Identomat

COMPLIANCE GUIDE

Fintech & Digital Payments Compliance in Latvia

COUNTRY Latvia

INDUSTRY Fintech & Digital Payments

LAST UPDATED 5 November 2026

KEY REGULATORS Latvijas Banka · Financial Intelligence Unit of Latvia · Consumer Rights Protection Centre

Key takeaways

- Payment and e-money businesses need a licence or registration from Latvijas Banka, the central bank and financial market supervisor, before serving customers in Latvia; firms licensed elsewhere in the European Union can passport in.
- Onboarding a customer online triggers enhanced due diligence by default. That is avoided only if the firm has the required safeguards and uses one of four government-approved remote methods: e-signature or electronic ID, live video identification, an identification payment from a bank or payment institution, or a document photo matched to a selfie.
- Video and selfie checks must leave a tamper-proof audit trail with a timestamp, the person's name and their IP address, all remote identification data must be stored unaltered, and ID documents must be checked against Latvia's register of invalid documents.
- Apps, websites and call centres must offer the service in Latvian (compliance deadline 30 September 2026), and payment providers must block card payments from Latvian residents to unlicensed online gambling sites.
- Supervision is being consolidated: buy now, pay later providers register with Latvijas Banka from 20 November 2026, consumer lenders move to Latvijas Banka on 1 January 2027, and the EU's single anti-money laundering rulebook applies from 10 July 2027.

Latvia is open to digital payment and e-money businesses, and new licences are issued regularly. The framework combines EU payment law with a national anti-money laundering (AML) statute and a government regulation that set out remote identification methods in detail.

The principal authorities are Latvijas Banka, which licenses and supervises payment and e-money institutions for prudential, AML and sanctions purposes, and the Financial Intelligence Unit of Latvia (FIU Latvia), which receives suspicious transaction reports and is the competent authority for sanctions. The biggest obstacle for a new entrant is building a remote onboarding flow that meets Cabinet of Ministers Regulation No. 392 point by point, because a flow that falls outside it turns every online customer into an enhanced due diligence case.

CONTENTS

1 Who regulates this sector
2 Licensing and authorisation
3 AML, KYC and customer due diligence
4 Identity verification and onboarding
5 Digital channels: what's different
6 Data protection and biometrics
7 Sector-specific obligations
8 Risk indicators and red flags
9 Enforcement and penalties
10 Recent changes and what to watch
11 What this means for identity verification
▪ Sources

1 Who regulates this sector

Regulator	Remit for fintech	Level	Official site
Latvijas Banka	Licensing and registration of payment and e-money institutions; prudential, AML/CFT and sanctions supervision; buy now, pay later register from 20 Nov 2026; consumer lending and payment consumer protection from 1 Jan 2027	National	bank.lv
Finanšu izlūkošanas dienests (FIU Latvia)	Suspicious transaction reports, threshold declarations, freezing orders, typologies; competent authority for sanctions	National	fid.gov.lv
Patērētāju tiesību aizsardzības centrs (Consumer Rights Protection Centre)	Consumer protection in payment services and licensing and AML supervision of consumer lenders until 31 Dec 2026	National	ptac.gov.lv
Datu valsts inspekcija (Data State Inspectorate)	Data protection, including biometric data used in onboarding	National	dvi.gov.lv
Valsts ieņēmumu dienests (State Revenue Service)	Decisions on unlicensed gambling operators that payment providers must block; politically exposed person data	National	vid.gov.lv

European Banking Authority and EU Anti-Money Laundering Authority	EU guidelines and technical standards; the single AML rulebook from 2027	Supranational	eba.europa.eu, amla.europa.eu

2 Licensing and authorisation

Under the Maksājumu pakalpojumu un elektroniskās naudas likums (Law on Payment Services and Electronic Money), Section 4, a payment institution or e-money institution may start business in Latvia only after receiving a Latvijas Banka licence, unless it qualifies for registration. Latvijas Banka decides on a licence within three months of receiving a complete application (Section 24). Initial capital on the day the licence is granted (Section 12) is:

