Identomat

COMPLIANCE GUIDE

Government & Public Services Compliance in Lithuania

COUNTRY Lithuania

INDUSTRY Government & Public Services

LAST UPDATED 9 November 2026

KEY REGULATORS Communications Regulatory Authority of the Republic of Lithuania · Ministry of the Economy and Innovation · Migration Department under the Ministry of the Interior

Key takeaways

- Government bodies in Lithuania are not covered by the anti-money laundering (AML) customer checks that banks must run. Their identity rules come from the national electronic identification law and the EU eIDAS Regulation instead.
- Every public e-service must have a set login strength (an "assurance level"). Administrative e-services need at least the middle level ("substantial") unless the body sets "high", and the level must match the confidence the body would require at the counter.
- People log in to the state portal with the national ID card, a mobile e-signature, LT ID or their bank. The regulator has rated Smart-ID, Mobile-ID and the Paysera app at the highest level, but only the ID card is notified to the EU, so only the card must be accepted by other EU countries.
- Remote identity checks for qualified electronic signatures are allowed by video only if the provider reads the biometric chip of the identity document and passes an independent conformity assessment. A new EU standard (ETSI TS 119 461) applies from August 2027.
- EU Digital Identity Wallets are due by December 2026, and from December 2027 private firms (other than micro and small enterprises) that must use strong online login have to accept them. Lithuania plans its own wallet for early 2027; the law change it needs is scheduled for Seimas consideration in November 2026 but had not yet been tabled.

Lithuania runs a mature, regulated electronic identity market. The Ministry of the Economy and Innovation sets policy, the Communications Regulatory Authority (RRT) supervises trust service providers and qualified eID providers, the State Digital Solutions Agency runs the state login and eID node infrastructure, and the Migration Department puts eID and qualified signature certificates on the national identity card.

For a technology or identity provider, the market is open but gated: a Lithuanian eID means counts for public services at a given level only once RRT has assessed and assigned that level. The biggest open question is the national EU Digital Identity Wallet, which still needs national legislation.

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
Ministry of the Economy and Innovation	Sets state policy on electronic identification and trust services; manages the State Information Resources Interoperability Platform (VIISP); chairs the eIDAS 2 working group	National	eimin.lrv.lt
Communications Regulatory Authority (RRT)	Supervises trust service providers and, since 2 January 2024, qualified eID providers; assigns assurance levels; investigates administrative offences by both	National	rrt.lt
State Digital Solutions Agency (VSSA)	Manages the National Electronic Identification Information System (the national eID node) and provides VIISP services; sets the assurance-level methodology for public e-services	National	vssa.lrv.lt

Migration Department under the Ministry of the Interior	Issues identity cards and passports; creates the eID and qualified signature certificates on the ID card; issues e-resident cards; operates the Lithuanian Migration Information System (MIGRIS, migracija.lt), used for visit bookings and migration and personal document services	National	migracija.lrv.lt
Ministry of the Interior	Authority responsible for the notified Lithuanian eID scheme (identity card)	National	vrm.lrv.lt
Registers Centre	Qualified eID provider for LT ID; operates remote qualified e-signature infrastructure and the Population Register	National (state enterprise)	registrucentras.lt
State Data Protection Inspectorate (VDAI)	Supervises the General Data Protection Regulation (GDPR) and the national data protection law, including fines on public bodies	National	vdai.lrv.lt
Financial Crime Investigation Service (FNTT)	Financial intelligence unit; receives reports from state institutions on possible money laundering	National	fntt.lrv.lt
European Union (eIDAS Regulation and implementing acts)	Directly applicable rules on eID, trust services and EU Digital Identity Wallets	Supranational	eur-lex.europa.eu

2 Licensing and authorisation

Public bodies need no licence to identify people, but the identity tools they rely on are regulated. Three routes matter for providers.

Supervised and qualified eID means

A provider established in Lithuania that wants its eID means recognised as a supervised eID means must notify RRT and submit a conformity assessment report from an eID conformity assessment body (Law on Electronic Identification and Trust Services for Electronic Transactions, No XIII-1120, Article 18^1(2)). Within 3 months of complete documents (extendable by up to 20 working days), RRT either assigns one of the eIDAS assurance levels or refuses to (Article 18^1(4) and (5)). RRT's guidelines (decision TN-709 of 21 December 2023) explain how it applies Implementing Regulation (EU) 2015/1502 in that assessment.

