Identomat

COMPLIANCE GUIDE

Banking & Digital Banking Compliance in Latvia

COUNTRY Latvia

INDUSTRY Banking & Digital Banking

LAST UPDATED 5 November 2026

KEY REGULATORS Latvijas Banka · European Central Bank · Financial Intelligence Unit of Latvia

Key takeaways

- Taking deposits in Latvia needs a credit institution licence, an EU passport or a third-country branch permit. New banks need at least EUR 5 million of starting capital, but a "specialised" bank, which includes one that serves customers only digitally, needs EUR 1 million (from 6 January 2026).
- Fully remote account opening is allowed. A government regulation lists four accepted methods: a qualified electronic signature or qualified increased security electronic ID, live video identification, data from an identification payment, or a document photo matched to a selfie.
- Remote onboarding counts as higher risk, which triggers enhanced due diligence (EDD, extra checks), unless the bank uses one of those approved methods and has controls in place. The payment-based and selfie methods cannot be used for customers linked to high-risk or low-tax countries.
- Since 1 January 2026, banks serving Latvian consumers must offer more than one way to apply and price branch and online services by real cost; the largest retail banks must also provide in-person identification.
- The EU Anti-Money Laundering Regulation applies directly from 10 July 2027, and Latvian law will have to be aligned with it. Fines under current law reach 10% of annual turnover or EUR 5 million, whichever is higher.

Latvia is open to digital banks, both locally licensed and passported from other EU countries. The Council of Europe's MONEYVAL evaluation (February 2026) notes that the country's financial system has been substantially transformed since 2018, and supervisors now pair anti-money laundering (AML) enforcement with a push against unnecessary account refusals.

Latvijas Banka, the central bank, is the national prudential and AML supervisor of banks; the European Central Bank (ECB) takes licensing decisions and directly supervises significant banks. The Financial Intelligence Unit of Latvia (FIU Latvia) receives suspicious transaction and threshold reports.

The main obstacle for a new entrant is building a remote onboarding process that meets the detailed technical conditions of Cabinet Regulation No. 392. Without them, every remote customer automatically needs enhanced due diligence.

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

Since 1 January 2023 Latvijas Banka has replaced the former Financial and Capital Market Commission as supervisor.

Authority	Remit	Level	Official site
Latvijas Banka	Licensing applications, prudential supervision, AML and sanctions-risk supervision of credit institutions; deposit guarantee fund	National	bank.lv
European Central Bank	Grants and withdraws bank authorisations; direct supervision of significant banks	Supranational (EU)	bankingsupervision.europa.eu
Financial Intelligence Unit (Finanšu izlūkošanas dienests)	Suspicious transaction reports, threshold declarations, freezing orders, sanctions exemptions	National	fid.gov.lv
Data State Inspectorate (Datu valsts inspekcija)	Data protection supervision; licenses shared customer due diligence tools	National	dvi.gov.lv

Register of Enterprises (Uzņēmumu reģistrs)	Beneficial ownership register; receives discrepancy reports	National	ur.gov.lv
Anti-Money Laundering Authority (AMLA)	EU AML authority; will directly supervise selected high-risk entities active in six or more Member States	Supranational (EU)	amla.europa.eu

2 Licensing and authorisation

Under Section 3 of the Kredītiestāžu likums (Credit Institutions Law), only a credit institution registered in an EU Member State, its branch, or a licensed third-country branch may carry on banking business in Latvia. A Latvian bank may start operating only after receiving a licence, which is issued for an unlimited period (Section 11). Applications go to Latvijas Banka; under the Single Supervisory Mechanism the ECB issues the authorisation, as Latvijas Banka Regulation No. 259 on credit institution licensing explains.

Capital

Initial capital of at least EUR 5 million, or EUR 1 million for a specialised credit institution (Section 21, as amended with effect from 6 January 2026). A specialised institution must meet one of three tests: a limited customer circle, services provided only digitally, or an innovative business model new to Latvia (Section 1, point 73).

