



Identomat

COMPLIANCE GUIDE

Insurance & Insurtech Compliance in Estonia

COUNTRY **Estonia**

INDUSTRY **Insurance & Insurtech**

LAST UPDATED **21 October 2026**

KEY REGULATORS **Financial Supervision and Resolution Authority (Finantsinspektsioon) ·
Financial Intelligence Unit · Data Protection Inspectorate**

Key takeaways

- Life insurers and insurance brokers that sell life insurance are covered by Estonia's anti-money laundering law and must identify and verify every customer before the policy is issued. Non-life insurance (motor, home, travel, health) is outside that law, although sanctions checks still apply to everyone.
- Any insurer based in Estonia needs a licence from Finantsinspektsioon, the financial supervisor; brokers must be entered in its list of intermediaries, and agents are listed by the insurer they work for. Insurers licensed elsewhere in the European Economic Area (EEA) can sell cross-border but must follow Estonian consumer rules, including documents in Estonian.
- Selling life cover fully online is allowed. If the customer lives outside the EEA, or monthly outgoing payments exceed 15,000 euros (individuals) or 25,000 euros (companies), the insurer must use a government-recognised electronic ID, a qualified trust service, or a remote method that records clear images and video and fails safely if the connection drops.
- A life insurer must name the policy beneficiary as soon as they are known and verify that person's identity before paying out, so identity checks happen twice: at sale and at claim.
- The EU Anti-Money Laundering Regulation applies directly from 10 July 2027 and will replace much of today's Estonian rulebook; selfies and face matching count as biometric data, which the Data Protection Inspectorate treats as needing consent or a basis in law.

Estonia is open to digital insurance. Insurers established in Estonia operate under a Finantsinspektsioon licence, EEA insurers can enter through cross-border provision, and online distribution is common. The customer due diligence burden falls on the life side of the business; non-life products carry conduct, data protection and sanctions duties but no statutory know-your-customer obligation.

The principal authorities are the Financial Supervision and Resolution Authority (Finantsinspektsioon), which licenses and supervises insurers and intermediaries, the Financial Intelligence Unit, which receives suspicious transaction and sanctions reports, and the Data Protection Inspectorate.

The biggest obstacle for a new life insurer is building a remote onboarding flow that meets the Money Laundering and Terrorist Financing Prevention Act's remote identification rules for non-EEA and higher-value customers, while also handling beneficiaries who are identified only at payout.

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
Financial Supervision and Resolution Authority (Finantsinspektsioon)	Insurer licensing, intermediary listing, conduct and prudential supervision, AML supervision of licensed insurers and brokers, ICT incident reporting under DORA	National	fi.ee
Financial Intelligence Unit (Rahapesu Andmebüroo)	Receives suspicious, unusual, cash and sanctions reports; issues reporting guidelines	National	fiu.ee
Data Protection Inspectorate (Andmekaitse Inspektsioon)	GDPR supervision, including biometric data used in onboarding	National	aki.ee
Consumer Protection and Technical Regulatory Authority	Handles consumer complaints about insurance alongside Finantsinspektsioon	National	ttja.ee
European Insurance and Occupational Pensions Authority (EIOPA)	EU insurance rulebook and supervisory convergence	Supranational	eiopa.europa.eu

The EU Anti-Money Laundering Authority (AMLA) drafts the technical standards that will accompany the EU Anti-Money Laundering Regulation.

2

Licensing and authorisation

Insurers

A company needs an operating licence to carry on insurance activities, and companies established in Estonia receive it from Finantsinspektsioon under the Insurance Activities Act (kindlustustegevuse seadus). The application, filed through the Finantsinspektsioon application portal since 18 March 2026, includes statutes, proof of paid-in capital and own funds, an operating plan, management and supervisory board details, shareholder and qualifying-holding data, the organisational structure and internal rules. The application fee is 1,000 euros. Finantsinspektsioon decides within three months of receiving a complete file and no later than six months after the application was filed.

An insurer from another EU member state may provide cross-border services in Estonia but must observe the Insurance Activities Act, the Motor Insurance Act, the Law of Obligations Act and the Consumer Protection Act. Policy conditions and notices for Estonian consumers must be understandable and in Estonian, and the insurer must apply the Money Laundering and Terrorist Financing Prevention Act and Finantsinspektsioon's guidelines.

Intermediaries

Estonian law distinguishes brokers, who represent the policyholder, from agents, who represent the insurer. A broker applies to Finantsinspektsioon to be entered in the list of intermediaries and must supply a professional liability insurance contract or guarantee, internal service rules and evidence that the board member responsible for distribution has the required experience and knowledge. Agents are entered in the list by the insurer immediately after the agency contract is signed; the insurer answers for the accuracy of those entries, and an agent cannot represent a second insurer for the same class of insurance.

