



Identomat

COMPLIANCE GUIDE

Travel & Hospitality Compliance in Estonia

COUNTRY **Estonia**

INDUSTRY **Travel & Hospitality**

LAST UPDATED **21 October 2026**

KEY REGULATORS **Police and Border Guard Board · Consumer Protection and Technical
Regulatory Authority · Financial Intelligence Unit**

Key takeaways

- Hotels, hostels, holiday rentals and other accommodation providers in Estonia must register every guest, normally from a passport or identity card, before the stay begins, and keep the record for two years.
 - The law does not say the registration has to happen at a reception desk, so the guest data can be collected online before arrival. The provider may still ask to see the guest's passport or identity card.
 - Travel firms selling package holidays must notify their activity to the state and hold insolvency cover of at least 3 to 7 per cent of planned annual sales, with a minimum of €13,000 or €32,000 depending on the activity. Online sellers must also give their website address.
 - Ordinary travel and hospitality businesses are not covered by Estonia's anti-money laundering law. It applies only to currency exchange and to any business that takes or makes cash payments of €10,000 or more.
 - Since 12 October 2025, non-EU short-stay visitors give fingerprints and a facial image at the Schengen external border. The EU's pre-travel authorisation for visa-free visitors (ETIAS) has no start date yet.
-

Estonia is open to online travel and hospitality businesses. There is no licence to book rooms or sell flights. Travel undertakings that sell packages file a notice of economic activities and post insolvency security, and accommodation providers need no specific authorisation under the Tourism Act.

The principal authorities are the Police and Border Guard Board, which supervises guest registration and runs border, passenger-data and travel-authorisation systems, and the Consumer Protection and Technical Regulatory Authority, which supervises travel undertakings and their security.

The biggest practical obstacle for a new entrant is designing a guest-registration flow that captures the statutory data set before arrival, handles the extra document fields for non-EEA guests, and keeps the records for exactly two years.

CONTENTS

- 1 Who regulates this sector
- 2 Licensing and authorisation
- 3 Identity framework (AML rules do not apply)
- 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

Estonia is a unitary state, so all of these authorities act nationally, except municipalities, which supervise accommodation standards in their own territory.

Authority	Remit in travel and hospitality	Level	Official site
Police and Border Guard Board (Politsei- ja Piirivalveamet)	Supervises guest registration; border control; Entry/Exit System; ETIAS; receives carriers' passenger data and passenger name records	National	politsei.ee
Consumer Protection and Technical Regulatory Authority (Tarbijakaitse ja Tehnilise Järelevalve Amet)	Supervises the Tourism Act (except guest registration); travel undertakings' notices, security and sales reports; misdemeanour proceedings	National	ttja.ee
Financial Intelligence Unit (Rahapesu Andmebüroo)	Authorises currency exchange providers; anti-money laundering supervision of businesses not supervised by the financial regulator; receives suspicion and cash reports	National	fiu.ee
Data Protection Inspectorate (Andmekaitse Inspektsioon)	Supervises processing of guest and passenger personal data	National	aki.ee
City and rural municipality governments	Supervise accommodation service requirements locally	Local	Each municipality

The Rescue Board supervises fire safety in accommodation, and the Estonian Tax and Customs Board is one of the competent authorities that may receive passenger name record data.

2

Licensing and authorisation

Travel undertakings (packages and linked travel arrangements)

The Tourism Act (turismiseadus) covers undertakings that organise or sell packages or facilitate linked travel arrangements. Section 6 sorts their activities into areas, such as packages with travel services in Estonia, packages abroad with charter or scheduled flights, and mediating packages put together by a tour operator outside the European Economic Area (EEA). There is no licence. Instead, § 8 requires a notice of economic activities filed through the Estonian information gateway or a notary. The notice gives the areas of activity, any partner travel undertakings, trademarks, places of business and, in the case of e-commerce, the website address.

Under § 15, a tour operator must hold security for repatriation, accommodation until return, refunds for cancelled packages and unused gift vouchers. The same duty applies to tour operators established outside the EEA that direct their activity to Estonia. Section 15¹ sets the amount as a share of planned annual sales:

- 7 per cent, minimum €32,000, for packages abroad with charter flights and for mediating non-EEA packages;
- 3 per cent, minimum €32,000, for packages with scheduled flights;
- 7 per cent, minimum €13,000, for packages abroad without flights;
- 3 per cent, minimum €13,000, for linked travel arrangements.

The security may be a guarantee or insurance from an EEA insurer, credit institution or financial institution. The Consumer Protection and Technical Regulatory Authority is the beneficiary. Under § 15², quarterly sales reports are due by the 20th day after each quarter.