Qualified eID providers may apply to be connected to the national eID node under VSSA's connection procedure, must keep a termination plan agreed with RRT, and must report changes to the service within 3 working days (Article 18^3).

Qualified trust services

Providers of qualified electronic signatures, seals and similar services are supervised by RRT under the eIDAS Regulation and appear on the Lithuanian trusted list. RRT's identity-verification procedure for issuing qualified certificates (decision TN-659, in force since 9 December 2023) binds them and any third party they authorise to carry out checks.

EU Digital Identity Wallet relying parties

Under Article 5b of Regulation (EU) No 910/2014 as amended by Regulation (EU) 2024/1183, any public or private relying party that intends to use EU Digital Identity Wallets must register in the Member State where it is established.

`Adopted, applies as wallets are provided` Lithuania's eIDAS 2 working group has identified the need for a national register of wallet participants and relying parties; the analysis it received in November 2025 proposed RRT as registrar.

3 Identity framework (AML rules do not apply)

State and municipal bodies are not obliged entities under the Law on the Prevention of Money Laundering and Terrorist Financing (No VIII-275). Article 2(10) lists the "other obliged entities" (auditors, bailiffs, accountants and tax advisers, notaries and lawyers, trust and company service providers, gambling and lottery companies, real estate agents, traders in precious goods and art, and others), and public authorities are not among them. The relevant provisions are unchanged in the version that applies from 1 January 2027.

Reporting to the FIU

State institutions that do not carry out criminal prosecution must inform FNTT when they notice possible money laundering or terrorist financing, breaches of the AML law and the measures taken against offenders (Article 8(1)).

Politically exposed persons list

Ministries supply FNTT with the information needed to compile and update the list of prominent public functions, within 20 working days of a written request and at least every 4 years (Article 7^{1}).

The framework that governs public services is Law No XIII-1120 (consolidated version from 18 October 2024) read with the eIDAS Regulation. Regulated private firms meet it from the other side: the AML law lets them identify a customer who is not physically present by using an EU-issued eID means under a scheme of high or substantial assurance, or a qualified electronic signature, among other methods (Article 11(1)).

4 Identity verification and onboarding

The national identity card

Under the identity card and passport issuance procedure (Order No 1V-200/V-62, consolidated version from 13 November 2025), citizens lodge applications in person, with narrow exceptions (point 10). The chip holds the holder's personal data, facial image and two fingerprints. At the request of a citizen aged 14 or over, made when applying, the card also carries an electronic identification certificate and a qualified electronic signature certificate created by the Migration Department. The card is Lithuania's only notified eID scheme ("Lithuanian eID Scheme (ATK)"), at level **high** (Commission notice C/2025/2448).

eID means supervised by RRT

eID means	Provider	Level assigned by RRT	Notified to the EU by Lithuania	RRT decision
LT ID	Registers Centre	Substantial	No	TN-637, 25 Sep 2024
Smart-ID	SK ID Solutions AS Lithuanian branch	High	No	TN-752, 7 Nov 2024
Mobile-ID	SK ID Solutions AS Lithuanian branch	High	No	TN-752, 7 Nov 2024

Paysera Mobile App	UAB Paysera LT	High	No	TN-24, 29 Jan 2026

Logging in to public e-services

Central state institutions must make their electronic services available through the E-Government Gateway, epaslaugos.lt (Government Resolution No 1659 of 16 December 2009, point 1). Under the VIISP Functioning Rules (point 18), users are identified with eID means issued or recognised in Lithuania or through the e-banking systems of banks operating in Lithuania. VIISP records the required eIDAS assurance level for every service it carries (VIISP Regulations, point 22.4.14). The Gateway's login page (checked 9 November 2026) offers three groups of options:

Login tab	Options offered
E-banking	Swedbank, SEB, Luminor, Citadele, Artea, URBO, LKU credit union group, Kreda, Rato, Paysera
E-signature	Mobile e-signature; LT ID; identity card (contactless or with a card reader); USB e-signature device; civil servant's, employee's or official's certificate
Foreigners	eIDAS (foreign notified eID); e-resident card (with a card reader or read by NFC)

Smart-ID is not offered as a separate login option on the Gateway, although RRT rates it at level high.