Authorisation	Initial capital or condition
Payment institution: money remittance only	EUR 20,000
Payment institution: payment initiation services	EUR 50,000
Payment institution: accounts, transfers, card issuing or acquiring	EUR 125,000
Electronic money institution	EUR 350,000
Registered payment institution (Section 5)	Only issuing payment instruments or money remittance; average payments up to EUR 3 million a month; users connected to Latvia; decision within 30 days
Registered e-money institution (Section 5.1)	Average outstanding e-money up to EUR 2 million; closed system only; holders connected to Latvia

Institutions licensed in another EU or EEA state can operate through a branch, agent or cross-border services once their home supervisor has notified Latvijas Banka (Section 31). The AML law also provides for a central contact point in Latvia appointed by an EEA payment or e-money institution to secure its compliance with Latvian AML rules (Section 1, point 6.3). A licensed e-money institution may also issue, hold and transfer its own e-

money tokens, following the procedure in the EU Markets in Crypto-Assets Regulation (Section 4(4)).

Latvijas Banka's published licensing roadmap starts with a free pre-application stage, where it answers questions within up to 30 days. It then checks a submitted application for completeness within 15 working days before the substantive review begins.

Non-bank consumer lending is a separate regime under the Patērētāju tiesību aizsardzības likums (Consumer Rights Protection Law), Section 8: a lender needs a special permit (licence) and paid-up share capital of at least EUR 425,000. The licensing authority moves from the Consumer Rights Protection Centre to Latvijas Banka on 1 January 2027 `Adopted, effective 1 Jan 2027`; licences already issued stay valid.

3 AML, KYC and customer due diligence

Payment and e-money institutions, other payment service providers and licensed consumer lenders are "financial institutions" and so obliged entities under the Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likums (Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing), Sections 1(7) and 3. Latvijas Banka supervises payment and e-money institutions for AML purposes (Section 45).

When CDD applies

Before a business relationship; for an occasional transfer of funds of EUR 1,000 or more; for other occasional transactions of EUR 15,000 or more; and on suspicion (Section 11). If due diligence cannot be completed, the firm must not open the account.

Ongoing review

Customer data must be reviewed according to risk, and at least once every five years (Section 11.1(1)(5)).

Risk scoring

Licensed payment and e-money institutions must calculate an automated numerical risk score for each customer unless Latvijas Banka agrees otherwise in writing, and all supervised institutions set product limits to match risk (Latvijas Banka Regulation No. 316, points 11 and 18).

Enhanced due diligence

Required for non-face-to-face customers unless the Regulation No. 392 conditions are met, for politically exposed persons and for customers from high-risk third countries (Sections 22 and 25.1).

Simplified measures. Identification and beneficial ownership measures may be waived for low-risk e-money only if the instrument cannot be reloaded or has a monthly limit of EUR 150 usable only in Latvia, holds no more than EUR 150, can be used only for goods or services from the issuer or its network, is not linked to a payment account, cannot be redeemed for cash or crypto-assets, and is monitored for suspicious activity (Section 27.1). Account information and payment initiation providers may apply simplified due diligence using only the data available to them (Section 26(3.1)).

Reporting. Suspicious transactions are reported immediately through FIU Latvia's online system (Section 31.4). A firm that refrains from a suspicious transaction must report by the next working day (Section 32). Payment service providers also file threshold declarations for cash transactions of EUR 7,000 or more and for cross-border payments sent or received of EUR 500,000 or more (Cabinet of Ministers Regulation No. 550, point 14.1). FIU Latvia requests must be answered within three working days when urgent and seven working days otherwise.

Records. Due diligence records, payment data and correspondence are kept for five years after the relationship ends, extendable by authorities for up to five more years, and then destroyed (Section 37).

4 Identity verification and onboarding

A natural person is identified from an identity document showing, for residents, name, surname and personal code; for non-residents, name, date of birth, photograph, document number, issue date and issuing state and authority (AML law, Section 12). The firm must confirm that the document is not listed in the Register of Invalid Documents (Section 12(3.1)) and keep a copy of it (Section 14). Private companies access the register under a contract with the Ministry of the Interior's Information Centre (Cabinet of Ministers Regulation No. 708, points 2 and 26).