The Insurance Activities Act prohibits an intermediary from transferring the marketing of insurance to someone else. For platforms that embed insurance in another product, this means the party presenting the offer must itself be the listed insurer, broker or agent.

Who is in scope

The Money Laundering and Terrorist Financing Prevention Act (rahapesu ja terrorismi rahastamise tõkestamise seadus) applies to financial institutions, which include an insurance undertaking to the extent it provides life insurance services, except services relating to mandatory funded pension contracts, and an insurance broker to the extent it markets life insurance or provides other investment-related services. Non-life insurance is not listed, so a non-life insurer or broker has no statutory due diligence obligation under the Act. Insurance agents are not listed separately; an insurer that relies on agents or outsources due diligence remains responsible for compliance.

When due diligence applies

Due diligence applies when a business relationship is established, on occasional transactions of at least 15,000 euros, when earlier data is doubtful, and on any suspicion regardless of thresholds. Identification, beneficial ownership, purpose of the relationship and politically exposed person checks must be completed before the relationship starts. A credit or financial institution may not offer services that can be used without identifying the customer and verifying the information.

Customer data

Name, personal identification code (or date of birth and residence), representation rights and contact details, verified against a credible and independent source.

Beneficial ownership

For corporate policyholders, the natural person with ultimate control or more than 25 per cent ownership, plus a registry extract where the EU state keeps a register. Differences from the Estonian register must be notified to the registrar.

Beneficiaries

Life policy beneficiaries are identified as soon as named or known; a class of beneficiaries must be described well enough to identify them at payout, when identity is verified. Assignees are identified at assignment.

Monitoring

Transactions are checked against the customer's profile, documents kept current, and the source of funds identified, with closer attention to complex or unusual patterns.

Simplified and enhanced due diligence

The Act lists life insurance contracts with a small premium, and pension insurance with no early surrender option that cannot be used as collateral, as lower-risk factors that may support simplified measures, provided monitoring stays adequate. Enhanced measures are mandatory for politically exposed persons, high-risk third countries, doubts about data or documents, and for remote relationships connected to high-corruption or sanctioned jurisdictions where an eIDAS scheme or qualified trust service is not used. A relationship started without meeting the customer and without the remote identification safeguards is listed as a higher-risk delivery channel.

Reporting and governance

Covered insurers and brokers need a documented risk assessment and rules of procedure, including for the risks of new sales channels and technologies. They appoint a management board member in charge and a compliance officer who works permanently in Estonia and whose appointment is coordinated with the Financial Intelligence Unit.

Under the Financial Intelligence Unit's guidelines, a suspicion that enhanced measures do not dispel requires a suspicious transaction report, and the insurer must not establish the relationship or must postpone the transaction; unusual but explained activity is reported without stopping the relationship. A cash transaction above 32,000 euros, in one payment or several related payments, must be reported. Sanctions doubts are reported to the same unit, and that duty applies to every person, so it reaches non-life insurers too.

4 Identity verification and onboarding

A natural person is identified on one of the documents listed in the Identity Documents Act, a valid foreign travel document, a qualifying driving licence, or a birth certificate for a child under seven. Where the original is not available, the insurer may rely on a notarised or officially certified copy or on other credible and independent information, including electronic identification and trust services, using at least two different sources.

Remote identification

When the customer is not met in person, section 31 of the Act sets the rules. Before relying on it, the insurer must adopt rules of procedure that secure identification and manage the risks of not meeting the person. The permitted tools are an electronic identification scheme notified under eIDAS (Regulation (EU) No 910/2014) at assurance level substantial or high, or a qualified trust service. Where neither can be used, the method must keep data correct and current, capture images, video, audio and data clearly enough to identify the

person unambiguously, and treat a dropped connection or technical fault as a failed identification.

Insurers may also check identity data against the Estonian database of identity documents. Finantsinspektsioon has adopted the European Banking Authority's Guidelines on the use of remote customer onboarding solutions as advisory guidelines, in effect since 29 May 2023, on a comply-or-explain basis.

Reliance and outsourcing

An insurer may rely on due diligence carried out by another firm subject to equivalent EU standards, or outsource identity checks under a written contract that preserves supervisory access and data retention. Finantsinspektsioon must be informed in advance of an outsourcing contract and its scope, outsourcing to a provider established in a high-risk third country is prohibited, and the insurer remains liable.