Choosing the assurance level

Law No XIII-1120 requires each public sector body to set an assurance level that is equivalent to the level applied when identity is established for public and administrative services (Article $18^2(1)$). A service that would require an identity document at the counter cannot accept a weaker login online. VSSA's methodology (Order No T-7(2025) of 24 January 2025) sets the working rules:

Rule	Methodology point
Users must authenticate with an eID means from a qualified eID provider at or above the level set for the service	3
Administrative e-services: at least substantial, unless the body sets high	5

The head of the body (or an authorised person) approves the level and is responsible for service security	7
If no level is set for a public or other e-service, a substantial-level means may be used	8
Reassess every two years, and within ten working days after an identity-related security incident	9
Register and investigate identity-related security incidents separately	11
Set the level separately for each service on a shared system	12
The body may score the service's risk with the methodology questionnaire; the level chosen may not be lower than the result	13 to 14

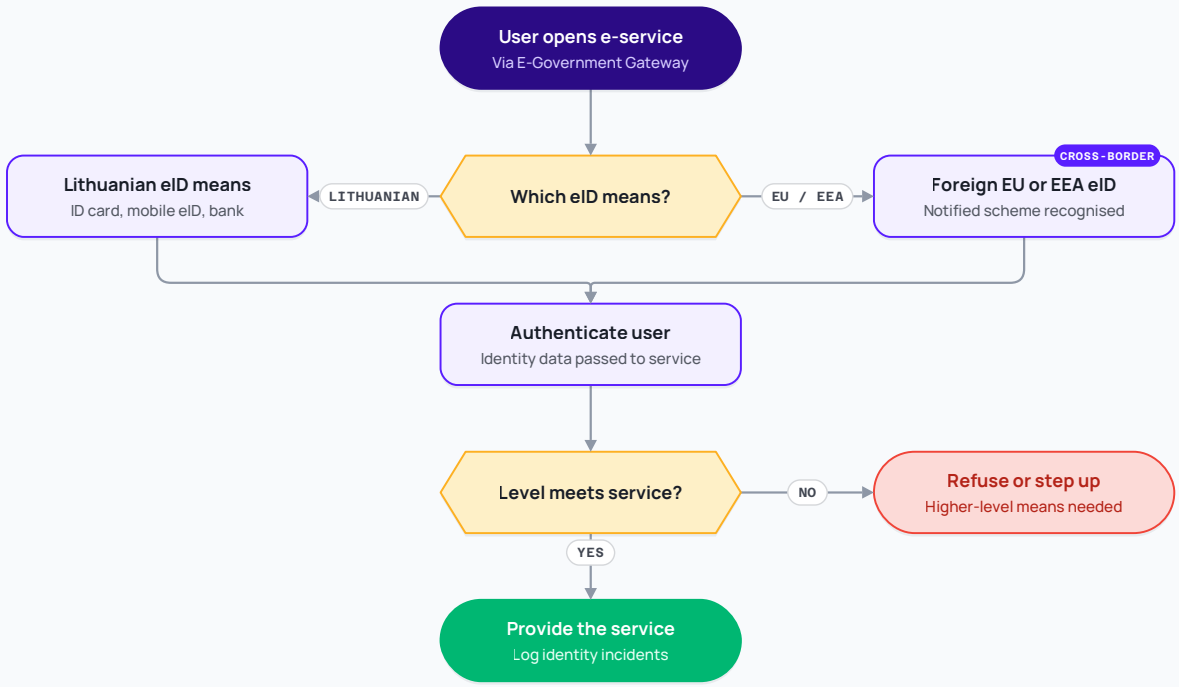


Figure 1. Online access to a Lithuanian public e-service.

