Identomat

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in Latvia

COUNTRY Latvia

INDUSTRY Telecom & Mobile Services

LAST UPDATED 5 November 2026

KEY REGULATORS Public Utilities Commission (SPRK) · Data State Inspectorate · Consumer Rights Protection Centre

Key takeaways

- A company registered in the EU can offer telecom services in Latvia after notifying the regulator, the Public Utilities Commission (SPRK); there is no licence to apply for, but numbers and spectrum need separate rights.
- Telecom operators are not covered by Latvia's anti-money laundering (AML) law, so there is no customer due diligence rule of the banking kind. Identity duties come from telecom law instead.
- Prepaid SIM cards can still be sold anonymously today, but that ends on 1 September 2027. From that date operators must collect and keep each new prepaid user's identity details and may not provide the service to an unregistered user.
- The rules apply equally to shops and online sales. How a buyer may be identified remotely will be set in government (Cabinet of Ministers) regulations that have not yet been issued (as of November 2026).
- Number porting checks, fraud blocking and 18-month data retention already apply, and SPRK has recently fined operators for numbering and consumer-contract breaches.

Latvia's telecom market is open to new entrants, including mobile virtual network operators (MVNOs) and online-only brands. Entry is by notification under the Electronic Communications Law, supervised by SPRK, with the Data State Inspectorate (DVI) and the Consumer Rights Protection Centre (PTAC) covering data protection and consumer protection.

The biggest change for a new entrant is mandatory prepaid registration from 1 September 2027. The law fixes the data set and the ban on serving unregistered users. The Cabinet of Ministers will set the procedure for registration, verification and exceptions, so remote onboarding flows cannot be finalised until those regulations are published.

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

The Electronic Communications Law (Elektronisko sakaru likums, 2022) names the Public Utilities Commission as the sector "Regulator".

Authority	Remit	Level	Official site
Public Utilities Commission (Sabiedrisko pakalpojumu regulēšanas komisija, SPRK)	Notification register, numbering and spectrum rights, number portability, numbering fraud, general authorisation, administrative fines	National	sprk.gov.lv
Data State Inspectorate (Datu valsts inspekcija, DVI)	GDPR supervision; may request traffic data from operators	National	dvi.gov.lv
Consumer Rights Protection Centre (Patērētāju tiesību aizsardzības centrs, PTAC)	Consumer protection, including distance contracts	National	ptac.gov.lv
Ministry of Smart Administration and Regional Development (VARAM) and Ministry of Transport	Sector policy; VARAM handles radio-communications offences	National	varam.gov.lv

Supervisory Committee of Digital Security (Digitālās drošības uzraudzības komiteja)	Registers and supervises qualified electronic identification providers	National	mod.gov.lv
Ministry of the Interior and State Police	Sponsor of prepaid registration; recipients of retained data	National	iem.gov.lv
European Union	European Electronic Communications Code, ePrivacy Directive, GDPR, eIDAS	Supranational	eur-lex.europa.eu

2 Licensing and authorisation

Latvia uses the EU general authorisation model. Under Section 16 of the Electronic Communications Law, a company must send SPRK a notification before it starts providing electronic communications networks or services. It becomes an electronic communications merchant, with the right to provide services, only once SPRK has received a complete notification; SPRK confirms receipt within a week. Number-independent messaging and calling apps are exempt. SPRK keeps a public register of merchants and enters companies registered in an EU Member State (Section 17); a merchant removed from it loses its numbering and spectrum rights (Section 18(3)).

The conditions are set in SPRK's General Authorisation and Registration Rules (decision No 1/22 of 15 September 2022). Numbers require numbering usage rights from SPRK (Section 63) and spectrum requires separate rights, so an MVNO with its own numbers needs a notification and numbering rights, but no spectrum.

Breaching the general authorisation conditions carries a warning or a fine for legal persons of 56 to 2,800 fine units (Section 120), which is EUR 280 to EUR 14,000 at the EUR 5 fine unit set by Section 16 of the Administrative Liability Law.

3 Identity framework (AML rules do not apply)

Electronic communications merchants are not among the obliged entities listed in Section 3 of the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing. They have no customer due diligence, beneficial ownership or suspicious transaction reporting duties under that law, unless they carry on a separate regulated activity such as payment services. Sanctions still apply: under Section 2(2) of the Law on

International Sanctions and National Sanctions of the Republic of Latvia, every person must comply with international and national sanctions, and Section 12(5) requires anyone implementing them, including by freezing assets, to inform the Financial Intelligence Unit of Latvia (FIU Latvia) immediately. Customers should therefore be screened against EU and national lists.