Accommodation providers

Accommodation service under § 17 means offering temporary sleeping accommodation. Section 18 reserves the type names (hotel, motel, guesthouse, hostel, holiday home, visitor's apartment, bed-and-breakfast) for establishments that meet their definitions. The Act imposes facility, hygiene and guest-registration duties but no permit.

Currency exchange

A hotel or travel business that offers foreign exchange becomes a financial institution under § 6 of the Money Laundering and Terrorist Financing Prevention Act. Under § 70 it needs authorisation from the Financial Intelligence Unit, unless it already holds an authorisation from the financial regulator or an EEA passport.

3

Identity framework (AML rules do not apply)

Travel agents, tour operators, carriers and accommodation providers are not listed as obliged entities in § 2 of the Money Laundering and Terrorist Financing Prevention Act (rahapesu ja terrorismi rahastamise tõkestamise seadus). The Act reaches the sector in two situations only.

Cash of €10,000 or more

A trader that receives or makes a cash payment of at least €10,000, as a single payment or linked payments within one year, is an obliged entity under § 2(1)5. It must apply due diligence each time under § 19(2): identify the payer from an identity document or travel document (§ 21), establish the source of the funds and check politically exposed person status. Any cash transaction over €32,000 must be reported to the Financial Intelligence Unit within two working days (§ 49(3)).

Currency exchange

A foreign exchange service provider is a financial institution. It applies full due diligence on business relationships, on occasional transactions of €15,000 or more (§ 19(1)2), and whenever money laundering is suspected. It reports suspicions within two working days and keeps records for five years (§ 47).

Outside those cases, identity in travel and hospitality is governed by three non-AML regimes:

- guest registration under § 24 of the Tourism Act;
- carriers' transmission of passenger data and passenger name records under the State Borders Act (riigipiiri seadus) and the Police and Border Guard Act (politsei ja piirivalve seadus);
- EU border systems operated by the Police and Border Guard Board.

None of these requires sanctions or politically exposed person screening by the operator.

Guest registration (Tourism Act § 24)

The accommodation provider must ensure each guest is registered before the provision of accommodation begins. Registration is "in general" based on the guest's travel document or identity card, or on another document or the guest's own statement where neither is available.

Guests who are citizens of Estonia, another EEA state or Switzerland, or foreigners living in Estonia on a residence permit or right of residence, give at least the following:

- given names and surnames;
- date of birth;
- citizenship;
- country of residence;
- the period of stay;
- the purpose of travel;
- the number of accompanying minors.

All other guests also give the type and number of their travel document and the state that issued it. A minor accompanying a parent need not be registered separately. A travel undertaking may register a group, and it is then responsible for the data matching the members' documents.

The guest is liable for the accuracy of the data, and the provider or travel undertaking may demand to see the travel document or identity card. Records are kept for two years from registration and supplied to the Police and Border Guard Board and security authorities on request.

Section 24 sets out data fields, not a verification technique. It does not require a copy of the document, a biometric check or liveness detection.

Carriers

Under § 9³ of the State Borders Act, carriers moving passengers across the external border by air, rail or water send the Police and Border Guard Board the passengers' travel-document data and travel details. They must inform passengers of this and delete the data within 24 hours of sending it. Under § 9⁷, air carriers also transfer passenger name records, the 20 data categories listed in § 25² of the Police and Border Guard Act. These include travel document details, contact data, payment information and travel agency data.