Remote identification is governed by Cabinet of Ministers Regulation No. 392 (as amended in June 2022). Before using it, the firm must have a documented risk assessment, an internal control system, trained staff, customer information about the process and security requirements for the technology (point 2). Point 7 lists four accepted methods:

- a secure electronic signature, qualified increased security electronic identification, or eIDAS-recognised solutions;
- video identification meeting point 10;
- identity data obtained from a credit institution or payment institution through an identification payment;

- comparison of a photo of the identity document with a selfie.

For video and selfie methods, the firm must check the document's remotely verifiable security features and compare the person biometrically (point 9). The document needs a machine-readable zone, read during the session, and optical security features, and forgery detection must be used (point 11); the captured image or video counts as the document copy. Selfie and identification-payment methods are barred where the customer or beneficial owner is linked to a high-risk third country or a low-tax jurisdiction (point 12).

Firms may outsource remote identification to a provider that follows EU AML requirements, provided they assess and monitor it (point 6); the firm stays responsible for the result (AML law, Section 23(3)). Agents that identify customers on a firm's behalf before onboarding are subject to Latvijas Banka Regulation No. 351, including an annual quality review.

Latvijas Banka's AML handbook (March 2026) adds supervisory expectations: proof that video or selfie capture is live rather than recorded; chip data treated as the most reliable source (citing EBA/GL/2022/15); checks that foreign qualified e-signatures come from an eIDAS qualified trust service provider; correct handling of residence permits; and regular testing of outsourced solutions.