Customer identity is governed by the Electronic Communications Law itself:

Registered end-user

Section 1 defines a registered end-user as one who has given the provider their identification data. Contracts must include the end-user's identifying data (SPRK decision No 1/30, point 4.1), and retained data cover a registered user's name, personal code or company name and registration number, and address (Sections 100 and 101).

Unregistered prepaid (until 31 Aug 2027)

Anonymous prepaid service is still lawful. For a prepaid user who is not registered, mobile operators retain the first activation date, time and activation location identifier, such as the cell ID (Section 100(2)(12)).

Mandatory prepaid registration

`Adopted, applies from 1 Sep 2027`

Amendments adopted on 29 October 2026 and proclaimed on 4 November 2026 require identity data for every new prepaid contract for numbered calls and messages or prepaid internet access, and ban service to unregistered users.

New Section 19(1)(7) entitles the operator to request the end-user's identification data when concluding the contract: for a natural person, name, surname, date of birth and Latvian personal code or, where there is none, the number, issue date, issuing country and issuing authority of an identity document; for a legal person, name and registration number. New Section 19(2)(22) requires the operator to store these data together with the SIM card's connection number, and new Section 19(3.1) prohibits providing the service to an unregistered end-user. The Cabinet of Ministers will set the procedure for registration, collecting and verifying identification data, processing those data, and any exceptions. Contracts concluded up to 31 August 2027 are not affected, so existing anonymous prepaid cards may continue.

4 Identity verification and onboarding

The amending law sets what must be collected but leaves the verification method to Cabinet regulations, which have not been issued (as of November 2026). The Government's explanatory memorandum to the bill (Saeima document No 4454, March 2026) states that users will identify themselves in person or remotely by providing identification data. Until the regulations are published, flows should support both channels and capture the full statutory data set.

Electronic identification as a remote route

Under Section 3(3) of the Law on Electronic Identification of Natural Persons, electronic identification is equivalent to an in-person identity document check when done with a qualified or qualified increased security means, or by a method agreed in writing. Section 19(1.1) requires electronic service providers to let users identify with any national electronic identification means, as far as technical interoperability allows. Section 19(1) also requires providers relying on qualified identification to keep authentication assertions and logs of failed attempts. The Supervisory Committee of Digital Security lists two qualified providers: the State Radio and Television Centre (LVRTC), for the eID card, eParaksts card, eParaksts card+ and eParaksts mobile, and SK ID Solutions, for Smart-ID.

Documents, biometrics and reliance

Latvian telecom law does not list accepted identity documents, mention selfie or liveness checks, or regulate reliance on third-party identity providers, so biometric matching falls under the GDPR (section 6). The registration duty, and the fine in new Section 119.1, rest with the operator.