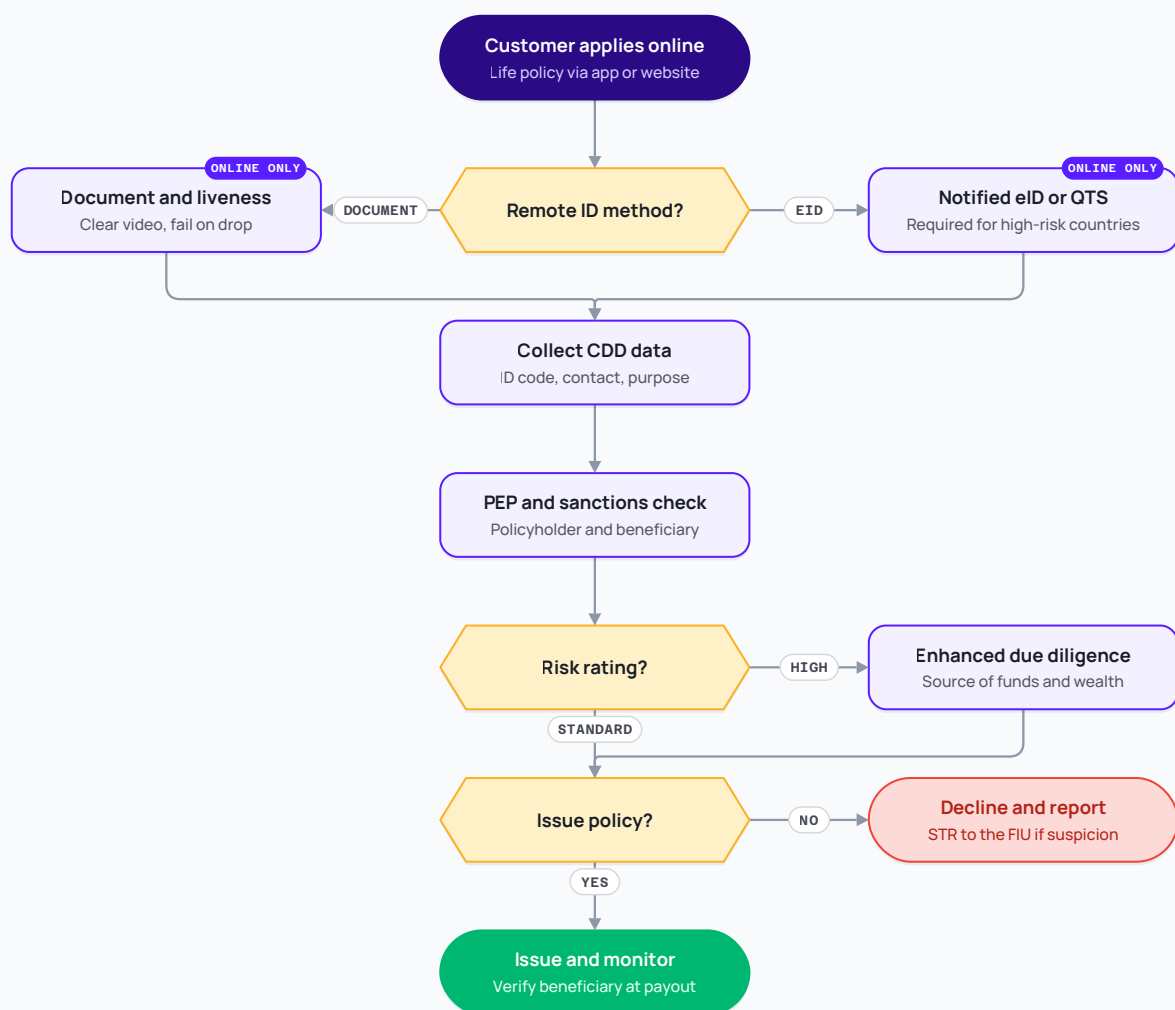


Figure 1. Online onboarding for a life insurance policy in Estonia.

Bottom line: the due diligence duties are the same online and in person, but remote life insurance onboarding must use specified identification tools once the customer is outside the EEA or payments exceed set monthly amounts, and remote sales without those safeguards count as higher risk.