Remote proofing for qualified certificates

RRT decision TN-659 allows remote identity checks before issuing a qualified certificate only with an eID means, an existing qualified certificate, or video identification (point 8). Video identification must give security equivalent to physical presence, confirmed by a conformity assessment body (point 13), and the provider must:

Requirement	Point
Use only identity documents with a chip holding biometric data that the provider can verify	14.2
Check document authenticity, face match against the document photo, and liveness; state false acceptance and false rejection rates in operational documents	14.4, 14.6
Run one uninterrupted live session over an encrypted channel, at least 1280×720 at 25 frames per second	15.1.1 to 15.1.4
Confirm with a random one-time code of at least six characters sent to the person's mobile device	15.1.5
Verify the document cryptographically through its chip	15.1.6

The decision predates the 2024 rewrite of Article 24 of the eIDAS Regulation, which is directly applicable. Article 24(1a) now permits an EU Digital Identity Wallet or a notified eID means at level high, an existing qualified certificate, other methods of high confidence confirmed by a conformity assessment body, or physical presence. Implementing Regulation (EU) 2025/1566 makes ETSI TS 119 461 V2.1.1 the reference standard.

`Adopted, applies from 19 Aug 2027`

5 Digital channels: what's different

Bottom line: the required level of confidence is the same online and at the counter, but online it is delivered through an assessed eID means, and only those with an RRT-assigned or EU-notified level count.

Requirement	In person	Online / remote	Difference
Level of identity confidence	Set for public and administrative services	Must be equivalent to the in-person level	`Same`
Evidence of identity	Established in person under the body's procedures	eID means at the level set for the service, or e-banking	`Differs`
Who vouches for the credential	The issuing authority of the document	RRT-assigned level or EU notification	`Differs`

Foreign users	Present their own documents	Notified EU and EEA eID means must be recognised	Differs
Signing a request to a public body	Handwritten signature	Qualified e-signature, scan of a signed request, or a form that identifies the sender	Differs
Obtaining the national eID	Application lodged in person (limited postal and representative exceptions); chip holds face and two fingerprints	Not available online	Differs
Proofing for a qualified certificate	Physical presence	eID means, existing qualified certificate, or video with chip and liveness checks	Differs
Personal code handling	Lawful basis needed; no publication	Same rules	Same
Reporting possible money laundering to FNTT	Applies to state institutions	Applies regardless of channel	Same

Written requests submitted online

Under the Rules for Examining Persons' Requests and Complaints in Public Administration Entities (Government Resolution No 875, consolidated from 3 September 2022, point 24.5), a request sent electronically must carry a digital copy of the signed request, a qualified electronic signature, or be submitted in a form that lets the body identify the sender or verify authenticity.

Mandatory recognition of foreign eID

eID means issued in other EU Member States under the eIDAS requirements and included in the list of eID schemes are recognised by entities providing electronic services in Lithuania (Law No XIII-1120, Article $18^2(2)$). Once wallets are provided, wherever eID is required to access a public sector body's online service, EU Digital Identity Wallets must also be accepted (eIDAS Article 5f(1)). The wallet deadlines run from 24 December 2024, when the implementing acts adopted under Article 5a(23) (Implementing Regulations (EU)

2024/2977, 2024/2979, 2024/2980 and 2024/2982) and Article 5c(6) (Implementing Regulation (EU) 2024/2981) entered into force. `Adopted, wallets due by Dec 2026`

Private sector acceptance

Private relying parties, except micro and small enterprises, that must use strong user authentication by law or contract (including transport, energy, banking, financial services, social security, health, postal services, education and telecommunications) must accept EU Digital Identity Wallets at the user's request within 36 months of the wallet implementing acts taking effect (Article 5f(2)). `Adopted, applies from Dec 2027`

6 Data protection and biometrics

The GDPR applies, supplemented by the Law on Legal Protection of Personal Data (No I-1374, consolidated version from 30 June 2026), which VDAI supervises.

- **Personal code.** The personal identification code may be processed only on a lawful basis under Article 6(1) GDPR, may not be published and may not be used for direct marketing (Article 3). A signature certificate may include it where its intended use requires (Law No XIII-1120, Article 14).
- **Children.** A child's own consent to information society services is valid from age 14 (Article 6), the same age from which the ID card can carry eID certificates.
- **Biometrics.** Biometric data processed to uniquely identify a person is a special category under Article 9(1) GDPR. Facial images and fingerprints are captured for the ID card chip; video identification for qualified certificates adds face matching and liveness checks, so providers need an Article 9(2) condition.
- **Wallet data.** Wallets must support interfaces that let users ask a relying party to erase personal data and report a relying party to the data protection authority for a suspicious request (eIDAS Article 5a(5)(a)).

