasion for a legal person, capped at the higher of 5,000,000 euros or 10 per cent of annual turnover (§ 65(2)). MERAS has parallel fines and levies (§§ 106, 109 and 114).

Finantsinspektsioon withdrew the payment institution authorisation of Ühisarveldused AS on 18 August 2025 for material breaches of MERAS and anti-money laundering requirements; the Tallinn Administrative Court lifted interim relief in May 2026, so the

withdrawal is effective while the main appeal continues. In September 2026 it ordered Wallester AS to remedy weaknesses in governance, client asset safeguarding and anti-money laundering controls by 31 December 2026.

10 Recent changes and what to watch

- **16 September 2026** **In force** : Finantsinspektsioon order against Wallester AS signals continued on-site scrutiny of payment institutions' AML staffing and safeguarding.
- **1 July 2026** **In force** : RahaPTS amendments took effect bringing crowdfunding service providers into the financial institution definition and barring payment providers from executing instructions where § 25 duties cannot be met.
- **June 2026** **Bill, not enacted** : Bill 947 SE, transposing the new EU Consumer Credit Directive, would bring buy-now-pay-later and interest-free credit under creditworthiness and pre-contract information rules.
- **June 2026** **Draft act in preparation** : the Ministry of Finance is preparing a new anti-money laundering act to transpose the Sixth Anti-Money Laundering Directive.
- **9 March 2026** **In force** : Finantsinspektsioon updated its advisory guideline on applying international financial sanctions.
- **18 July 2025** **In force** : MERAS amendments allow payment and e-money institutions to participate in settlement systems for instant payments.
- **10 July 2027** **Adopted, applies 10 Jul 2027** : the EU Anti-Money Laundering Regulation (EU) 2024/1624 becomes directly applicable and will replace much of RahaPTS.

11 What this means for identity verification

Build two onboarding paths. Estonian and other EEA residents with modest volumes can be verified with two independent sources, typically a national digital ID authentication plus a document or database check, with a fresh selfie for anyone not rated lower risk. Non-EEA residents and customers expected to exceed 15,000 euros a month (25,000 euros for companies) need a notified eID at substantial or high assurance, a qualified trust service, or a document, face and liveness flow that records images and video at identifying quality and aborts on any interruption. Residents of high-risk third countries can only be onboarded remotely through a notified eID or qualified trust service.

Treat e-resident cards as a second factor, not a standalone document. Monitor outgoing payment volumes after onboarding, because crossing the monthly threshold triggers the

stronger method. Store digital identification evidence, database query logs and timestamps for five years after the relationship ends, then delete them. Collect business customers' beneficial owner register extracts and report discrepancies. Plan now for the EU Anti-Money Laundering Regulation from July 2027.

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 NFC chip reading, face match and biometric liveness, with recordings and timestamps kept for the five-year retention period.
- Video KYC for customers outside the EEA or above the monthly payment thresholds where a notified eID cannot be used.
- AML screening against sanctions, PEP and adverse-media lists at onboarding and through ongoing monitoring.
- KYB and beneficial owner verification for business customers, including register extracts.
- No-code workflows that route each customer to the verification path the rules require.

[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], RT I, 17.11.2017, 2, consolidated version in force from 21.07.2026, §§ 6, 9, 14,

15, 17, 19 to 25, 27, 31, 36 to 43, 47 to 51, 64, 65, 82, 84, 96, Riigi Teataja, [English translation](#); [Estonian text](#)

- Makseasutuste ja e-raha asutuste seadus [Payment Institutions and E-money Institutions Act], consolidated version in force from 01.03.2026, §§ 3, 5, 7, 11, 12, 14, 18, 19, 29, 46, 47, 50, 59, 61, 64, 106, 109, 114, Riigi Teataja, [riigiteataja.ee](#)
- Makseasutuste ja e-raha asutuste seaduse ning makse- ja arveldussüsteemide seaduse muutmise seadus [amending act on settlement system access], Riigi Teataja news, 08.07.2025, [riigiteataja.ee](#)
- Finantsinspektsiooni soovituslik juhend „Krediidi- ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks“ [Advisory guideline on AML organisation and preventive measures], amended 08.04.2024, section 4.3.1, [fi.ee](#)
- Finantsinspektsiooni soovituslik juhend „Rahvusvahelise finantssanktsiooni kohaldamine krediidi- ja finantseerimisasutustes“ [Advisory guideline on applying international financial sanctions], amended 09.03.2026, [fi.ee](#)
- Rahapesu Andmebüroo, Juhend kahtlaste tehingute tunnuste kohta [Guide on indicators of suspicious transactions], last amended 22.07.2024, [fiu.ee](#)
- Finantsinspektsioon, Finantsinspektsioon teavitas turgu rahapesu ja terrorismi rahastamise riskidest, 21.03.2025, [fi.ee](#)
- Finantsinspektsioon, Tallinna Halduskohus tühistas Ühisarveldused AS-i esialgse õiguskaitse, 19.05.2026, [fi.ee](#)
- Finantsinspektsioon, Finantsinspektsioon tegi Wallester AS-ile ettekirjutuse, 16.09.2026, [fi.ee](#)
- Finantsinspektsioon, Finantsinspektsioon trahvis Svea Finance AS-i kokku 200 000 euroga, 11.06.2025, [fi.ee](#)
- Finantsinspektsioon, Finantsinspektsioon trahvis Bondora AS-i 200 000 euroga, 30.04.2025, [fi.ee](#)
- Finantsinspektsioon, Finantsinspektsioon korraldas turuosalistele rahapesu tõkestamise ja sanktsioonide teemalise infopäeva, 19.06.2026, [fi.ee](#)
- Riigikogu, Bill 947 SE, Võlaõigusseaduse ja teiste seaduste muutmise seadus (uue tarbijakrediidi direktiivi ülevõtmine), initiated 15.06.2026, [riigikogu.ee](#)
- Andmekaitse Inspektsioon, Vastus selgitustaotlusele (biometric data), 04.02.2026, [aki.ee](#)
- Regulation (EU) 2024/1624 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Article 90, EUR-Lex, [eur-lex.europa.eu](#)