Identomat

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in Lithuania

COUNTRY Lithuania

INDUSTRY Telecom & Mobile Services

LAST UPDATED 9 November 2026

KEY REGULATORS Communications Regulatory Authority of the Republic of Lithuania · State Data Protection Inspectorate

Key takeaways

- No licence is needed to provide mobile or other electronic communications services in Lithuania: a provider notifies the Communications Regulatory Authority (RRT) where its activity is on RRT's list, and generally needs RRT's permission to use numbers and radio frequencies.
- Since 1 January 2025, a mobile provider may not serve a new prepaid (pay-as-you-go) customer until that person's identity has been established. Prepaid contracts concluded before that date are not caught.
- Since 6 February 2026, a provider must also ensure that no person holds more than 50 active prepaid SIM cards on its network (for prepaid contracts concluded from 6 February 2026), and that a prepaid SIM can be activated only from the EU, the European Economic Area, the UK or Switzerland.
- Providers choose their own identification method, but when they identify eSIM customers remotely for activation or switching they must use measures that leave no doubt about the customer's identity. Customers must also be able to cancel through any channel used to sign up, and eSIM users must be able to switch provider without a new card.
- Telecom operators are not covered by Lithuania's anti-money laundering (AML) law, but they must retain subscriber and traffic data for law enforcement, block spoofed calls and fake SMS, and face fines of up to 3% of annual electronic communications revenue (5% for a repeat breach).

Lithuania's mobile market is open to new entrants, including mobile virtual network operators (MVNOs) and prepaid brands, under a general authorisation rather than a licence. The Communications Regulatory Authority of the Republic of Lithuania (RRT) is the sector regulator; the State Data Protection Inspectorate (VDAI) supervises the privacy and data retention chapter of the electronic communications law.

The biggest practical change for a new entrant is the end of anonymous prepaid SIM cards in 2025, followed in 2026 by limits on the number of cards and on where they can be activated. Because the method of identification is the provider's choice, the evidential strength of remote checks for online and eSIM sales sits with the operator.

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 for mobile and telecom services	Level	Official site
Communications Regulatory Authority of the Republic of Lithuania (RRT)	Sector regulator: notification, numbers and spectrum, consumer rules, number portability, anti-fraud measures, penalties; also supervises trust services and qualified e-identification providers (Law No XIII-1120, art. 3)	National	rrt.lt
Ministry of Transport and Communications	Electronic communications policy (Law on Electronic Communications, art. 4)	National	sumin.lrv.lt
State Data Protection Inspectorate (VDAI)	Supervises Chapter IX of the Law on Electronic Communications (data processing, privacy, retention; art. 5(2)) and the GDPR (Law No I-1374, art. 7)	National	vdai.lrv.lt
Ministry of the Economy and Innovation of the Republic of Lithuania	Policy on electronic identification and trust services (Law No XIII-1120, art. 3)	National	eimin.lrv.lt

Financial Crime Investigation Service (FNTT)	Anti-money laundering authority (AML Law, art. 5); ensures implementation of financial sanctions (Law on International Sanctions)	National	fntt.lrv.lt
European Union	European Electronic Communications Code (Directive (EU) 2018/1972), GDPR, European Digital Identity framework	Supranational	eur-lex.europa.eu

The State Consumer Rights Protection Authority supervises the safety of products connected with electronic communications networks and terminal equipment (Law on Electronic Communications, art. 5(1)).

2 Licensing and authorisation

The Law on Electronic Communications (No IX-2135), consolidated version in force from 1 July 2026, follows the general authorisation model of the European Electronic Communications Code. Under art. 35(1), businesses may provide electronic communications networks and services **without a separate prior permission** from any state authority, provided they comply with the law and RRT's general conditions.

- **Notification:** RRT approves a list of activities that must be notified before they start (art. 35(3)). The information requested may not exceed what is needed to identify the provider and enter it in RRT's list of providers (art. 35(4)). A provider can ask RRT for a standard confirmation of notification (art. 35(6)).
- **Numbers and spectrum:** RRT manages radio frequencies and numbers (art. 57(1)); numbers are managed under the National Numbering Plan approved by RRT (art. 57(8)). Unless RRT has said a resource can be used without a separate permit, a person must apply to RRT before using it (art. 61(1)). MVNOs that give their own numbers to customers take on number duties, including portability.
- **Exit:** a provider must notify RRT before ceasing a notified activity (art. 35(7)), and pays RRT fees (art. 35(8)).