7 Sector-specific obligations

Preparing for the EU Digital Identity Wallet

An inter-institutional working group set up by Order No 4-45 of the Minister of the Economy and Innovation (in force from 3 February 2026) coordinates eIDAS 2 implementation. At its meeting of 26 November 2025 it recorded the aim of offering a national wallet ("EUDIW LT") to residents by the end of 2026 and the need to amend Law No XIII-1120 and related acts.

The analytical study presented at that meeting set a timeline of drafting by the ministry and VSSA in the second quarter of 2026, Government approval in the third and Seimas adoption in the fourth, with live use from early 2027. The Seimas autumn 2026 session work programme (Resolution No XV-1194 of 22 September 2026, item 21) includes a Government bill amending Law No XIII-1120 to implement the European Digital Identity framework, assign responsibility for the wallet system, set the rights and duties of wallet ecosystem participants and update trust services rules, with consideration planned for November 2026. As of 9 November 2026 the bill had not yet been registered.

`Planned bill, Seimas consideration scheduled Nov 2026`

Under the plan, person identification data would be activated with existing eID means: the ID card at level high (through the mCard app or a card reader), or a qualified electronic signature or the non-notified Mobile-ID and Smart-ID schemes at level substantial, supplemented by a facial comparison with the image held in the Population Register. VSSA was proposed as wallet provider, RRT as supervisor and registrar, and the Registers Centre or the Migration Department as provider of person identification data.

Qualified eID providers' ongoing duties

Providers must keep each supervised eID means compliant with every requirement of its level, keep their termination plan current and notify RRT of changes within 3 working days (Article 18^{3}). RRT has also adopted a procedure for reporting security or integrity breaches of supervised eID means and trust services.

8 Risk indicators and red flags

IDENTITY ABUSE IN DIGITAL PUBLIC SERVICES

- **Impersonated institutions**: messages imitating financial institutions, law enforcement or other bodies to obtain login or confidential data (Bank of Lithuania).
- **Credential phishing**: links asking for e-banking, Smart-ID or Mobile-ID codes.
- **Unwitting confirmation**: a person approves a credit application or signs a contract believing they are confirming something else.
- **Level mismatch**: a service accepting an eID means below the level set for it.
- **Repeated identity incidents**: identity-related security incidents on a service, which must be logged and trigger reassessment within ten working days.
- **Replayed or manipulated video**: video identification sessions that are interrupted, reuse recordings or fail liveness and chip checks.
- **Unregistered relying party**: a wallet data request from a party with no valid registration, or requests for more attributes than needed.

9 Enforcement and penalties

Target	Penalty	Basis
Supervised eID means	Level changed or withdrawn if a non-conformity is not fixed within the deadline (at least 10 working days)	Law No XIII-1120, Article 18^1(6)
Trust service providers (persons or managers of legal persons)	EUR 150 to 1,150; EUR 1,100 to 3,000 where users suffered damage	Code of Administrative Offences, Article 147
Qualified eID providers (persons or managers of legal persons)	EUR 150 to 1,150; EUR 1,100 to 3,000 where users suffered damage	Code of Administrative Offences, Article 147^1
Trust service providers (EU minimum for the maximum fine)	At least EUR 5,000,000, or for legal persons 1% of worldwide turnover if higher	eIDAS Article 16(2)

Public authorities and bodies (GDPR)	Up to 0.5% of budget and income, max EUR 30,000 (Art. 83(4)(a) to ©); up to 1%, max EUR 60,000 (Art. 83(5)(a) to (e), 83(6))	Law No I-1374, Article 33

RRT investigates offences under Articles 147 and 147[1] (Code, Article 589(24)). These amounts are unchanged in the versions of the Code already adopted through January 2028; eIDAS Article 16 separately requires Member States to provide for the higher maximum fines shown above.

In January 2025 VDAI fined the Employment Service EUR 9,000 after an email attachment exposed the data of 41,086 jobseekers, breaching the confidentiality and security duties in Articles 5(1)(f), 24(1) and 32(1)(b) and (d) GDPR (decision 3R-57 of 17 January 2025). VDAI set a starting amount of 15% of the EUR 60,000 cap for public bodies.