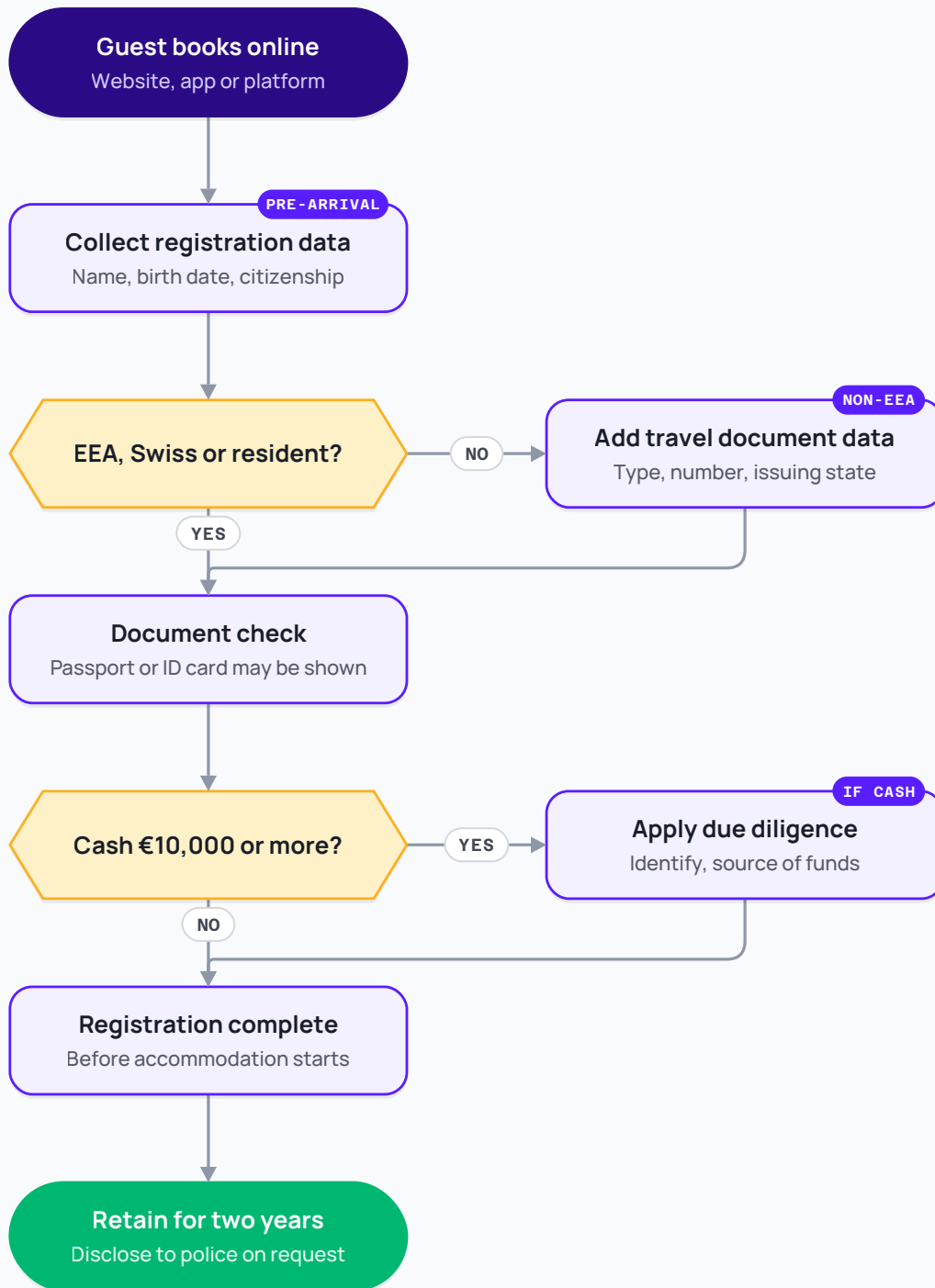


Figure 1. Online guest registration for an accommodation provider in Estonia.

Bottom line: Estonia's guest-registration and passenger-data rules are channel-neutral. The online-specific rules are a website disclosure for travel undertakings, stricter remote-identification methods for currency exchange, and a cash trigger that only bites in person.

Requirement	In person / desk	Online / remote	Difference
Guest data set and timing	Before the stay begins	Before the stay begins; may be collected pre-arrival	Same
Right to see the document	May demand passport or ID card	Same right; no remote method prescribed	Same
Guest record retention	Two years	Two years	Same
Travel undertaking notice	Places of business	Also website address	Differs
Package security	3 to 7 per cent of planned sales	Same amounts	Same
Passenger name record notice	At booking and ticket purchase	At booking and ticket purchase	Same
Currency exchange identification	Identity document	Defined remote methods for non-EEA residents and high outflows	Differs
Cash due diligence trigger	Cash of €10,000 or more	Not triggered by card or transfer	Differs

Online check-in is permitted, but the law gives no remote method

Section 24 of the Tourism Act requires registration before the stay starts but says nothing about where or how. A pre-arrival web or app form therefore satisfies the data duty. The provider's right to see the document is the same whether the guest is at a desk or using a self-service flow, and the law neither requires nor prohibits document scanning, chip reading or face matching. Adding them goes beyond the statutory minimum.

Remote identification for currency exchange

Section 31 of the Money Laundering and Terrorist Financing Prevention Act sets the rules for credit and financial institutions identifying customers who are not physically present. A formal remote-identification standard applies in two cases:

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

In those cases the provider must use an eIDAS-notified electronic identification scheme at the substantial or high assurance level, a qualified trust service, or another means that keeps data current, captures images, video and data clearly enough to identify the person unambiguously, and fails the identification if the connection drops. For customers resident in a high-risk third country, only the notified scheme or qualified trust service is allowed. An e-resident's digital identity document must be paired with another identity document.