For serious or systematic breaches, RRT can prohibit a business from providing networks or services for up to 3 years, or suspend or withdraw its rights to use numbers and frequencies (art. 90(5)).

3 Identity framework (AML rules do not apply)

Telecom operators are not obliged entities under the Law on the Prevention of Money Laundering and Terrorist Financing (No VIII-275). It applies to financial institutions and to the "other obliged entities" in art. 2(10), such as auditors, notaries, gambling and lottery companies and real estate agents; electronic communications providers are not listed. The EU Anti-Money Laundering Regulation (EU) 2024/1624, which applies from 10 July 2027 (art. 90), does not list them either (art. 3). A telecom group that also offers payment or e-money services is covered for that activity only.

Identity duties for telecoms come instead from the electronic communications framework:

Prepaid subscriber identification

Art. 40(1[1]): a person concluding a prepaid mobile contract must give the provider the data needed to identify them as a subscriber, and the provider may not provide prepaid mobile services if identity has not been established.

Prepaid SIM limits

RRT's Rules for the Provision of Electronic Communications Services, point 20[1]: at most 50 active prepaid SIM cards per person on a network, and activation only from the EU, EEA, UK or Switzerland.

Port-out identity matching

RRT's number portability procedure lets the donor operator refuse a port where the subscriber data supplied (number, name, personal code, or company name and code) do not match its records (point 14.1).

Retention for law enforcement

Art. 77(2) and Annex 1: subscriber, traffic and location data are retained and provided free of charge to competent authorities, generally for 6 months.

There is no customer due diligence, beneficial ownership or suspicious transaction reporting duty for the telecom service itself. Telecom providers, like any person, must apply international sanctions; the Law on International Sanctions (No IX-2160) names FNTT among the institutions that ensure financial sanctions are implemented.

4 Identity verification and onboarding

Prepaid customers

Art. 40(1[1]) was added by amending Law No XIV-2386 of 19 December 2023. The duty applies **only to prepaid contracts concluded from 1 January 2025, when the amending**

law took effect (art. 3(1) and (4)). Existing anonymous prepaid cards remain lawful until their contracts end.

The statute lists neither data elements nor accepted documents. RRT has stated that each provider decides how to carry out identification. The provider must publish the duty and its procedure at customer service centres and on its website (point 4.9 of the Rules for the Provision of Electronic Communications Services, consolidated from 6 February 2026) and set it out in the contract or service terms (point 23.3).

From 6 February 2026 (RRT Council Resolution TN-43), point 20[1] of the Rules also requires that one person cannot hold more than 50 active prepaid SIM cards on the provider's network (for prepaid contracts concluded from 6 February 2026, when TN-43 took effect; TN-43 point 2), and that a SIM can be activated only while the person is in Lithuania, another EU or EEA state, the UK or Switzerland.

The method must also produce data that work downstream: the portability procedure matches name and personal code (asmens kodas), and the retention annex expects subscriber name and address.

Remote identification standard

RRT's Procedure for Remote Activation of Public Mobile Services and Remote Change of Provider (order No 1V-277), in force since 1 January 2023, covers activating mobile services and changing provider on devices with an embedded SIM (eSIM) without a physical card swap (point 1). It lets providers obtain all information needed to establish a customer's identity and the reliability and authenticity of the data supplied. Where a provider establishes identity remotely in this process, it must use technical and organisational measures that ensure **no doubt arises** as to identity or the reliability and authenticity of the data (point 5). No method, assurance level or liveness standard is prescribed, and no equivalent text addresses other online sales, such as physical SIM cards ordered online.

Postpaid and business customers

Neither the Law nor the Rules set an identification rule for postpaid contracts; art. 40(1) applies the general contract requirements of the Civil Code, the Law and the Rules. For business subscribers, the portability procedure keys on company name and company code.