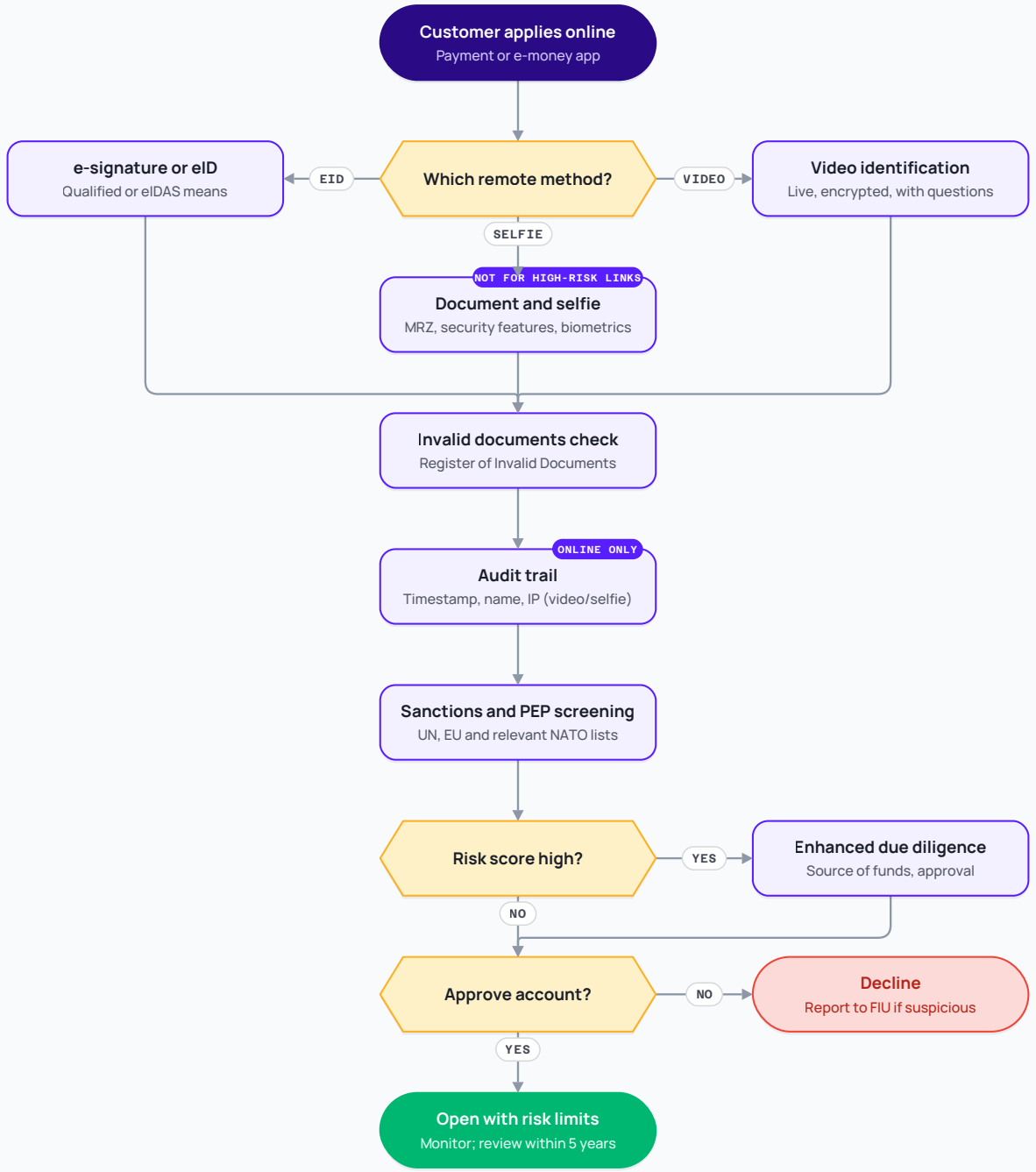


Figure 1. Remote onboarding for a payment or e-money account in Latvia under Cabinet of Ministers Regulation No. 392.

Minors. Since 15 October 2026 a payment provider may open an account or issue an instrument to a minor of any age, with age-appropriate limits. Until the age of 16 a parent or legal representative opens and manages it; from 16 the minor may contract alone (Payment Services Law, Section 79.1).

5 Digital channels: what's different

Bottom line: remote onboarding is permitted, but it triggers enhanced due diligence unless the firm has the required safeguards and uses one of the four methods in Regulation No. 392, which also sets document, biometric and logging requirements.

Requirement	In person	Online / remote	Difference
Risk treatment	Risk-based CDD	EDD unless Regulation No. 392 method and mitigations used	Differs
Accepted identification	Identity document examined in person	e-signature or eID, video, identification payment, or document plus selfie	Differs
Document requirements	Valid identity document	For video and selfie: machine-readable zone, optical security features and forgery detection	Differs
Biometric comparison	Visual comparison by staff	Biometric recognition and comparison required for video and selfie methods	Differs
Evidence kept	Copy of the document	Unalterable identification data; for video and selfie, a timestamped audit trail with name and IP address	Differs
Account access	Branch procedures	Strong customer authentication for online access and payments	Differs
Invalid documents check	Required	Required	Same
Latvian-language service	Required at service points	Required in apps, websites and call centres	Same
Responsibility when outsourcing	Firm remains responsible	Firm remains responsible	Same

Remote identification as an EDD trigger

Section 22(2)(1) of the AML law requires enhanced due diligence for customers not identified in person, unless the firm has mitigating policies and training and uses a Regulation No. 392 method. Section 23 adds at least one extra measure, such as further documents, a first payment from the customer's own bank account or, for residents, a secure e-signature.

Video identification standard

Video identification must run live over an encrypted audio and video stream, with the face uncovered and compared with the document photo, the document legible and verification questions asked; an interrupted stream means starting again (Regulation No. 392, point 10).

Account security and payment design

Strong customer authentication applies to online account access, payment initiation and risky remote actions, with remote payments dynamically linked to amount and payee (Payment Services Law, Section 104.4). Euro-area providers have had to offer verification of the payee since 9 October 2025 (Regulation (EU) 2024/886, Article 5c). Apps, websites and call centres must be available in Latvian, including for providers passporting in without a branch (Section 44.4).