Pending changes at the border

Adopted, start date not yet set ETIAS will require visa-exempt travellers to obtain an online authorisation before travel. The Police and Border Guard Board describes a six-month transitional period after launch.

Adopted, in force 28 Jan 2025 Regulation (EU) 2025/12 replaces Directive 2004/82/EC with new rules on carriers collecting and transferring advance passenger information.

6 Data protection and biometrics

The General Data Protection Regulation applies directly in Estonia and is supervised by the Data Protection Inspectorate.

For guest registration, the legal basis is the statutory duty in § 24 of the Tourism Act. That duty defines the data set: identity fields, plus document fields only for non-EEA guests. It also fixes a two-year retention period, so collecting more fields, keeping document images or storing records longer needs a separate justification.

Carriers have a tighter regime. They must tell passengers about passenger-data transfers and delete the transmitted advance passenger data within 24 hours. The Police and Border Guard Board keeps passenger name records for five years and pseudonymises them after six months.

Biometric capture at the border is a state function. Under the Entry/Exit System, the Police and Border Guard Board records the facial image and fingerprints of non-EU short-stay

travellers and keeps them in the central system for three years after exit. Travel businesses do not take part in that collection.

For currency exchange, the Money Laundering and Terrorist Financing Prevention Act treats processing for anti-money laundering purposes as a matter of public interest under the General Data Protection Regulation (§ 48). It requires the identification procedure data, including time stamps, to be kept for five years where § 31 remote identification is used (§ 47(6)).

7 Sector-specific obligations

Passenger data for carriers

Air, rail and sea carriers crossing the external border send travel-document data to the Police and Border Guard Board. Air carriers, including those carrying transit and transfer passengers through Estonian airspace, also transfer passenger name records. Air carriers or their agents must explain this to passengers both when a flight is booked and when the ticket is bought, which covers online travel agencies selling on a carrier's behalf.

Entry/Exit System and ETIAS

Estonia started using the Entry/Exit System at all its border crossing points on 12 October 2025. The system records entries, exits and refusals of entry of non-EU short-stay travellers, with or without a visa. ETIAS will apply to nationals of visa-exempt third countries. A travel authorisation will cost €20, last up to three years or until the passport expires, and be tied to one passport.

Insolvency security and sales reporting

Travel undertakings must keep their security sufficient at all times and prove it. They must recalculate it on the basis of previous-year sales where those exceeded planned sales, and inform the Consumer Protection and Technical Regulatory Authority promptly if insolvency prevents them from performing a package. The Authority decides on the use of the security, sets a claims period of at least 14 days and arranges repatriation and refunds. The security does not form part of a bankruptcy estate.

Risk indicators and red flags

IDENTITY AND PAYMENT RED FLAGS IN TRAVEL AND HOSPITALITY

- **Split cash:** several cash payments by one guest or group that together reach €10,000 within a year, which triggers due diligence.
- **No document:** a guest who cannot show a passport or identity card and registers on a statement alone.
- **Group mismatch:** travel-group lists from an agency that do not match members' documents, for which the agency is responsible.
- **Inconsistent nationality:** a declared EEA citizenship that does not match the document, which would avoid the extra non-EEA document fields.
- **Unsecured package seller:** a partner selling packages in Estonia without a notice of activity or security on record.
- **Large exchange:** currency exchange of €15,000 or more outside a business relationship, or monthly outflows above the remote-identification thresholds.
- **Third-party payer:** bookings paid by an unrelated person or company with no explanation, relevant where cash or exchange triggers apply.

Enforcement and penalties

Penalties are set per misdemeanour, with separate caps for individuals and legal persons:

Breach	Provision	Individual	Legal person	Authority
Selling packages or linked travel arrangements without security	Tourism Act § 31 ¹	Up to 300 fine units	Up to €50,000	Consumer Protection and Technical Regulatory Authority
Failing to send, or sending wrong, passenger data	State Borders Act § 17 ³	Up to 300 fine units	Up to €32,000	Police and Border Guard Board

Failing to transfer, or transferring wrong, passenger name records	State Borders Act § 17 ⁵	Up to 300 fine units	Up to €32,000	Police and Border Guard Board
Failing to identify and verify a customer (cash traders, currency exchange)	Money Laundering and Terrorist Financing Prevention Act § 84	Up to €1,000,000 or twice the benefit	Up to €1,000,000 or twice the benefit	Financial Intelligence Unit

The specific misdemeanour for failing to register guests was repealed with effect from 1 January 2015. The duty remains, and the Police and Border Guard Board supervises it using the state supervision measures of the Law Enforcement Act, as allowed by § 30¹ of the Tourism Act, including entry to premises used for the business.

