Identomat

COMPLIANCE GUIDE

Government & Public Services Compliance in Latvia

COUNTRY Latvia

INDUSTRY Government & Public Services

LAST UPDATED 5 November 2026

KEY REGULATORS Ministry of Smart Administration and Regional Development · Supervisory Committee of Digital Security · Office of Citizenship and Migration Affairs

Key takeaways

- Latvia's public services run on a state-backed digital identity: the national eID card, the eParaksts tools and Smart-ID all let a person prove who they are online with the same legal effect as showing an identity document in person.
- Any business or public body that offers an online service with electronic login must let people use any national electronic identification tool (the eID card or eParaksts), unless technical compatibility rules it out.
- A high-trust digital identity still starts face to face: the first qualified credential (normally the eID card) is issued only after an in-person document check. With that card, people can then set up further credentials, such as the eParaksts mobile app, remotely.
- From 1 December 2026, signing certificates on about 346,000 eID cards are being revoked and replaced by a remote signing service; login with those cards keeps working, but systems that sign with eID cards must be adapted.
- Latvia must offer a European Digital Identity Wallet (a state-recognised phone app for identity and signatures) by 24 December 2026. Larger private firms that must use strong online authentication will have to accept it by 24 December 2027.

The public sector is open to online delivery and largely built for it: identity documents, the state services portal Latvija.gov.lv and the official electronic address (e-address) are built around qualified electronic identity. Government bodies are not obliged entities under the anti-money laundering law, so the rules that matter are the Law on Electronic Identification of Natural Persons, the Personal Identification Documents Law and the Electronic Documents Law, together with the EU eIDAS Regulation.

The principal authorities are the Ministry of Smart Administration and Regional Development (policy and eIDAS 2.0 implementation), the State Digital Development Agency (portal, e-address and wallet project), the Supervisory Committee of Digital Security (supervisor of qualified identity providers) and the Office of Citizenship and Migration Affairs (identity documents). The biggest constraint for a new entrant is that only people in the Natural Persons Register can hold a qualified Latvian eID. Non-residents can obtain a foreigner's eID card but must collect it in person; otherwise foreign users rely on other EU countries' notified schemes or service-specific routes.

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

Authority	Remit	Level	Official site
Viedās administrācijas un reģionālās attīstības ministrija (Ministry of Smart Administration and Regional Development, VARAM)	Lead ministry for public services, digital transformation and state digital technology; coordinates digital identity and wallet implementation	National	Cabinet Regulation No. 586
Valsts digitālās attīstības aģentūra (State Digital Development Agency, VDAA)	Runs the state services portal, the e-address system and the national eIDAS gateway; leads the wallet project	National	Cabinet Regulation No. 375
Digitālās drošības uzraudzības komiteja (Supervisory Committee of Digital Security)	Registers and supervises qualified electronic identification providers; eIDAS supervisory body for trust services; notifies Latvian eID schemes to the European Commission	National (Ministry of Defence)	cyber.gov.lv
Nacionālais kiberdrošības centrs (National Cybersecurity Centre)	Supervises cybersecurity duties of public bodies and other essential entities; provides the committee's secretariat	National (Ministry of Defence)	National Cybersecurity Law

Pilsonības un migrācijas lietu pārvalde (Office of Citizenship and Migration Affairs, PMLP)	Issues identity cards and passports; controller of the Personal Identification Documents Information System	National	pmlp.gov.lv
Datu valsts inspekcija (Data State Inspectorate, DVI)	Supervisory authority under the General Data Protection Regulation (GDPR); oversees the state biometric data system	National	Personal Data Processing Law
Financial Intelligence Unit of Latvia (Finanšu izlūkošanas dienests, FIU Latvia)	Receives suspicious-transaction information that state bodies must report	National	AML/CTPF Law
European Commission	eIDAS implementing acts; publishes the list of notified eID schemes	Supranational (EU)	eur-lex.europa.eu

The state-owned Latvian State Radio and Television Centre (LVRTC) is not a regulator but the qualified provider behind eID card certificates and eParaksts.