Requirement	In person / agent-led	Online / remote	Difference
Products in AML scope	Life insurance and life-insurance broking	Same products	Same
Timing of due diligence	Before the policy is issued	Before the policy is issued	Same
Identity evidence	Original identity document	eID, trust service, or two independent sources	Differs
Non-EEA residents	Standard document check	eIDAS scheme, qualified trust service or safeguarded remote method required	Differs
Higher-value customers	Standard document check	Safeguarded method above 15,000 euros (individuals) or 25,000 euros (companies) a month in outgoing payments	Differs
High-risk third countries	Enhanced due diligence	Enhanced due diligence and only an eIDAS scheme or qualified trust service	Differs
Risk classification	Not a channel risk factor	Higher-risk factor if remote safeguards are not applied	Differs
E-residents	Identity document	E-resident digital ID plus a second listed document	Differs
Beneficiary at payout	Verified at payment	Verified at payment	Same

When the remote safeguards are mandatory

Section 31 makes the safeguarded methods compulsory for a credit or financial institution identifying someone remotely where the customer resides outside the EEA, or where outgoing payments under the contract exceed 15,000 euros a month for an individual or 25,000 euros for a legal person. For residents of a high-risk third country, only an eIDAS-notified scheme or a qualified trust service will do. A domestic policy below the payment thresholds can be onboarded with other reliable remote methods, but written rules of procedure for remote identification are still required.

E-residents

Where an e-resident's digital identity document is used remotely, another document from the statutory list must be used at the same time. An e-resident card alone does not complete remote identification.

Location and device signals

The Financial Intelligence Unit lists an IP address pointing to a higher terrorist-financing-risk country, unusual VPN use, or frequently changing location data as a risk indicator. For digital insurers, device and network data collected at onboarding and login therefore feed the reporting process.

6 Data protection and biometrics

The General Data Protection Regulation (GDPR) applies directly and is supervised in Estonia by the Data Protection Inspectorate. The AML Act ties the two regimes together: insurers must be able to explain their due diligence measures to the data protection authority, and must consider its guidelines when designing customer risk models and remote identification procedures.

The Inspectorate's published position (February 2026) is that using a technical tool to compare physiological features such as a face image to identify a person brings the processing under Article 9 GDPR, that biometric processing cannot rest on the performance of a contract, and that it requires either valid consent or a basis in law, plus a data protection impact assessment under Article 35 even where consent is the basis. For remote onboarding outside the eIDAS route, an insurer should document whether its face matching relies on the AML Act's identification duty or on explicit consent, and offer a non-biometric alternative such as eID where consent is used.

Payout and assignment controls

Life insurance is the one product where identity is checked twice by law. The beneficiary's identity is verified at the time of payment, and an assignee is identified when the policy is assigned. Claims and surrender systems therefore need an identity verification step, not only the sales funnel.

Agent and distribution oversight

The insurer maintains the list entries for its agents and answers for them, and must remove an agent when the contract ends. Finantsinspektsioon may delete an agent or broker that breaches the Insurance Activities Act or puts clients' interests at risk. Where agents collect identity data, the insurer's outsourcing contract and advance notice to the supervisor under the AML Act apply.

Digital operational resilience

The Digital Operational Resilience Act (DORA, Regulation (EU) 2022/2554) has applied since 17 January 2025 to insurers and insurance intermediaries. It covers ICT risk management, incident reporting to Finantsinspektsioon, testing and the register of third-party ICT providers, which includes cloud identity verification vendors. From 1 November 2026 major ICT incident reports go through the Eesti Pank and Finantsinspektsioon data collection portal.

LIFE INSURANCE INDICATORS FROM THE FINANCIAL INTELLIGENCE UNIT

- **Early-exit interest:** unusual interest at signing in cancellation or the payout if a claim arises soon after.
- **Short-term life cover:** a life policy for less than three years combined with other suspicious features.
- **Disproportionate premiums:** premiums out of line with the insured risk and contract terms.
- **Beneficiary swap:** beneficiary replaced mid-term by someone with no family link to the policyholder.
- **Indifferent surrender:** early termination without concern for penalties or costs.
- **Cash purchase:** financial products bought with more than 10,000 euros in cash without a credible explanation.
- **Third-party documents:** identification supplied by an intermediary with no clear reason to be involved.
- **Location masking:** IP address in a higher-risk country, unusual VPN use or rapidly changing location data.

Finantsinspektsioon supervises licensed insurers and brokers, including their compliance with the AML Act, and can issue precepts, impose misdemeanour fines, and delete intermediaries from the list. Fines are imposed per misdemeanour under the relevant act. For breaches of the Insurance Activities Act by a legal person, Finantsinspektsioon states that the maximum fine is now up to 400,000 euros, against 32,000 euros under the earlier rules.

The most relevant recent case involves an online broker. In 2024 Finantsinspektsioon fined IIZI Kindlustusmaakler AS 24,000 euros for transferring the marketing of insurance and failing to act in clients' interests, and Harju County Court upheld the decision. On 12 June 2025 the Supreme Court annulled the decision and ended the proceedings because the limitation period had expired, without ruling on how the outsourcing prohibition should be read, so the prohibition stands but its boundaries for embedded and platform distribution remain untested in court.