What is changing

The EU Anti-Money Laundering Regulation `Adopted, applies 10 Jul 2027` allows verification by document or by eIDAS electronic identification at level substantial or high (Article 22(6)). Under the European Digital Identity Framework `Adopted, phased dates`, wallets are due 24 months after core implementing acts that entered into force on 24 December 2024, and regulated private services using strong user authentication must accept them on request by late December 2027 (Regulation (EU) 2024/1183, Articles 5a(1) and 5f(2)). The EU payments package `Political agreement, not adopted` of 27 November 2025 would extend name-and-IBAN checks to all credit transfers and make providers liable for some impersonation fraud. AMLA's final draft standards on customer due diligence `Final draft, not adopted` would allow remote document-based checks only as a fallback, where the customer cannot reasonably present an identity document in person and has no eIDAS means at level substantial or high or relevant qualified trust service; the firm must justify this and meet listed safeguards (draft Article 7).

6 Data protection and biometrics

The General Data Protection Regulation applies in full, supervised by the Data State Inspectorate. Biometric data used to uniquely identify a person is a special category under Article 9(1), so selfie and video methods need an Article 9(2) condition; Regulation No. 392 is the national rule that requires the biometric comparison.

Due diligence data may be used only to prevent money laundering and terrorism and proliferation financing, never for commercial purposes (AML law, Section 11.1(8)). The Inspectorate's list of processing requiring a data protection impact assessment includes biometric identification combined with a high-risk criterion such as AML or fraud database screening, so biometric remote onboarding will normally need one before launch. Remote identification data, including video, must be kept unalterable for the statutory five years after the relationship ends; a firm combining e-signature with video may keep only images of the person and document (Regulation No. 392, point 16).

7 Sector-specific obligations

Sanctions, including NATO-member lists

Under the Starptautisko un Latvijas Republikas nacionālo sankciju likums (Law on International Sanctions and National Sanctions of the Republic of Latvia), financial market participants apply UN, EU and national sanctions and, under Cabinet criteria, EU or NATO member state sanctions that significantly affect the financial market (Sections 11(6) and 13(4)). A documented sanctions risk assessment and internal control system are required (Section 13.1), and freezes must be reported to FIU Latvia immediately (Section 12(5)).

Unlicensed gambling payment blocking

Payment providers must not serve gambling operators named in a State Revenue Service decision, must stop transfers to them within three working days, and must refuse remote card payments by Latvian-resident cards to unlicensed online gambling operators, reporting refusals each year by 1 February (Payment Services Law, Section 44.2).

Fraud risk management

Latvijas Banka's February 2025 fraud risk guidelines (comply or explain) expect an annual documented fraud risk assessment, a management plan and procedures to reject, suspend and recall suspicious payments.

Buy now, pay later

From 20 November 2026 `Adopted, effective 20 Nov 2026`, large enterprises offering their own deferred payment credit must register with Latvijas Banka (Consumer Rights Protection Law, Section 8.6). Creditworthiness checks apply unless payment is due within 50 days, or 14 days for large online sellers. Latvijas Banka Regulation No. 427 requires a board member responsible for the service and AML, and an AML internal control description from 10 July 2027.

8 Risk indicators and red flags

PAYMENT AND E-MONEY INDICATORS (FIU LATVIA, 2024)

- **Money mules**: personal accounts used to pass on funds quickly, often to foreign payment institutions or crypto providers.
- **Transit payments**: funds withdrawn or forwarded shortly after they arrive.
- **Shared IP addresses**: different accounts operated from the same IP address.
- **Crypto conversion**: funds in a payment institution account mainly used to buy virtual currency.
- **Nested providers**: a payment institution receiving funds from other payment institutions' accounts, or with weak monitoring.
- **Online gambling layering**: winnings from several gambling platforms cited as the source of funds.
- **Investment scams**: platforms promising unrealistically high returns.
- **Impersonation fraud**: customers told by a "bank employee" or "police officer" to move money urgently.

9 Enforcement and penalties

For AML breaches, Latvijas Banka may fine a financial institution up to 10% of annual turnover, or up to EUR 5 million where that is higher, and responsible individuals up to EUR 5 million (AML law, Section 78(3)). Other sanctions include warnings, public statements, licence suspension or withdrawal and removal of responsible persons (Section 78(1)). Decisions stay published for five years.