Timeline

An application is decided within three months of a complete file, and no later than 12 months after it was filed (Section 14).

Fit and proper

Founders must be identifiable, of impeccable reputation and with documented lawful funds (Section 16); the AML officer candidate is part of the application (Section 15).

EU passport

A bank licensed elsewhere in the EU may open a Latvian branch or serve Latvian customers cross-border after the home-supervisor notification procedure (Section 12.1), without a Latvian licence.

Since 9 June 2026, third-country bank branches (CRD VI) must hold segregated capital of at least EUR 10 million (class 1) or EUR 5 million (class 2) (Section 33.15). Eligible deposits are covered by the deposit guarantee fund, managed by Latvijas Banka, up to EUR 100,000 per depositor (Noguldījumu garantiju likums, Deposit Guarantee Law, Section 3).

3 AML, KYC and customer due diligence

Credit institutions are 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, "AML Law"), supervised by Latvijas Banka (Section 45). Latvijas Banka Regulation No. 316 (2024) adds minimum due diligence content, a mandatory numerical customer risk-scoring system and IT requirements, and incorporates the EBA risk factor guidelines (EBA/GL/2021/02).

When customer due diligence applies

Section 11 requires customer due diligence (CDD) before a business relationship starts; for occasional transactions of EUR 15,000 or more (single or linked); for occasional transfers of funds of EUR 1,000 or more; and whenever money laundering is suspected or earlier data is doubtful. Customer files must be reviewed in line with risk and at least once every five years (Section 11.1). If CDD cannot be completed, the bank must not open the account, must end any existing relationship, and must consider a report (Section 11(7)).

Beneficial ownership

Banks must establish the beneficial owner using the Register of Enterprises, adding a customer declaration or other sources based on risk (Section 18(3)). A mismatch must be reported to the register within three working days (Section 18(3.1)). Since 1 July 2026 companies must also hold and register the extent of each beneficial owner's control, such as ownership and voting percentages (Sections 18.1(4) and 18.2). For members, shareholders and sole traders the Register of Enterprises fills it in by 31 December 2026; other entities submit it with their next beneficial owner update. From 5 October 2026 to 9 July 2027 the Register shows only the total extent, not the breakdown per intermediate entity.

Enhanced due diligence triggers

Section 22 requires EDD for customers not physically present at identification (unless the conditions in section 5 below are met), politically exposed persons, correspondent relationships, transfers to or from self-hosted crypto addresses, and other higher-risk

cases. Dealing with shell banks is prohibited (Section 21). Regulation No. 316 requires automated screening of customers, beneficial owners, representatives and shareholders against sanctions and politically exposed person lists before onboarding and at least daily afterwards (point 44.6).

Reporting and retention

- **Suspicious transactions**: reported to the Financial Intelligence Unit without delay through its electronic system (Section 31.4). A bank that refrains from a suspicious transaction must report by the next working day (Section 32).
- **Threshold declarations**: under Cabinet Regulation No. 550 (2021), payment service providers, a category that includes banks (Law on Payment Services and Electronic Money, Section 2(2)), file a declaration for cash transactions of EUR 7,000 or more and cross-border payments of EUR 500,000 or more; cash foreign-exchange purchases or sales of EUR 5,000 or more are also declared (point 14).
- **Retention**: five years after the relationship ends, which the Financial Intelligence Unit, supervisors or law enforcement may extend by up to five years (Section 37).

4 Identity verification and onboarding

Section 12 of the AML Law sets the identification data. For residents: name, surname and personal identity code. For non-residents: name, surname, date of birth, photograph, document number and date of issue, and issuing country and authority. A non-resident who visits in person must present a document valid for entry into Latvia; one identified remotely may use a domestic passport or another document recognised by their home country (Section 12(3)). In every case the bank must check that the document is not in the Register of Invalid Documents (Section 12(3.1)).