Recent changes and what to watch

- **10 July 2027:** EU Anti-Money Laundering Regulation (EU) 2024/1624
Adopted, applies from 10 Jul 2027. Life insurers and intermediaries will apply directly applicable EU due diligence rules, with AMLA technical standards, and much of the Estonian Act's detail will be replaced.
- **1 November 2026:** DORA incident reporting moves to the Eesti Pank and Finantsinspektsioon data collection portal Effective 1 Nov 2026. Insurers should update incident runbooks and access rights.
- **21 July 2026:** AML Act amendment (RT I, 11.07.2026, 2) In force. Revises the lower-risk factor for listed-company customers; check simplified due diligence rules for corporate policyholders.
- **18 March 2026:** Finantsinspektsioon application portal In force. Insurer licence and broker listing applications are filed through the portal.
- **12 June 2025:** Supreme Court ends IIZI misdemeanour case on limitation grounds In force. The ban on transferring insurance marketing remains, with no court guidance on platform models.
- **1 July 2024:** Remote identification rules in section 31 of the AML Act rewritten In force. eIDAS schemes, qualified trust services and safeguarded remote methods replaced the earlier approach.

What this means for identity verification

Separate the flows by product. Life and investment-linked products need full due diligence before issue; non-life products need sanctions screening and conduct controls but not statutory know-your-customer checks.

Offer Estonian and other eIDAS-notified electronic IDs at assurance level substantial or high as the primary remote route, because they satisfy section 31 for every customer group, including high-risk third country residents. Keep document capture with liveness as a fallback for customers without eID, configured to record clear images and video and to fail closed on a dropped session.

Capture the personal identification code and contact details, test residence against the EEA boundary, and track monthly outgoing payments so a customer who crosses 15,000 or 25,000 euros is moved to a section 31 method. Require a second document for e-residents.

Treat payout and assignment as verification events. Store beneficiary details at policy level and verify the beneficiary's identity before payment.

Document the legal basis for face matching, complete an impact assessment, and notify Finantsinspektsioon before outsourcing identity checks.

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 KYC onboarding for life policies, with ID document capture and verification (including NFC), face match and biometric liveness.
- Video KYC sessions that record clear images and video for remote identification records.
- AML screening against sanctions, PEP and adverse-media lists for policyholders and beneficiaries, with ongoing monitoring.
- KYB and beneficial owner verification for corporate policyholders.
- No-code workflow builder to add identity re-verification at payout and assignment, 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], RT I, 17.11.2017, 2, consolidated English translation of the version in force from 21.07.2026, §§ 2, 6, 9, 13, 14, 17, 19 to 26, 31, 35 to 38, Riigi Teataja, riigiteataja.ee; Estonian text, riigiteataja.ee

- Juhend kahtlaste tehingute tunnuste kohta [Guidelines on the characteristics of suspicious transactions], Financial Intelligence Unit, approved 19.07.2022, last amended 22.07.2024, points 12 to 23 and UTR indicator 1.4, fiu.ee
- Explanatory guidelines on reporting to the Financial Intelligence Unit, Financial Intelligence Unit, clauses 3 to 6 and 23, fiu.ee
- The operating licence for an insurance company, Finantsinspektsioon, page last edited 18.03.2026, fi.ee
- Registration of insurance intermediaries, Finantsinspektsioon, page last edited 18.03.2026, fi.ee
- Money laundering prevention and implementation of financial sanctions guidelines and legislation, Finantsinspektsioon, page last edited 01.04.2026, fi.ee
- Suunised klientide kaugtuvastamise lahenduste kohta [Guidelines on the use of remote customer onboarding solutions, EBA/GL/2022/15], adopted as Finantsinspektsioon advisory guidelines, effective 29.05.2023, fi.ee
- Misdemeanour proceedings against IIZI Kindlustusmaakler AS terminated by the Supreme Court due to expiry of the limitation period, Finantsinspektsioon news, 25.03.2025, updated 25.08.2026, fi.ee
- DORA määrusest ja nõuetest Eesti finantssektoris tegutsevatele ettevõtetele [DORA and its requirements for Estonian financial sector firms], Finantsinspektsioon, last amended 19.10.2026, fi.ee
- Vastus selgitustaotlusele [Reply to a request for explanation on biometric data], Data Protection Inspectorate, 04.02.2026, aki.ee
- Public consultations on AMLA Regulatory Instruments, Finantsinspektsioon, page last edited 21.04.2026, fi.ee
- Regulation (EU) 2024/1624 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, OJ L, 2024/1624, 19.6.2024, Article 90, EUR-Lex, eur-lex.europa.eu