On 25 June 2025 Latvijas Banka warned Paysera LT, a Lithuanian e-money institution, for internal control deficiencies and AML breaches in serving Latvia through agents. FIU Latvia's 2026 national risk assessment reports that inspections of payment and e-money institutions found significant gaps, including weak risk scoring and missing automated alerts.

10 Recent changes and what to watch

- **10 July 2027** `Adopted, applies 10 Jul 2027`: the EU Anti-Money Laundering Regulation applies directly, with a EUR 10,000 occasional transaction threshold and a narrower e-money exemption for non-reloadable products up to EUR 150. The EU Anti-Money Laundering Authority selects the entities it will supervise directly in 2027, with direct supervision from 2028.
- **1 January 2027** `Adopted, effective 1 Jan 2027`: consumer protection supervision of payment services, and licensing and AML supervision of consumer lenders, move from the Consumer Rights Protection Centre to Latvijas Banka.
- **20 November 2026** `Adopted, effective 20 Nov 2026`: new buy now, pay later rules take effect, with registration of large-enterprise providers at Latvijas Banka.
- **15 October 2026** `In force`: payment accounts for minors with age-appropriate limits are permitted; Latvijas Banka must run a reporting channel for payment law breaches.
- **30 September 2026** `Final draft, not adopted`: AMLA's final report on draft standards for customer due diligence under Article 28(1) of the Anti-Money Laundering Regulation, submitted to the European Commission on 1 October 2026, limits remote document-based checks to a justified fallback with safeguards. The standards are proposed to apply six months after entry into force.
- **30 September 2026** `In force`: deadline for Latvian-language documents and digital interfaces for payment services.
- **27 November 2025** `Political agreement, not adopted`: the EU Payment Services Regulation and amendments to PSD2 were agreed politically; Parliament's committee approved the text on 5 May 2026, and formal adoption is pending.
- **9 October 2025** `In force`: euro-area providers must send instant euro credit transfers and offer verification of the payee.

11 What this means for identity verification

- **Design to the list.** Map each remote flow to one of the four Regulation No. 392 methods, with machine-readable zone, security-feature and invalid-document checks.
- **Route by risk.** Send customers linked to high-risk third countries or low-tax jurisdictions to e-signature, eID or video identification.
- **Biometrics and liveness.** Prove live capture and compare faces biometrically; no certified presentation-attack standard is named, so set, test and document your own, and read the chip where possible.
- **Evidence.** Store all remote identification data unaltered, with timestamped name and IP logs for video and selfie sessions, for five years after the relationship ends.
- **Re-verification.** Refresh due diligence on material change and at least every five years.

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, MRZ and security-feature checks, face match and biometric liveness detection.
- Video KYC sessions with live agent questioning and a timestamped audit trail.
- AML screening against sanctions, PEP and watchlists at onboarding and through ongoing monitoring.
- No-code workflow builder to route customers by risk, for example to video KYC or e-signature for higher-risk profiles.
- KYB and beneficial owner verification for business customers and merchants.