2 Licensing and authorisation

Public bodies need no licence to deliver online services. The authorisation that matters is the status of **qualified** or **qualified increased security** electronic identification provider under the Fizisko personu elektroniskās identifikācijas likums (Law on Electronic Identification of Natural Persons, the eID law). Only identification carried out with these credentials is automatically treated as equivalent to an in-person document check (Section 3(3)).

Registration

A provider files its service terms, a security description, an audit opinion from an approved expert, proof of insurance and a compliance declaration (Section 8(1)). The supervisor decides within one month, extendable by up to two months (Section 8(2) and (3)).

Ongoing conditions

Liability insurance (Section 12) and an annual security audit (Section 17(4)). Qualified providers must host systems and data in the EU or EEA; qualified increased security providers must host them in Latvia (Cabinet Regulation No. 560, points 4 and 5).

Who is registered

The committee supervises two providers. Its register lists LVRTC as a qualified increased security provider (since 13 December 2018) for the eID card, eParaksts karte, eParaksts karte+ and eParaksts, and the Latvian branch of SK ID Solutions AS as a qualified provider (since 18 May 2023) for Smart-ID.

Non-qualified identity services count as equivalent to an in-person check only where the parties have agreed that method in writing (Section 3(3)(2) and (3)). Service providers must regularly check that the qualified providers they rely on remain on the register (Section 19(1)(5)). The same committee supervises and approves trust service providers (Cabinet Regulation No. 695, points 1.2 and 2.3).

3 Identity framework (AML rules do not apply)

State institutions are not 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). They must report suspicious transactions to FIU Latvia (Section 3.1) and supply information it requests (Section 54), but there is no customer due diligence regime for citizens using public services.

Identity is governed instead by the eID law, the Personu apliecinošu dokumentu likums (Personal Identification Documents Law), the Elektronisko dokumentu likums (Electronic Documents Law) and eIDAS as amended by Regulation (EU) 2024/1183.

The government scheme also anchors private-sector remote onboarding: under the AML law, a non-face-to-face customer triggers enhanced due diligence unless the entity has

risk controls in place and uses the identification methods set by the Cabinet (Section 22(2)(1)). Cabinet Regulation No. 392 lists qualified electronic signatures and qualified increased security electronic identification first among those methods (point 7.1).

4 Identity verification and onboarding

Documents

The identity card (eID card) has been the mandatory identity document for Latvian citizens and non-citizens aged 15 and over since 1 May 2023; people who held only a passport on 30 April 2023 may keep using it until it becomes invalid (Personal Identification Documents Law, Section 9(1) and transitional provision 5). Its chip holds the data for qualified increased security electronic identification and qualified electronic signatures, and is a valid means of proving identity for electronic services (Section 5(4) and (5)). For third-country nationals the residence permit is the identity card (Section 5(2)). Non-residents can obtain a foreigner's eID card: they can register in the Natural Persons Register remotely with a questionnaire signed with a qualified electronic signature, then collect the card at a PMLP office or one of 18 designated Latvian embassies for a EUR 170 state fee (PMLP; Ministry of Foreign Affairs).

Two national assurance tiers

A **qualified** eID credential must meet the EU technical specifications for at least the "substantial" assurance level, and a **qualified increased security** credential those for "high" (Cabinet Regulation No. 560, points 7.1 and 8.5, referring to Implementing Regulation (EU) 2015/1502). Authentication needs at least two factors, encrypted single-use sessions and mutual recognition (point 6).

Proofing and data checks

Before issuing a qualified credential, the provider must verify the person's identity in their presence on the basis of an identity document (Law on Electronic Identification of Natural Persons, Section 5(2); Regulation No. 560, point 3.4). The provider may contract these steps out but keeps full liability (Section 5(5)). Once a person holds an eID card, further credentials can be added remotely: LVRTC lets card holders sign the eParaksts mobile contract by reading the card's chip with its eID Scan phone app; without a card, the contract is signed in person via courier (eparaksts.lv). At each authentication the person's data must be checked against the Natural Persons Register using data no older than 24 hours (Section 7(8)); qualified increased security providers must refresh validity information immediately (Regulation No. 560, point 11.4). The provider then gives the

service an authentication statement naming the person, their personal code and the time (Section 4).