Remote identification is governed by Cabinet Regulation No. 392 (2018, as amended 2022), which permits four methods, chosen on a risk basis (point 7):

- a secure (eIDAS qualified) electronic signature, qualified increased security electronic identification under the Fizisko personu elektroniskās identifikācijas likums (Law on Electronic Identification of Natural Persons), or solutions usable in Latvia under the eIDAS Regulation (EU) No 910/2014;
- real-time video identification;
- identity data obtained from a credit or payment institution through an identification payment or similar method;
- comparison of a photo of the identity document with a selfie.

For video and document-plus-selfie methods the bank must check the document's remotely verifiable security features and carry out biometric recognition and comparison (point 9). The document must have a machine-readable zone that is actually read, optical security features such as holograms, and forgery detection must be applied (point 11).

Latvijas Banka's AML handbook (March 2026, section 5.10) adds the EBA remote onboarding guidelines (EBA/GL/2022/15): banks must show video or selfie capture is live, treat chip data as most reliable, and check that foreign qualified e-signatures come from eIDAS qualified providers.

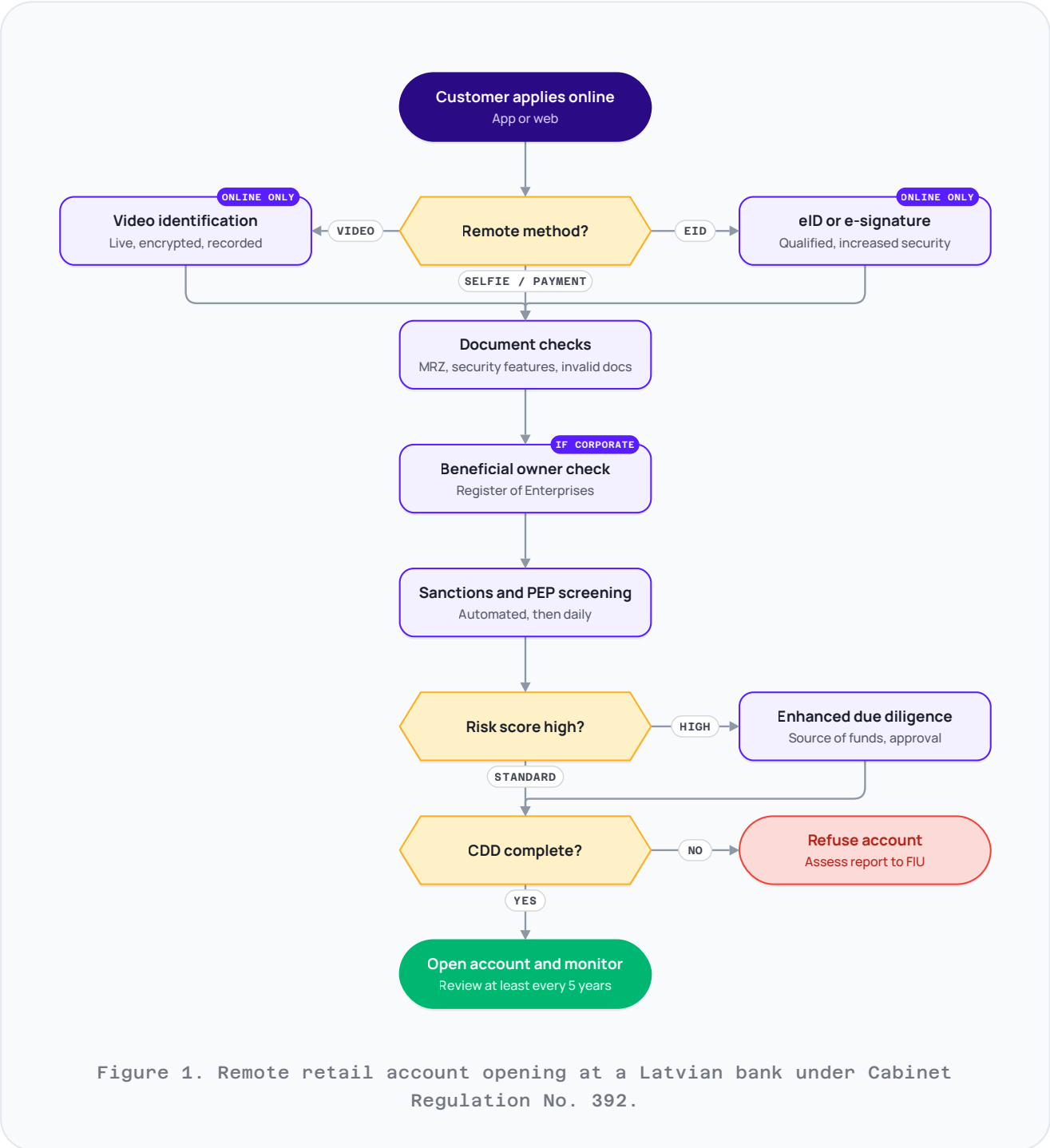


Figure 1. Remote retail account opening at a Latvian bank under Cabinet Regulation No. 392.

Reliance and outsourcing. Remote identification may be outsourced to a provider that applies EU AML standards and is monitored by the bank (Regulation No. 392, point 6). Banks may accept CDD results from other EU or equivalent institutions but remain liable (AML Law, Section 29). Agents identifying customers for the bank fall under Latvijas Banka Regulation No. 351 (2024), which excludes technical remote identification providers that meet Regulation No. 392 (point 2.2).

5 Digital channels: what's different

> **Bottom line:** remote onboarding is a statutory EDD trigger in Latvia unless the bank uses one of the four methods in Cabinet Regulation No. 392 and has risk controls in place.

Requirement	In person / branch	Online / remote	Difference
Risk treatment	Standard CDD	EDD unless Regulation No. 392 method and controls are used	Differs
Accepted methods	Physical identity document	eID or e-signature, video, identification payment, document plus selfie	Differs
Non-resident documents	Document valid for entry into Latvia	Home-country domestic passport or recognised ID also accepted	Differs