Against travel undertakings, the Consumer Protection and Technical Regulatory Authority can also call on the security and pay travellers' claims from it.

10 Recent changes and what to watch

- **In force 1 Oct 2026** New consolidated versions of the State Borders Act and the Police and Border Guard Act took effect. Carriers should confirm that their passenger-data and passenger name record procedures match the current text.
- **In force 6 Jun 2026** Amendments to the Police and Border Guard Act updated cross-border information exchange and the conditions for re-identifying pseudonymised passenger name records on request from Europol, another Member State or a third country.
- **In force 1 May 2026** The Tourism Act was amended (RT I, 18.03.2026, 2) in its supervision chapter. Guest-registration duties are unchanged.
- **In force 12 Oct 2025** The Entry/Exit System replaced passport stamping for non-EU short-stay travellers at all Estonian border crossing points.
- **Adopted, in force 28 Jan 2025** Regulation (EU) 2025/12 on advance passenger information entered into force and will replace Directive 2004/82/EC. Carriers should plan for new transmission arrangements.
- **Adopted, start date not yet set** ETIAS remains planned with a transitional period after launch. Booking flows serving visa-exempt travellers should prepare to prompt for it.

Two data tiers. Registration forms need a branch: EEA, Swiss and Estonian-resident guests give seven fields, and everyone else adds document type, number and issuing state. Reading the machine-readable zone or the chip of a passport is a convenient way to fill those fields accurately, but the law does not require it.

Timing. Registration must be complete before the stay starts, so pre-arrival online collection with a document check at key handover or self-check-in fits the rules.

Minimisation and retention. Schedule deletion at two years for guest records. Do not keep document images, selfies or biometric templates by default, because § 24 does not call for them.

Payment triggers. Cash of €10,000 or more, including linked payments within a year, and any currency exchange bring in anti-money laundering identification. For remote exchange customers living outside the EEA, that means a notified electronic identification at the substantial or high level, a qualified trust service, or a video or document method meeting the statutory quality and fail-safe standard; customers in high-risk third countries need the first two.

Border alignment. Passenger-facing products should keep the passport used for booking consistent with the one used for ETIAS and the Entry/Exit System, and show carriers' passenger-data notices at both booking and ticket purchase.

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:

- Pre-arrival guest registration with ID document capture and verification, including NFC chip reading, to fill the statutory data fields accurately.
- Face match and biometric liveness for self-check-in flows where an operator chooses to confirm the guest holds the document.
- KYC onboarding and AML screening for currency exchange and for cash payments that reach the 10,000 euro due diligence threshold.
- No-code workflow builder to branch registration for EEA and non-EEA guests and apply retention rules, 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

- **Turismiseadus [Tourism Act]**, RT I 2000, 95, 607, as amended by RT I, 18.03.2026, 2, version in force from 1 May 2026, §§ 3, 6, 8, 15–15⁴, 17–19, 24, 30–31⁵, Riigi Teataja, [Estonian text](#) and [English translation](#)
- **Rahapesu ja terrorismi rahastamise tõkestamise seadus [Money Laundering and Terrorist Financing Prevention Act]**, version in force from 21 July 2026, §§ 2, 6, 19–21, 31, 47–49, 64, 70, 84, Riigi Teataja, [Estonian text](#) and [English translation](#)
- **Riigipiiri seadus [State Borders Act]**, version in force from 1 October 2026, §§ 9³, 9⁷, 17³, 17⁵, 17⁶, Riigi Teataja, riigiteataja.ee
- **Politsei ja piirivalve seadus [Police and Border Guard Act]**, version in force from 1 October 2026, §§ 25²–25⁵, Riigi Teataja, [English translation](#)

- Regulation (EU) 2025/12 on the collection and transfer of advance passenger information for enhancing and facilitating external border checks, OJ L, 2025/12, 8.1.2025, EUR-Lex, eur-lex.europa.eu
- Entry/Exit System (EES), Schengen border control, Police and Border Guard Board, politsei.ee
- Estonia and other European countries are introducing a new Entry/Exit System, Police and Border Guard Board news release, October 2025, politsei.ee
- European Travel Information and Authorisation System, Police and Border Guard Board, politsei.ee