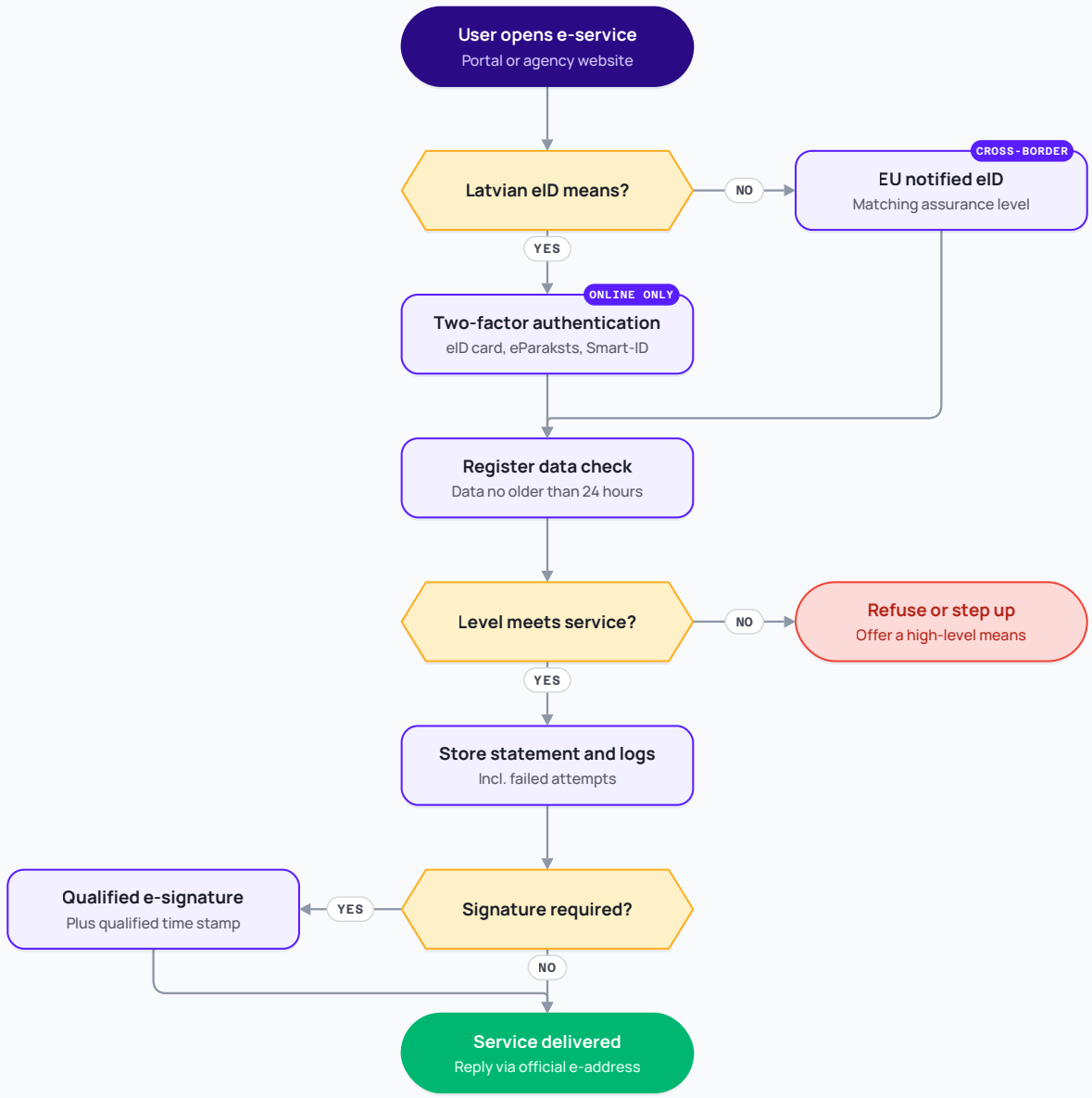


Figure 1. Online access to a Latvian public e-service with electronic identification.