Document copies and evidence	Copy of the identity document	Image or video counts as the copy; timestamped audit trail with IP address	Differs
High-risk or low-tax country links	EDD (mandatory for high-risk third countries)	Payment-based and selfie methods prohibited	Differs
Liveness	Customer physically present	Proof that video or selfie is captured live	Differs
Account access	Not applicable at the counter	Strong customer authentication for online access and payments	Differs

Invalid documents check	Required	Required	Same
Record retention	5 years after relationship ends	5 years, including video and audio streams	Same

The EDD default and how to avoid it

Section 22(2)(1) of the AML Law makes EDD mandatory for customers not present in person, unless the bank has risk-mitigating policies and trained staff and identifies the customer by the technological means set by the Cabinet. Regulation No. 392 adds a documented risk assessment, customer information about the process, and security requirements for the technology (point 2).

Video identification standard

Video identification must be real-time with synchronised, encrypted audio and video; the face must be compared with the document photo, be uncovered and clearly lit; the agent must ask verification questions; and the stream must be uninterrupted, or the session repeated (point 10). An automated stream that falls short counts only as a supporting control (point 10.1).

Limits on the lighter methods

The identification payment and document-plus-selfie methods are not available where the customer or beneficial owner is linked to a high-risk third country or a low-tax or no-tax jurisdiction (point 12). Where in-person identification is not used, Section 23 of the AML Law also lets the bank require the first payment to come from an account in the customer's name at an EU-regulated credit institution.

Account security and branch access

Once the account is open, strong customer authentication with two independent factors is required for online account access, payment initiation and other risky remote actions (Maksājumu pakalpojumu un elektroniskās naudas likums, Law on Payment Services and Electronic Money, Section 104.4). Since 1 January 2026 banks serving consumers through a Latvian entity or branch must also offer at least two ways to apply, account for customers without electronic identification, and price in-person and remote services by actual cost (Credit Institutions Law, Section 73.2). Banks holding at least 5% of Latvian payment accounts and household deposits must provide in-person identification in specified cities.