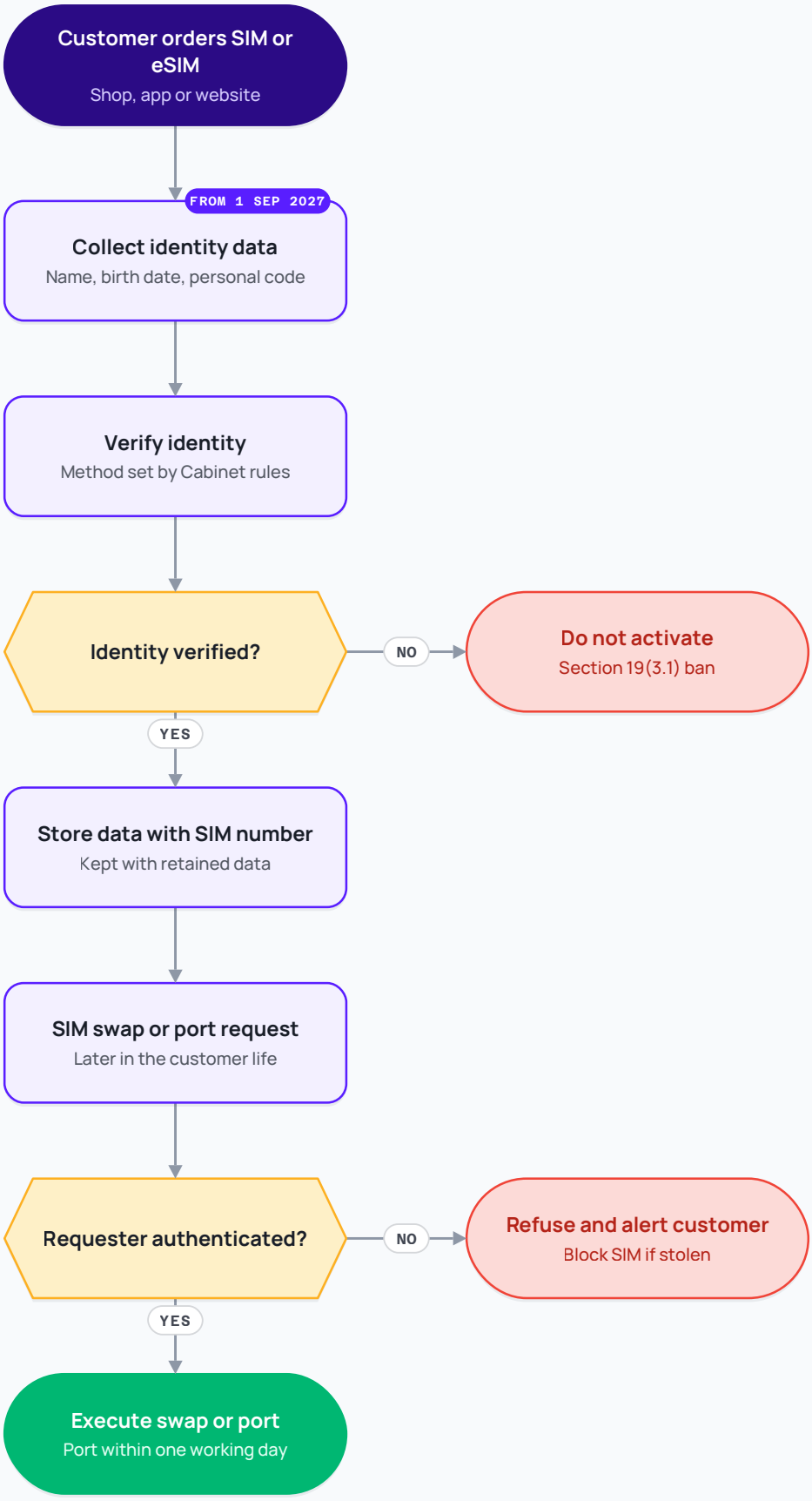


Figure 1. Prepaid SIM or eSIM onboarding and later SIM swap or port-out in Latvia, as required from 1 September 2027.

5 Digital channels: what's different

Bottom line: the prepaid registration duty is channel-neutral, but the remote methods that will satisfy it depend on Cabinet regulations still to be issued, while qualified electronic identification is already treated in law as equal to an in-person document check.

Requirement	In person / land-based	Online / remote	Difference
Notification to SPRK	Required before service	Required; number-independent apps exempt	Same
Prepaid identity data (from 1 Sep 2027)	Statutory data set	Same statutory data set	Same
How identity is checked	Document inspection	Qualified eID equals in-person check; other methods by written agreement or Cabinet rules	Differs
Contract summary before signing	Required	Required, including distance contracts	Same
Porting an unregistered prepaid number	Show the SIM card	Same rule; no remote procedure specified	Same
Biometric data	Not normally processed	Face matching is special-category data under GDPR	Differs
EU Digital Identity Wallet	Not applicable	Must be accepted on request by December 2027 where strong authentication is required (larger firms)	Differs
Data retention	18 months	18 months	Same

Online activation and eSIM

New Section 19(3.1) attaches to the service, not the point of sale, so online and eSIM activation needs the same registration as a shop sale from 1 September 2027. The law refers to the identification module card and does not mention eSIM; eSIM handling will depend on the Cabinet procedure.

Distance contracts

Contracts may be concluded electronically (Section 36(2)). Under Section 36(3) the consumer must be able to see the contract summary before concluding the contract; if technical reasons prevent this, the contract takes effect only once the consumer confirms agreement after receiving it. SPRK has enforced this for distance contracts (see section 9), and the withdrawal right in Section 12 of the Consumer Rights Protection Law also applies.