Who can hold a qualified Latvian eID

Qualified and qualified increased security services cover only people included in the Natural Persons Register; anyone else is identified under the rules of the specific service (Section 2(2)). The state portal's login module offers the eID card, eID Scan and eParaksts mobile (qualified increased security), Smart-ID (qualified) and eIDAS login. Individual systems differ: the tax authority's declaration system also accepts certain internet-bank logins and, since 1 January 2026, keeps passwords only for foreigners who cannot obtain a

foreigner's eID card and for customs-system users (State Revenue Service). For cross-border access, Latvia accepts eID schemes that other EU states have notified, at the assurance level the service requires (Section 21). Latvia's own scheme (eID karte, eParaksts karte, eParaksts karte+ and eParaksts) has been on the EU list of notified schemes since its publication on 18 December 2019 (OJ C/2024/7543).

5 Digital channels: what's different

Bottom line: online identification with a qualified Latvian eID has the same legal effect as showing an identity document in person, but the first qualified credential must be issued after a face-to-face identity check.

Requirement	In person	Online / remote	Difference
Legal effect of identification	Identity document presented	Qualified or qualified increased security eID equals an in-person document check	Same
Initial identity proofing	Document check at issuer	First qualified credential needs an in-person check; later credentials can be added remotely with the eID card	Differs
Accepted credentials	Identity card, passport	State login: eID card, eID Scan, eParaksts mobile, Smart-ID, EU eIDAS login	Differs
User's choice of credential	Any valid identity document	Service must accept any national eID means, subject to technical compatibility	Differs
Assurance level	Visual document inspection	Substantial or high, matched to the service	Differs
Checks at each use	Document validity inspected	Register data no older than 24 hours checked at every authentication	Differs

Document-and-selfie checks	Not used	Not offered by the state login module; AML obliged entities may use them under Cabinet Regulation No. 392	Differs
Signed documents to and from public bodies	Handwritten signature	Qualified e-signature plus qualified time stamp	Differs
Evidence kept	Application records	Authentication statements and failed-attempt logs	Differs
Biometric capture	Face image and fingerprints taken when a document is issued	No access to the state biometric system for private relying parties	Differs
Data protection	GDPR and Personal Data Processing Law	GDPR and Personal Data Processing Law	Same

Relying parties must accept every national eID means

Since 1 February 2023, any provider of an electronic service in Latvia that uses electronic identification, private or public, must let users identify with any national eID means, as far as technical compatibility in ordinary use allows (Law on Electronic Identification of Natural Persons, Section 19(1.1)). Restrictive contract terms are void (Section 3(4)); national eID means are free (Section 14(2)).

Public bodies have connection and fallback duties

Public bodies must connect e-services to a qualified identification service within a year of that provider's registration (Section 19(2)) and, where interoperability blocks the national eID, let people obtain the credential they need remotely (Section 19(4)).

Signatures carry an extra step

In document exchange with state and municipal bodies, an electronic document counts as signed when it bears a qualified electronic signature and a time stamp, or an electronic signature the parties agreed in writing to use (Electronic Documents Law, Section 3(5)).

6 Data protection and biometrics

The GDPR applies with the Fizisko personu datu apstrādes likums (Personal Data Processing Law): biometric data for unique identification needs a GDPR Article 9(2) ground or a regulatory enactment under Article 9(4) (Section 25(2)).

The Biometrijas datu apstrādes sistēmas likums (Biometric Data Processing System Law) creates a state information system holding facial images and, where obtainable, fingerprint images collected mainly when identity documents, seafarers' documents and driving licences are issued (Sections 5 and 6). Access is limited to listed authorities such as the State Police, the State Border Guard, PMLP, courts and emergency hospitals, plus other public bodies where a regulatory enactment provides for it (Section 14(1)); private relying parties are not on the list. The Interior Digital Centre runs the system (Cabinet Regulation No. 335, point 9; Cabinet Regulation No. 234, point 12). The DVI supervises it (Section 16).