Pending: the EU Anti-Money Laundering Regulation (EU) 2024/1624 `Adopted, applies 10 Jul 2027` allows verification through eIDAS electronic identification at assurance level "substantial" or "high" or relevant qualified trust services (Article 22(6)).

6 Data protection and biometrics

The General Data Protection Regulation (EU) 2016/679 applies in full. Face matching in remote onboarding processes biometric data for the purpose of uniquely identifying a person, a special category whose processing is prohibited unless an Article 9(2) exception applies. The AML Law states that processing personal data for AML purposes is carried out in the public interest (Section 5.2(1)). CDD data may be used only to prevent money laundering and terrorism and proliferation financing; use for any other purpose, including commercial purposes, is prohibited (Section 11.1(8)).

Remote identification data must be unalterable and video and audio kept for the retention period, unless video identification is combined with a qualified e-signature or eID and the images are kept (Regulation No. 392, point 16). Licensed shared CDD tools (Sections 17.1 to 17.3) are licensed and supervised by the Data State Inspectorate; data on natural-person customers may be shared through an open tool only with their consent.

7 Sector-specific obligations

Correspondent banking

Correspondent relationships need an assessment of the respondent's licence, reputation and AML controls, board approval and documented responsibilities, and are barred with institutions that serve shell banks (AML Law, Section 24).

Risk-based approach, not de-risking

A February 2024 national strategy targets banks refusing whole customer categories instead of applying a risk-based approach, and Latvijas Banka's 2026 supervision priorities stress access to financial services. From 15 October 2026, balances of terminated customers other than Latvian-resident individuals pass to the State if unclaimed for five years (AML Law, Section 43(2.1)).

Sanctions risk systems

Regulation No. 316 requires automated screening of payments, including the payment purpose, against sanctions lists, with matches stopped or blocked (point 44). Since 1 April 2024 the Financial Intelligence Unit decides on sanctions exemptions; Latvijas Banka supervises sanctions-risk controls.

8 Risk indicators and red flags

BANKING INDICATORS FROM THE FINANCIAL INTELLIGENCE UNIT TYPOLOGIES (2024)

- **Transit accounts**: funds transferred onward or withdrawn in cash shortly after arrival.
- **No economic link to Latvia**: account opened in a country that is neither the customer's residence nor place of business.
- **Nominee control**: company controlled by a person holding similar posts in many other companies, with no relevant experience.
- **Shared identifiers**: counterparties linked by the same board member, address, phone number or IP address.
- **Payment recalls**: several payment recall requests received on one account, a fraud indicator.
- **Impersonation scams**: customer told by a supposed police officer or bank employee to transfer funds urgently.

9 Enforcement and penalties

Section 78 of the AML Law lets Latvijas Banka issue public statements and warnings, suspend or revoke a licence, ban responsible persons and order corrective action. For credit and financial institutions, fines reach 10% of total annual turnover, or up to EUR 5 million where 10% is lower; individuals responsible face fines up to EUR 5 million (Section

78(3)). Sanctions are published, and decisions can be appealed to the Administrative Regional Court (Section 79).

- 6 December 2023: AS LPB Bank (now AS Magnetiq Bank) fined EUR 2,016,342 under an administrative agreement for internal control, CDD, transaction monitoring and reporting failings (Latvijas Banka).
- 12 December 2023: AS Reģionālā investīciju banka fined EUR 259,867 for weak due diligence of high-risk customers and transaction monitoring (Latvijas Banka).
- 26 March 2024: the former Chair of Baltic International Bank SE personally fined EUR 31,731 for internal control and AML risk management breaches (appealed; upheld by the Council of Latvijas Banka).
- 20 December 2024: Signet Bank AS received a warning for AML breaches.

All four appear in Latvijas Banka's sanctions register, which lists AML sanctions against these four credit institutions. MONEYVAL's mutual evaluation, published on 19 February 2026, found significant progress in risk-based banking supervision since the previous evaluation and placed Latvia in regular follow-up.