10 Recent changes and what to watch

- **Dec 2027:** private relying parties under a strong authentication duty must accept EU Digital Identity Wallets on request. `Adopted, applies from Dec 2027` Covered firms need wallet acceptance in login and onboarding flows.
- **19 Aug 2027:** Implementing Regulation (EU) 2025/1566 applies ETSI TS 119 461 to identity proofing for qualified certificates. `Adopted, applies from 19 Aug 2027` Remote proofing processes built to RRT decision TN-659 need checking against it.
- **Dec 2026:** deadline for Member States to provide EU Digital Identity Wallets. `Adopted, due Dec 2026` Lithuania's planned go-live is early 2027, after the EU deadline.
- **Nov 2026:** Seimas consideration of the Government bill amending Law No XIII-1120 for the EU Digital Identity Wallet, as scheduled in the autumn session programme. `Planned bill, not yet registered` The bill will set wallet roles, ecosystem participants' duties and updated trust services rules.
- **13 May 2026:** VSSA switched the E-Government Gateway to a modernised identity-verification subsystem within VIISP. `In force` Existing integrations using the V2 protocol were moved to the new infrastructure automatically.
- **29 Jan 2026:** RRT assigned level high to the Paysera Mobile App (decision TN-24). `In force` A fourth supervised eID means is available.
- **24 Jan 2025:** VSSA adopted the methodology for setting assurance levels for public e-services. `In force` Public bodies must approve the level for each service, reassess it periodically and log identity incidents.

11 What this means for identity verification

- **Design to the level, not the tool.** Map each public service to its assurance level and accept only eID means with a matching RRT-assigned or EU-notified level.
- **Support the Lithuanian ecosystem.** Alongside the ID card (high, notified), the RRT-supervised means are Smart-ID and Mobile-ID (high), Paysera Mobile App (high) and LT ID (substantial). The E-Government Gateway itself offers ten e-banking providers, mobile e-signature, LT ID, the ID card (including contactless reading), USB signature devices and official certificates, but not Smart-ID.
- **Plan for cross-border users.** Notified EU and EEA eIDs must be recognised now, and EU Digital Identity Wallets once provided.
- **Video identification needs NFC.** For qualified certificates, video checks must read and cryptographically verify the document chip, test liveness and use a one-time code, and must pass a conformity assessment.
- **Log identity incidents.** Public bodies must record identity-related incidents and reassess levels after them.
- **Minimise identifiers.** Keep the personal code out of public outputs and marketing, and request only the wallet attributes a service needs.

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 reading of the Lithuanian identity card chip, for services that need a documentary check alongside eID login.
- Biometric liveness and face match as a supplementary check where a workflow adds facial comparison to a substantial-level credential.
- Age verification for services that depend on age thresholds such as the age of 14 for consent and eID certificates.
- A no-code workflow builder to route users by the assurance level each service requires, with cloud, on-premises or hybrid deployment for public-sector data residency.

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

- **Elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymas (Law on Electronic Identification and Trust Services for Electronic Transactions), No XIII-1120**, consolidated version from 18 October 2024, Articles 3, 14, 18^{1} to 18^{3}, e-seimas.lrs.lt; English translation by RRT, e-seimas.lrs.lt
- **Pinigų plovimo ir teroristų finansavimo prevencijos įstatymas (Law on the Prevention of Money Laundering and Terrorist Financing), No VIII-275**, consolidated versions from 30 June 2026 and 1 January 2027, Articles 2(10), 7^{1}, 8(1), 11(1), e-seimas.lrs.lt; English translation (as last amended 15 April 2021, title only relied on), e-seimas.lrs.lt