Qualified identification providers keep audit records of authentication statements and failed attempts for five years (Law on Electronic Identification of Natural Persons, Section 14(1)(13)) and must report breaches to the supervisor, the DVI and the person (Section 14(1)(17)).

7 Sector-specific obligations

Official electronic address

The Oficiālās elektroniskās adreses likums (Official Electronic Address Law) makes the e-address mandatory for state institutions and for every entity in the Enterprise Register, as well as for some defence personnel and male citizens aged 18 to 27 (Section 5(1)). Natural persons aged 14 and over may use it voluntarily (Section 5(2)). An e-address is created by logging in to Latvija.gov.lv with a qualified eID means (Section 7(2)).

Remote eID signature transition

The Cosmo 8.1 chip's certification as a qualified signature creation device ends on 9 December 2026. PMLP has announced that signing certificates on affected cards will be revoked from 1 December 2026 and replaced by LVRTC's "Attālināts eID paraksts" (remote eID signature), which creates the qualified signature remotely with a short-lived certificate valid for 15 minutes after the user authenticates with the card (PMLP notice, updated 4 November 2026). Cabinet Regulation No. 646 of 27 October 2026, in force from 1 December 2026, lets the card's authentication certificate be used to apply for this service. Identification with these cards continues; eID card signing integrations must be adapted.

Cybersecurity duties

Under the Nacionālās kiberdrošības likums (National Cybersecurity Law), state institutions (other than state security bodies) and derived public persons such as municipalities are essential service providers (Section 20(5) and (6)). After a significant incident they must send an early warning within 24 hours and an initial report within 72 hours (Section 34(2) and (3)), for most public bodies to CERT.LV (Section 9(2)(2)). For qualified trust service providers the initial report is due within 24 hours. The law's fines do not apply to public bodies (Section 46(12)).

Wallet readiness

Cabinet Order No. 483 of 13 August 2026 funds a EUR 6.5 million VDAA project to deliver a certified wallet by 24 December 2026 (Order No. 483). VARAM says the wallet will be voluntary and will not replace existing eID tools (VARAM wallet page).

8 Risk indicators and red flags

IDENTITY FRAUD AROUND LATVIAN PUBLIC E-SERVICES

- **SMS "new e-address message" links**: Latvija.gov.lv states that it never sends e-address notifications by SMS.
- **Fake agency decisions**: emails with forged State Social Insurance Agency benefit decisions seeking personal and bank data; CERT.LV lists requests to enter bank credentials or confirm with Smart-ID as warning signs (September 2026).
- **Unprompted authentication requests**: the State Revenue Service warns users not to approve login requests they did not start.
- **Phone requests for personal code and address** by callers posing as social services (CERT.LV).
- **Shared credentials**: passing eID data to others is prohibited (Law on Electronic Identification of Natural Persons, Section 18(3)).
- **Revoked credentials**: false identity information, death, a name change or a wanted-person notice requires immediate revocation (Section 6(2)).
- **Processor-side breaches**: unauthorised access to municipal databases run by an IT processor in late 2024 led to DVI reprimands for the controlling municipalities.

9 Enforcement and penalties

Identity providers. The eID law has no fines. The supervisor may terminate a qualified service and delete the provider from the register (Section 16); providers are liable for losses caused by faulty issuance or management (Section 15), and users for losses caused by false information or careless handling (Section 18(4)).

Public bodies and data protection. For unlawful processing by a public-law body, the Personal Data Processing Law provides a warning or a fine on the responsible official of up to 200 fine units (Section 38), and one fine unit is EUR 5 (Administrative Liability Law, Section 16(2)), so up to EUR 1,000 per official. The DVI also uses GDPR corrective powers and publishes violations by public bodies (Personal Data Processing Law, Section 4(2)).

Recent action. On 22 September 2025 the DVI reprimanded Valmiera municipality after attackers accessed databases of the Unified Municipal System, run by an IT processor, between 29 October and 2 November 2024. The DVI, which opened separate inspections of 45 controllers, found that the municipality had not ensured security testing of the system or supervision of the processor (GDPR Articles 28 and 32); on 20 November 2025 the DVI director upheld the reprimand (DVI decision No. 1-2.3/23-DVI); a parallel decision covers Rēzekne municipality (DVI decision No. 1-2.3/31-DVI).