10 Recent changes and what to watch

- **10 Jul 2027** `Adopted, applies 10 Jul 2027` EU Anti-Money Laundering Regulation (EU) 2024/1624 becomes directly applicable, with a EUR 10,000 cap on cash payments for goods and services; national rules will need to be realigned.
- **1 Jul 2027** `Adopted, starts by 1 Jul 2027` AMLA begins its first selection of high-risk banks and financial institutions active in at least six Member States for direct EU supervision.
- **1 Jan 2027** `Adopted, effective 1 Jan 2027` AML supervision of licensed consumer lenders moves from the Consumer Rights Protection Centre to Latvijas Banka.
- **15 Oct 2026** `In force` AML Law amendments: unclaimed balances of terminated customers who are not Latvian-resident individuals pass to the State after five years.
- **1 Oct 2026** `Final draft, not adopted` AMLA sent the Commission its final draft standards (RTS) on customer due diligence under Article 28(1) of the AML Regulation (report of 30 September 2026). Draft Article 7 allows remote document-based checks only as a fallback: the customer cannot reasonably present an identity document in person and has no eIDAS means at "substantial" or "high" level or relevant qualified trust service; the firm must justify it and meet listed safeguards. Proposed to apply six months after entry into force.

- **1 Jul 2026** `In force` The duty to register the extent of each beneficial owner's control applies; from 5 October 2026 to 9 July 2027 the Register of Enterprises shows only the total control extent, not the breakdown per intermediate entity.
- **11 Mar 2026** `In force` Latvijas Banka's AML and sanctions handbook adds a remote identification section that applies the EBA remote onboarding guidelines, including live-capture checks.
- **6 Jan 2026** `In force` EUR 1 million minimum initial capital for specialised credit institutions, including digital-only banks.

11 What this means for identity verification

- **Method selection**: build to one of the four Regulation No. 392 methods; anything else leaves remote customers in mandatory EDD.
- **Document checks**: read the machine-readable zone or chip, check security features and the Register of Invalid Documents.
- **Biometrics and evidence**: face matching with live-capture checks for video and selfie flows; keep timestamped images or streams with the IP address.
- **Country routing**: send customers linked to high-risk or low-tax jurisdictions to video, eID or in-person identification.
- **Re-verification**: refresh CDD at least every five years; rescreen sanctions and PEP lists daily.
- **AMLA draft RTS**: if adopted as drafted, remote document checks become a justified fallback for customers without in-person or eIDAS options.
- **Fallback**: retail banks serving Latvian consumers need a non-digital route for customers without electronic identification.

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 identity verification with ID document capture, machine-readable zone and security feature checks, face match and biometric liveness.
- Video KYC with recorded, timestamped sessions for live video identification flows.
- KYB and beneficial owner verification for corporate customers.
- AML screening against sanctions, PEP and adverse-media lists at onboarding and through ongoing monitoring.
- No-code workflow builder to route customers to different identification methods based on risk and country.

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), Sections 5.2, 11, 11.1, 12, 18, 18.1, 18.2, 21 to 25, 25.1, 29, 31.4, 32, 37, 42, 43, 45, 77 to 79, version in force from 15 October 2026, likumi.lv
- **Kredītiestāžu likums** (Credit Institutions Law), Sections 1, 3, 11, 12.1, 14 to 16, 21, 33.15, 73.1, 73.2 (Section 1(73) and Section 21 as amended by the law of 11 December 2025, in force 6 January 2026), likumi.lv
- **Ministru kabineta noteikumi Nr. 392** (Cabinet Regulation No. 392), remote customer identification, 3 July 2018, as amended by Regulation No. 331 of 7 June 2022, likumi.lv