European Digital Identity Wallets `Adopted, phased application`

Article 5f(2) of Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183, requires private relying parties in sectors including telecommunications that must use strong user authentication for online identification to accept European Digital Identity Wallets at the user's voluntary request, no later than 36 months after the implementing acts under Articles 5a(23) and 5c(6) entered into force. Those acts (Implementing Regulations (EU) 2024/2977, 2024/2979, 2024/2980, 2024/2981 and 2024/2982) were published on 4 December 2024 and entered into force on the twentieth day after publication (24 December 2024), which puts the deadline at 24 December 2027; the 2026 amending act (Implementing Regulation (EU) 2026/1731) sets no new date. Micro and small enterprises are exempt.

6 Data protection and biometrics

The GDPR applies, supervised by DVI under the Personal Data Processing Law. Telecom-specific rules in the Electronic Communications Law sit on top of it:

- **Confidentiality.** Section 94 prohibits disclosing information about an end-user or the services it receives without consent, except to the authorities named in the law.
- **Breach procedures.** Section 95 requires an internal data breach procedure meeting Cabinet minimum requirements.
- **Retention.** Section 99(4) requires retained data to be kept for 18 months and supplied on request to the authorities listed in Section 99(1), including pre-trial investigators,

security services, prosecutors and courts. From 1 September 2027 the retained data set for prepaid users will include their identification data (amended Section 100(2)(12)). Transitional provision 18 records that the data retention regime is to be brought into line with EU law and the Constitution; until then, data are released under the relevant procedural laws where necessary and justified.

- **Biometrics.** Face matching or liveness data used to identify a customer are biometric data processed for uniquely identifying a person, a special category under Article 9(1) GDPR. Nothing in telecom law requires biometrics, so an operator using them needs an Article 9(2) condition, typically explicit consent, and should offer a non-biometric route.

7 Sector-specific obligations

Number portability and port-out checks

Section 43 gives end-users a free right to keep their number when switching. The recipient operator must port and activate the number no later than one working day after the agreed date, and the user may not lose service for more than one working day. SPRK's Number Portability Rules (decision No 1/11 of 18 August 2022) set the identity checks: a user with a contract gives name, surname and personal code (or company name and registration number), the number and the donor operator; a user without a contract gives the SIM card serial number and must present the SIM card. The recipient may request and check other information needed to establish the user's right to port. The donor confirms or refuses, with reasons, within 24 hours excluding weekends and public holidays, and mobile numbers are switched on weekdays between 03:00 and 05:00.

SIM replacement and lost SIMs

Latvian telecom rules do not prescribe a specific authentication method for SIM replacement. Operators must run a free 24-hour helpdesk where a lost or stolen SIM card can be blocked (SPRK decisions No 1/22, point 10.3, and No 1/30, point 7.3), and Section 19(2)(8) requires security measures to protect end-users' data. For lost handsets, Cabinet Regulation No 42 of 2023 lets an operator check the applicant's identity document before blocking the device. SIM swap authentication is therefore the operator's own control and should be documented as such.

Numbering fraud and spoofed calls

SPRK's Numbering Fraud Prevention Rules (decision No 1/27, in force 1 October 2022) define fraud indicators, including full or partial alteration of the calling number. An operator must also stop routing traffic from numbers used by its own customers when it arrives from

another operator's network, except in roaming. An operator that detects fraud must stop routing immediately, inform the affected end-user, and report to SPRK within 10 working days. Under Section 64(4), an operator that fails to stop routing can lose its numbering rights and be refused new ones for three years. Section 98(8.1) requires operators receiving international interconnect calls to process terminal location data, including roaming status, to prevent fraud.

8 Risk indicators and red flags

TELECOM FRAUD AND IDENTITY-ABUSE INDICATORS

- **Calling number alteration**: a calling number changed in whole or in part (SPRK fraud indicator).
- **Domestic numbers from abroad**: calls from Latvian numbers received over a foreign operator's network, outside roaming.
- **Unanswered call bursts**: missed calls from foreign or premium-rate numbers designed to prompt call-backs.
- **Unbalanced traffic**: outgoing calls or messages far exceeding incoming ones, or uniform traffic at unusual hours.
- **SIM box use**: SIM banks offering numbers from more than 80 countries to open anonymous accounts, dismantled by the State Police in operation "SIMcartel" (October 2025).
- **Numbering rights passed on**: numbers sub-assigned to foreign operators without traffic control (SPRK enforcement, 2026).
- **Anonymous prepaid cards**: unregistered cards used in phone fraud, the stated reason for the 2026 amendments.