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

- **Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likums [Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing]**, version in force from 15.10.2026, Sections 1, 3, 11, 11.1, 12, 14, 22, 23, 25.1, 26, 27.1, 31.4, 32, 37, 45, 78, likumi.lv
- **Maksājumu pakalpojumu un elektroniskās naudas likums [Law on Payment Services and Electronic Money]**, version in force from 15.10.2026 and version from 01.01.2027, Sections 4, 5, 5.1, 12, 24, 31, 44.2, 44.4, 79.1, 104.4, 105, 108, likumi.lv
- **Likums "Par fizisko personu elektronisko identifikāciju" [Law on Electronic Identification of Natural Persons]**, Section 1, point 4.1 (official English translation), likumi.lv
- **Latvijas Bankas likums [Latvijas Banka Law]**, in force from 1 January 2023, Section 5 and transitional provisions, likumi.lv
- **Ministru kabineta noteikumi Nr. 392 [Cabinet of Ministers Regulation No. 392] on non-face-to-face customer identification**, 3 July 2018, as amended by Regulation No. 331 of 7 June 2022, likumi.lv
- **Latvijas Bankas noteikumi Nr. 316 [Latvijas Banka Regulation No. 316] on customer risk, due diligence and IT solutions**, 17 September 2024, likumi.lv
- **Latvijas Bankas noteikumi Nr. 351 [Latvijas Banka Regulation No. 351] on cooperation with third parties for customer identification**, 25 November 2024, likumi.lv
- **Ministru kabineta noteikumi Nr. 550 [Cabinet of Ministers Regulation No. 550] on suspicious transaction reports and threshold declarations**, 17 August 2021, point 14, likumi.lv
- **Starptautisko un Latvijas Republikas nacionālo sankciju likums [Law on International Sanctions and National Sanctions of the Republic of Latvia]**, version in force from 15.10.2026, Sections 11, 12, 13, 13.1, likumi.lv
- **Patērētāju tiesību aizsardzības likums [Consumer Rights Protection Law]**, current version and version from 01.01.2027, Sections 8, 8.6 and transitional provisions, likumi.lv
- **Latvijas Banka, deferred payment service providers invited to comply with new Consumer Rights Protection Law requirements**, 21 October 2026, bank.lv
- **Latvijas Banka, Vadlīnijas finanšu krāpšanas riska uzraudzībai, pārvaldībai un ierobežošanai [Guidelines on financial fraud risk]**, February 2025, sections 1 and 3, bank.lv
- **Latvijas Banka, Financial Market Participant Register: Sanctions** (Paysera LT entry, 25 June 2025), uzraudziba.bank.lv
- **Latvijas Banka, Licensed payment institution (licensing roadmap)**, bank.lv
- **Latvijas Banka, Vadlīnijas NILLTPF novēršanas un sankciju riska pārvaldīšanas iekšējās kontroles sistēmas izveidei un klientu izpētei [AML handbook]**, March 2026, section 5.10, bank.lv

- **Latvijas Bankas noteikumi Nr. 427 [Latvijas Banka Regulation No. 427] on registration of deferred payment service providers**, 19 October 2026, effective 20 November 2026, points 6 and 26, likumi.lv
- **Ministru kabineta noteikumi Nr. 708 [Cabinet of Ministers Regulation No. 708] on the Register of Invalid Documents**, version in force from 9 December 2025, points 2 and 26, likumi.lv
- **FIU Latvia, Nacionālais NILLTPF risku novērtēšanas ziņojums 2023-2025 [National ML/TF/PF risk assessment]**, 2026, section 5.9, fid.gov.lv
- **Datu valsts inspekcija, list of processing operations requiring a data protection impact assessment**, 18 December 2018, item 13, dvi.gov.lv
- **Council of the EU, Payment services: Council and Parliament agree to step up the fight against fraud and increase transparency**, 27 November 2025, consilium.europa.eu
- **European Parliament, Legislative Train: Payment services regulation**, updated 25 October 2026, europarl.europa.eu
- **AMLA, Final Report: Draft Regulatory Technical Standards under Article 28(1) of Regulation (EU) 2024/1624**, 30 September 2026, Article 7 and Article 29, amla.europa.eu
- **AMLA, Press Release: AMLA finalises key standards for the private sector**, 1 October 2026, amla.europa.eu
- **AMLA, AMLA takes next step toward 2027 selection of entities for direct supervision**, 12 May 2026, amla.europa.eu
- **FIU Latvia, Typologies and Indicators of Money Laundering**, 3rd revised edition, 2024, typologies 21 and 23, indicators B4, C6, G3, G5, G6, H, I, fid.gov.lv
- **Regulation (EU) 2024/1624 (Anti-Money Laundering Regulation)**, Articles 19, 22(6) and 90, eur-lex.europa.eu
- **Regulation (EU) 2024/886 (instant credit transfers in euro)**, Articles 5a(8) and 5c, eur-lex.europa.eu
- **Regulation (EU) 2024/1183 (European Digital Identity Framework)**, Articles 5a(1) and 5f(2), eur-lex.europa.eu
- **Commission Implementing Regulations (EU) 2024/2979 and 2024/2981**, published 4 December 2024, eur-lex.europa.eu, eur-lex.europa.eu
- **Regulation (EU) 2016/679 (General Data Protection Regulation)**, Article 9, eur-lex.europa.eu