10 Recent changes and what to watch

- **24 December 2027** `Applies from 24 Dec 2027` Private relying parties (other than micro and small enterprises) that must use strong user authentication must accept the wallet at the user's request (Regulation 2024/1183, Article 5f(2)).
- **10 July 2027** `Applies from 10 Jul 2027` The EU Anti-Money Laundering Regulation (EU) 2024/1624 lets obliged entities verify identity with eID means at "substantial" or "high" assurance (Article 22(6)(b)).
- **24 December 2026** `Applies from 24 Dec 2026` Deadline for each Member State to provide a European Digital Identity Wallet, 24 months after the first implementing acts took effect (Regulation 2024/1183, Article 5a(1)). Public bodies that require eID must also accept the wallet (Article 5f(1)).
- **1 December 2026** `Adopted, effective 1 Dec 2026` Cabinet Regulation No. 646 enables the remote eID signature; revocation of signing certificates on Cosmo 8.1 eID cards starts the same day. Check every eID-card signing integration.

- **30 September 2026** `In force` Amendment to the Law on Electronic Identification of Natural Persons: eID means must be revoked when a wanted-person notice is issued for someone subject to a custodial security measure (Section 6(2)(7)).
- **30 June 2026** `Bill, not enacted` The Cabinet approved for the Saeima a bill amending the Natural Persons Register Law to give third-country nationals who apply for a work visa a Latvian personal code (Ministry of the Interior). Register inclusion is the precondition for a qualified Latvian eID.

11 What this means for identity verification

- **Federate before you proof.** Offer every national eID, which equals an in-person check, and plan for the wallet; document and selfie checks suit users outside the register (Section 3(3)).
- **Map assurance levels per service** and step up lower-level credentials, including foreign ones.
- **Plan for non-registered users**: people outside the Natural Persons Register cannot hold a qualified Latvian eID.
- **Separate identification from signing**; test the remote eID signature before 9 December.
- **Keep authentication statements and failed-attempt logs** (Section 19(1)(1)).
- **Biometrics stay with the state**: private face matching needs a legal basis.

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:

- ID document capture and verification, including NFC chip reading, for users who cannot authenticate with a national eID.
- Biometric liveness and face match for remote journeys that rely on documents rather than federated eID.
- Age verification and proof of address checks configured per public-service journey.
- No-code workflow builder to route users between eID login, document checks and step-up verification, with an audit trail for each check.
- Cloud, on-premises or hybrid deployment to fit public-sector data location and hosting requirements.

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

- **Fizisko personu elektroniskās identifikācijas likums** (Law on Electronic Identification of Natural Persons), 2015, version in force from 30.09.2026, likumi.lv
- **Cabinet Regulation No. 560** (19.09.2017), technical and organisational requirements for qualified and qualified increased security eID providers, likumi.lv
- **Cabinet Regulation No. 695** (01.11.2016), Digitālās drošības uzraudzības komitejas nolikums (Statutes of the Supervisory Committee of Digital Security), likumi.lv
- **Register of qualified and qualified increased security eID providers**, Supervisory Committee of Digital Security (entries to 18.05.2023), mod.gov.lv