The explanatory memorandum to the prepaid amendments reports 8,701 fraud events recorded by the State Police in 2025 (EUR 23.8 million obtained), up from 4,096 (EUR 16.1 million) in 2024, mostly using Latvian operators' prepaid SIM cards.

9 Enforcement and penalties

SPRK handles most administrative offences under the law (Section 125(2)). Fines are set in EUR 5 fine units, with warnings as an alternative.

Breach	Provision	Legal persons
End-user rights, special requirements, general authorisation, numbering or spectrum conditions	Sections 118, 119, 120, 123	Warning or 56 to 2,800 units (EUR 280 to EUR 14,000)
Roaming rules	Section 122	Warning or 140 to 2,800 units (EUR 700 to EUR 14,000)
Serving an unregistered prepaid user `From 1 Sep 2027`	Section 119.1	Warning or up to 200 units (up to EUR 1,000)

Recent SPRK actions:

- **SIA "Tet", May 2025.** EUR 14,000 for failing to give consumers contract summaries before concluding contracts, including distance contracts.
- **SIA "Rigatta", June 2026.** EUR 1,900 across three cases for passing numbering rights for fixed numbers to a foreign operator and failing to control traffic, which allowed calls from Latvian fixed numbers to originate abroad.

10 Recent changes and what to watch

- **4 November 2026:** amendments to the Electronic Communications Law published (Latvijas Vēstnesis No 213) `Adopted, applies from 1 Sep 2027`. The law enters into force on 18 November 2026, consolidating emergency calls on 112; prepaid registration, the ban on serving unregistered users and the new fine apply to contracts concluded from 1 September 2027.
- **3 November 2026:** public consultation closed on a Ministry of Transport bill to register SIM-box systems `Draft, consultation closed`. Unregistered SIM boxes would be banned, subject to Cabinet exceptions, with a register kept by SIA "Elektroniskie sakari".
- **Pending:** Cabinet of Ministers regulations on the registration and verification procedure and exceptions `Not yet issued`. They will set the allowed remote methods.
- **29 September 2026:** SPRK opinion meeting on amendments to the Numbering Fraud Prevention Rules `Consultation closed, not adopted`. The draft adds fraud indicators and stricter monitoring of incoming traffic, with a transition period.
- **18 August 2026:** the EU e-Evidence Regulation (EU) 2023/1543 applies `In force`. Authorities in other Member States can order providers to produce or preserve data; Latvia's implementing amendments to the Electronic Communications Law (bill No 1477/

Lp14) were adopted on 29 October 2026 and not yet proclaimed as of 5 November `Adopted, not yet proclaimed`.

- **Data retention reform:** Ministry of Transport bill to align retention rules with EU law and the Constitution `Draft, not submitted to the Saeima`. The 18-month regime applies until it is adopted.
- **24 December 2027:** deadline for larger telecom relying parties to accept EU Digital Identity Wallets under Article 5f(2) of the amended eIDAS Regulation `Adopted, applies from Dec 2027`.

11 What this means for identity verification

- **Data capture.** Collect name, surname, date of birth and Latvian personal code, with a fallback for foreign identity documents (number, issue date, issuing country and authority), and company name and registration number for business customers.
- **Remote methods.** Qualified national eID already counts as an in-person check; document and selfie flows should be ready to adapt to the Cabinet procedure.
- **Gate activation.** From 1 September 2027 no prepaid numbered service or prepaid internet access may start until registration is complete, in every sales channel.
- **Link identity to the SIM.** Store identification data against the SIM connection number so it can be produced as retained data.
- **Life-cycle checks.** Authenticate SIM swap and port requests against registered data, and keep evidence of the checks.
- **Biometrics and retention.** Treat face data as special-category data, keep it no longer than needed, and separate it from the 18-month retained data.

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 for prepaid SIM and eSIM activation, capturing the full data set the Electronic Communications Law requires.
- ID document capture and verification, including NFC chip reading, for customers with Latvian or foreign identity documents.
- Face match with biometric liveness for remote onboarding, configurable so a non-biometric route can be offered.
- Re-verification of the account holder before SIM swap or port-out, with phone and email verification.
- No-code workflow builder and an audit trail for each check, with cloud, on-premises or hybrid deployment.