- **Asmens duomenų teisinės apsaugos įstatymas (Law on Legal Protection of Personal Data), No I-1374**, consolidated version from 30 June 2026, Articles 3, 6, 33, e-seimas.lrs.lt
- **Administracinių nusižengimų kodeksas (Code of Administrative Offences)**, consolidated version 1 November to 31 December 2026, Articles 147, 147[1], 589(24), e-seimas.lrs.lt
- **Dėl Asmens tapatybės kortelės ir paso išdavimo tvarkos aprašo patvirtinimo (Identity card and passport issuance procedure), Order No 1V-200/V-62**, consolidated version from 13 November 2025, e-seimas.lrs.lt
- **VSSA Director's Order No T-7(2025) on the methodology for assessing the eID assurance level suitable for electronic services**, 24 January 2025, consolidated from 11 August 2025, points 3 to 14, e-seimas.lrs.lt
- **VSSA Director's Order No T-4(2025) on the National Electronic Identification Information System regulations**, 21 January 2025, e-seimas.lrs.lt
- **RRT Council decision No TN-659 on the procedure for verifying identity when issuing qualified certificates**, 7 December 2023, points 8 to 15, e-seimas.lrs.lt
- **RRT Council decision No TN-709 on the supervision procedure for qualified eID providers and guidelines on choosing the assurance level**, 21 December 2023, e-tar.lt
- **RRT Council decision No TN-752 assigning level high to Smart-ID and Mobile-ID**, 7 November 2024, rrt.lt
- **Communications Regulatory Authority, Elektroninė atpažintis (Electronic identification)**, supervised qualified eID means, rrt.lt
- **Government Resolution No 1659 on use of the interoperability system of public administration information systems**, 16 December 2009, point 1, e-tar.lt
- **Minister of the Economy and Innovation Order No 4-886 approving the VIISP Regulations**, 9 August 2021, consolidated from 29 November 2023, points 5.7, 22.4.14, e-tar.lt
- **VIISP Functioning Rules, Order No T-228**, consolidated from 13 January 2024, points 17 to 19, e-tar.lt
- **Government Resolution No 875, Rules for Examining Persons' Requests and Complaints in Public Administration Entities**, consolidated from 3 September 2022, point 24.5, e-seimas.lrs.lt
- **Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework**, Articles 5a, 5b, 5f, 16, 24, eur-lex.europa.eu
- **Commission Implementing Regulations (EU) 2024/2977, 2024/2979, 2024/2980 and 2024/2982** (adopted under Article 5a(23)) on person identification data and electronic attestations of attributes, integrity and core functionalities, notifications concerning the wallet ecosystem, and protocols and interfaces, and **Commission Implementing Regulation (EU) 2024/2981** (adopted under Article 5c(6)) on certification of European Digital Identity Wallets, all of 28 November 2024, OJ L 4 December 2024, in force 24 December 2024, 2024/2977, 2024/2979, 2024/2980, 2024/2981, 2024/2982
- **Commission Implementing Regulation (EU) 2025/1566** on reference standards for verifying identity for qualified certificates, 29 July 2025, Article 2 and Annex, eur-lex.europa.eu
- **Regulation (EU) 2016/679 (GDPR)**, Article 9, eur-lex.europa.eu

- **Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No 910/2014**, C/2025/2448, 25 April 2025, eur-lex.europa.eu
- **Ministry of the Economy and Innovation, eIDAS darbo grupė (eIDAS working group)**, Order No 4-45, updated 11 May 2026, eimin.lrv.lt
- **eIDAS working group, minutes of the meeting of 26 November 2025** (dated 8 December 2025), pages 2 to 3, eimin.lrv.lt
- **Seimas Resolution No XV-1194 approving the work programme of the V (autumn) session**, 22 September 2026, item 21, e-seimas.lrs.lt
- **Ministry of the Economy and Innovation, EIMIN į Seimą neša 18 įstatymų paketą (EIMIN's 18-bill package for the Seimas)**, 10 February 2026, eimin.lrv.lt
- **State Digital Solutions Agency, VSSA atnaujina prisijungimą prie elektroninių paslaugų (VSSA updates login to e-services)**, 12 May 2026, vssa.lrv.lt
- **EUDI wallet feasibility study, interim results presented to the eIDAS working group**, November 2025, slides 5 to 11, eimin.lrv.lt
- **State Digital Solutions Agency, Istorija (History) and VIISP pages**, vssa.lrv.lt
- **E-Government Gateway, Prisijungimas (login page)**, login options viewed 9 November 2026, epaslaugos.lt
- **VDAI decision No 3R-57 on the Employment Service**, 17 January 2025, vdai.lrv.lt
- **Bank of Lithuania, Duomenų viliojimas (Phishing)**, updated 25 October 2024, lb.lt; **Naujas sukčiavimo būdas (New fraud method)**, 10 June 2024, lb.lt