- **Ministru kabineta noteikumi Nr. 550** (Cabinet Regulation No. 550), suspicious transaction reports and threshold declarations, 17 August 2021, point 14, likumi.lv
- **Latvijas Bankas noteikumi Nr. 316** (Latvijas Banka Regulation No. 316), customer risk, due diligence and IT requirements, 17 September 2024, likumi.lv
- **Latvijas Bankas noteikumi Nr. 351** (Latvijas Banka Regulation No. 351), cooperation with third parties for customer identification, 25 November 2024, likumi.lv
- **Latvijas Bankas noteikumi Nr. 259** (Latvijas Banka Regulation No. 259), credit institution licensing, 27 November 2023, likumi.lv
- **Maksājumu pakalpojumu un elektroniskās naudas likums** (Law on Payment Services and Electronic Money), Sections 2 and 104.4, likumi.lv
- **Vadlīnijas noziedzīgi iegūtu līdzekļu legalizācijas ... novēršanas un sankciju riska pārvaldīšanas iekšējās kontroles sistēmas izveidei un klientu izpētei** (AML handbook), Latvijas Banka, March 2026, section 5.10, bank.lv
- **Guidelines on the use of Remote Customer Onboarding Solutions** (EBA/GL/2022/15), European Banking Authority, 22 November 2022, applicable from 2 October 2023, eba.europa.eu
- **MONEYVAL commends Latvia for significant progress in strengthening its AML/CFT/CPF framework**, Council of Europe, 19 February 2026, coe.int
- **Elektronisko dokumentu likums** (Electronic Documents Law), Section 1, point 2 (secure electronic signature), likumi.lv
- **Patieso labuma guvēju īstenotās kontroles veida un apjoma reģistrācija no 2026. gada 5. oktobra** (Registration of the type and extent of beneficial owners' control), Register of Enterprises, 5 October 2026, ur.gov.lv
- **Noguldījumu garantiju likums** (Deposit Guarantee Law), Section 3, likumi.lv
- **Regulation (EU) 2024/1624** (Anti-Money Laundering Regulation), Articles 22, 77, 80 and 90, eur-lex.europa.eu
- **Regulation (EU) 2024/1620** establishing the Anti-Money Laundering Authority, Articles 12 and 13, eur-lex.europa.eu
- **Final Report: Draft Regulatory Technical Standards under Article 28(1) of Regulation (EU) 2024/1624**, Anti-Money Laundering Authority, 30 September 2026, draft Articles 7 and 29, amla.europa.eu; press release "AMLA finalises key standards for the private sector", 1 October 2026, amla.europa.eu
- **Skaidrojums par grozījumiem Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likumā attiecībā uz patiesā labuma guvēja valstspiederību un kontroles apjomu** (Explanation of amendments on beneficial owners' nationality and extent of control), Register of Enterprises, 1 July 2026, ur.gov.lv
- **Regulation (EU) 2016/679** (General Data Protection Regulation), Article 9, eur-lex.europa.eu
- **Noziedzīgi iegūtu līdzekļu legalizācijas tipoloģijas un pazīmes** (Money laundering typologies and indicators), 3rd edition, 2024, Financial Intelligence Unit, fid.gov.lv

- **Sanctions**, exemptions competence transferred to the Financial Intelligence Unit from 1 April 2024, Latvijas Banka, updated 10 July 2024, bank.lv
- **Latvia's financial market supervision priorities**, Latvijas Banka, 6 January 2026, bank.lv
- **Papildinātas vadlīnijas noziedzīgi iegūtu līdzekļu legalizācijas novēršanai un sankciju riska pārvaldīšanai** (Supplemented AML and sanctions risk guidelines), Latvijas Banka, 11 March 2026, bank.lv
- **Finanšu sektors kļūs godprātīgiem klientiem draudzīgāks** (Financial sector to become friendlier to law-abiding customers), Latvijas Banka, 6 February 2024, bank.lv
- **Enforcement notices**: AS LPB Bank, now AS Magnetiq Bank (6 December 2023) and AS Reģionālā investīciju banka (12 December 2023), Latvijas Banka; sanctions register, credit institutions segment (Baltic International Bank SE, 26 March 2024; Signet Bank AS, 20 December 2024), bank.lv