Request a meeting

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- **Elektronisko sakaru likums [Electronic Communications Law]**, 14 July 2022, consolidated text, Sections 1, 16 to 19, 36, 43, 63, 64, 94, 95, 98 to 101, 118 to 125 and transitional provisions, likumi.lv
- **Grozījumi Elektronisko sakaru likumā [Amendments to the Electronic Communications Law]**, adopted 29 October 2026, Latvijas Vēstnesis No 213, 4 November 2026, in force 18 November 2026 (prepaid provisions from 1 September 2027), likumi.lv
- **Saeima dossier for bill No 1246/Lp14**, with second-reading proposals table (No 4454B) and the Government's explanatory memorandum (No 4454, March 2026), titania.saeima.lv

- **Saeima press release, "Priekšapmaksas SIM kartes turpmāk būs jāreģistrē" [Prepaid SIM cards will have to be registered]**, 29 October 2026, lvportals.lv
- **Administratīvās atbildības likums [Administrative Liability Law]**, Section 16 (fine unit), likumi.lv
- **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 and 3, likumi.lv
- **Starptautisko un Latvijas Republikas nacionālo sankciju likums [Law on International Sanctions and National Sanctions of the Republic of Latvia]**, Sections 2 and 12, likumi.lv
- **Fizisko personu elektroniskās identifikācijas likums [Law on Electronic Identification of Natural Persons]**, Sections 3 and 19, likumi.lv
- **Fizisko personu datu apstrādes likums [Personal Data Processing Law]**, likumi.lv
- **Patērētāju tiesību aizsardzības likums [Consumer Rights Protection Law]**, Sections 10 and 12, likumi.lv
- **Supervisory Committee of Digital Security, electronic identification page and register of qualified providers**, mod.gov.lv
- **Cabinet Regulation No 42, rules on the central database of lost terminal devices**, 31 January 2023, point 4, likumi.lv
- **SPRK decision No 1/30, Elektronisko sakaru pakalpojumu līguma noteikumi [Electronic Communications Service Contract Rules]**, 22 September 2022, points 4.1 and 7.3, likumi.lv
- **SPRK decision No 1/22, Vispārējās atļaujas un reģistrācijas noteikumi elektronisko sakaru nozarē [General Authorisation and Registration Rules]**, 15 September 2022, point 10.3, likumi.lv
- **SPRK decision No 1/11, Numura saglabāšanas pakalpojuma nodrošināšanas noteikumi [Number Portability Rules]**, 18 August 2022, points 4 to 7, likumi.lv
- **SPRK decision No 1/27, Numerācijas krāpniecības novēršanas noteikumi [Numbering Fraud Prevention Rules]**, 22 September 2022, points 2 to 9, likumi.lv
- **SPRK, penalty against SIA "Tet" for failure to provide contract summaries**, 23 May 2025, sprk.gov.lv
- **SPRK, penalty for breach of numbering rights conditions and lack of traffic control**, 10 June 2026, sprk.gov.lv
- **SPRK, opinion meeting on amendments to the Numbering Fraud Prevention Rules**, 28 September 2026, sprk.gov.lv
- **SPRK, consultation document on amendments to the Numbering Fraud Prevention Rules**, 22 February 2024, sprk.gov.lv
- **Draft law 26-TA-2559, Grozījumi Elektronisko sakaru likumā (SIM-box registration)**, Ministry of Transport, public consultation 20 October to 3 November 2026, tapportals.mk.gov.lv
- **Saeima dossier for bill No 1477/Lp14 (e-evidence amendments to the Electronic Communications Law)**, titania.saeima.lv
- **Regulation (EU) 2023/1543 on European Production and Preservation Orders for electronic evidence**, Articles 1 and 34, eur-lex.europa.eu

- **State Police, international operation "SIMcartel"**, 17 October 2025, vp.gov.lv
- **Draft law 23-TA-176, Grozījumi Elektronisko sakaru likumā (data retention)**, Ministry of Transport, Legislative Drafting Portal, tapportals.mk.gov.lv
- **Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 (European Digital Identity Framework)**, 11 April 2024, Article 5f(2), eur-lex.europa.eu
- **Commission Implementing Regulations (EU) 2024/2977, 2024/2979, 2024/2980, 2024/2981 and 2024/2982**, 28 November 2024, OJ L of 4 December 2024, for example eur-lex.europa.eu
- **Commission Implementing Regulation (EU) 2026/1731**, 15 July 2026, amending the 2024 wallet implementing regulations, eur-lex.europa.eu
- **Regulation (EU) 2016/679 (General Data Protection Regulation)**, Article 9, eur-lex.europa.eu