- **Personu apliecinošu dokumentu likums** (Personal Identification Documents Law), 2012, as amended, likumi.lv
- **Elektronisko dokumentu likums** (Electronic Documents Law), 2002, version from 06.01.2026, likumi.lv
- **Oficiālās elektroniskās adreses likums** (Official Electronic Address Law), 2016, likumi.lv
- **Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likums** (AML/CTPF Law), Sections 3.1, 22 and 54, likumi.lv
- **Cabinet Regulation No. 392** (03.07.2018), procedure for non-face-to-face customer identification, likumi.lv
- **Fizisko personu datu apstrādes likums** (Personal Data Processing Law), 2018, Sections 4, 25 and 38, likumi.lv
- **Administratīvās atbildības likums** (Administrative Liability Law), Section 16, likumi.lv
- **Biometrijas datu apstrādes sistēmas likums** (Biometric Data Processing System Law), 2009, version from 19.05.2026, likumi.lv
- **Cabinet Order No. 483** (13.08.2026) and annex, European Digital Identity Wallet implementation project, likumi.lv
- **ES Digitālās identitātes maks** (EU Digital Identity Wallet), VARAM, updated 19.03.2026, varam.gov.lv
- **Changes to e-signature use on some eID cards**, PMLP notice, published 15.05.2026, updated 04.11.2026, pmlp.gov.lv
- **Identity card (eID)**, PMLP, updated 28.07.2025, pmlp.gov.lv
- **Latvija.gov.lv**, state services portal, notice on SMS notifications, latvija.gov.lv
- **Kiberlaikapstākļi 2026, septembris** (Cyber weather, September 2026), CERT.LV, 07.10.2026, cert.lv
- **DVI decision No. 1-2.3/23-DVI** (20.11.2025), Valmiera municipality, dvi.gov.lv; **DVI decision No. 1-2.3/31-DVI** (21.11.2025), Rēzekne municipality, dvi.gov.lv
- **Cabinet Regulation No. 134 of 21 February 2012, Personu apliecinošu dokumentu noteikumi** (Personal Identification Documents Regulations), version from 01.12.2026, likumi.lv; amending **Cabinet Regulation No. 646** (27.10.2026, in force 01.12.2026), likumi.lv
- **Cabinet Regulation No. 375**, Valsts digitālās attīstības aģentūras nolikums (Statutes of the State Digital Development Agency), points 4.2, 4.26 and 4.27, likumi.lv; **Cabinet Regulation No. 586** (03.09.2024), VARAM statutes, points 1 and 5.7, likumi.lv
- **Cabinet Regulation No. 335** (16.06.2026), Iekšlietu digitālā centra nolikums (Statutes of the Interior Digital Centre), likumi.lv; **Cabinet Regulation No. 234** (biometric system rules), version from 23.09.2026, likumi.lv
- **Nacionālās kiberdrošības likums** (National Cybersecurity Law), 2024, version from 01.10.2026, Sections 3, 9, 20, 34 and 46, likumi.lv
- **Elektroniskā identifikācija** (Electronic identification), Supervisory Committee of Digital Security page, National Cybersecurity Centre, cyber.gov.lv
- **What is a foreigner's eID card**, PMLP, updated 19.02.2026, pmlp.gov.lv

- **Foreigner eID card**, Ministry of Foreign Affairs (list of 18 issuing embassies), updated 04.02.2025, mfa.gov.lv
- **eParaksts mobile** and **eID Scan**, LVRTC product pages, eparaksts.lv, eparaksts.lv
- **Vienotās pieteikšanās modulis** (single login module for Latvija.gov.lv), VDAA, login options as displayed on 05.11.2026, latvija.gov.lv
- **Elektroniskās deklarēšanas sistēma** (Electronic Declaration System) login page, security notice, State Revenue Service, eds.vid.gov.lv; **Important information for foreigners and EMDAS users about connecting to the EDS**, 07.10.2025, vid.gov.lv
- **Plānots piešķirt personas kodu ārzemniekiem, kuri pieprasa vīzas ar tiesībām uz nodarbinātību Latvijā**, Ministry of the Interior, 30.06.2026, iem.gov.lv
- **Commission Implementing Regulation (EU) 2024/2981** (OJ L, 4.12.2024), certification of European Digital Identity Wallets, EUR-Lex
- **Regulation (EU) 2024/1183** amending Regulation (EU) No 910/2014 (European Digital Identity Framework), Articles 5a and 5f, EUR-Lex
- **Commission Implementing Regulation (EU) 2024/2977** (OJ L, 4.12.2024), person identification data and attestations for wallets, EUR-Lex
- **Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No 910/2014**, OJ C/2024/7543, 20.12.2024, EUR-Lex
- **Regulation (EU) 2024/1624** (Anti-Money Laundering Regulation), Articles 22 and 90, EUR-Lex