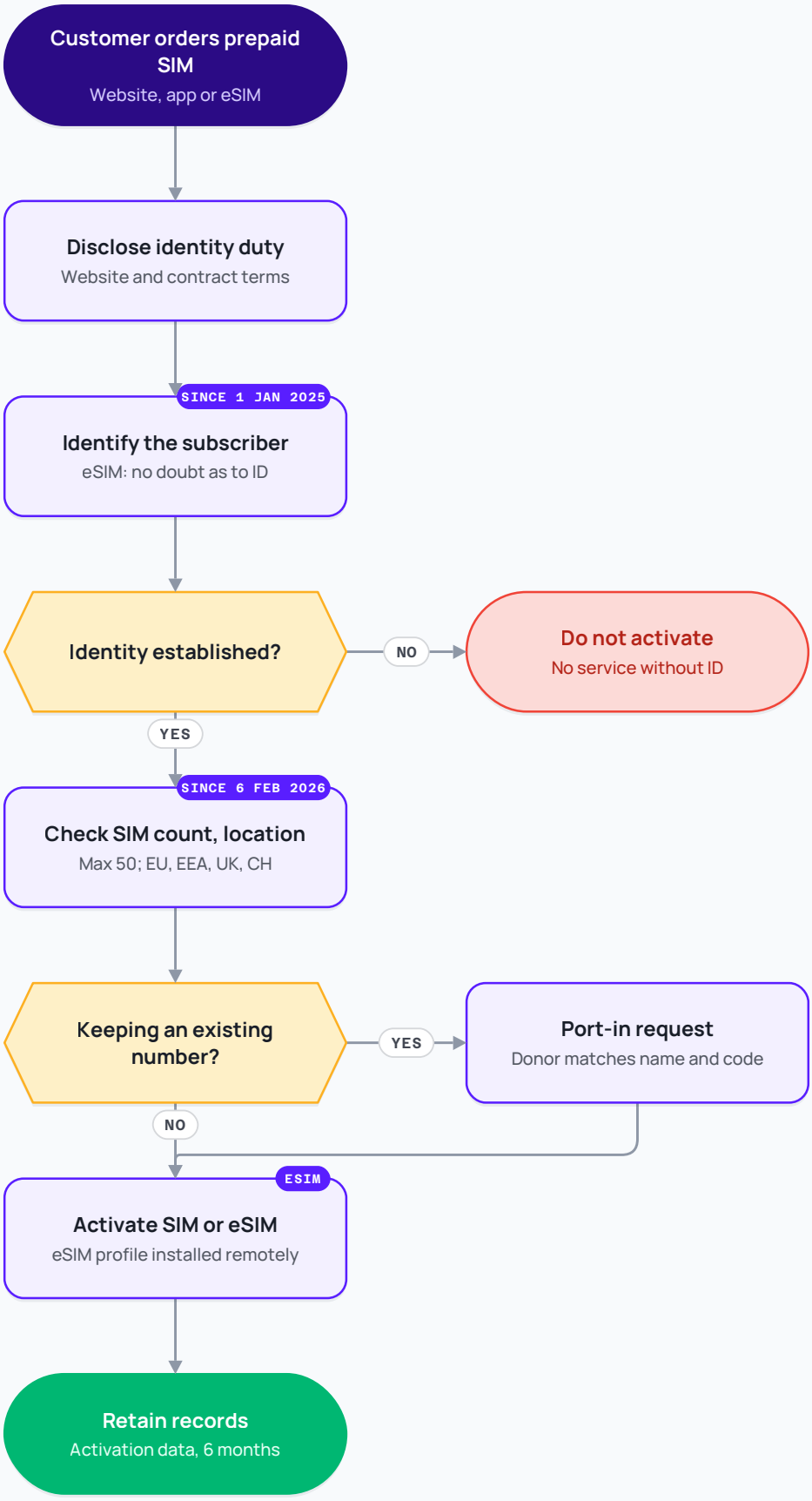


Figure 1. Online prepaid SIM or eSIM activation in Lithuania, with optional number port-in.

5 Digital channels: what's different

Bottom line: the duty to identify prepaid customers applies in every channel, but remote identification for eSIM activation must leave no doubt about the customer's identity, customers must be able to leave through the channels they joined by, and eSIM users must be able to switch without physical access to the device.

Requirement	In person / retail	Online / remote	Difference
Identity before service (new prepaid)	Required	Required	Same
Identification method	Set by provider	Set by provider; for eSIM, measures must leave no doubt as to identity	Differs
Prepaid SIM cap and activation location	50 per person; EU, EEA, UK, CH	50 per person; EU, EEA, UK, CH	Same
Publishing the identification procedure	At customer service centres	On the website	Same
Cancelling the contract	Any channel offered for signing	Online, if contracts are signed online	Differs
Port-out identity check	Name and personal code matched	Name and personal code matched	Same
Switching provider	New SIM card	eSIM: no new module or physical access	Differs
Biometric data	GDPR art. 9 if face matching is used	GDPR art. 9 if face matching is used	Same
Retention of activation data	6 months	6 months	Same

Remote identification: provider's method, "no doubt" standard

Neither art. 40(1[1]) nor the Rules list approved remote methods or require liveness or video. An operator may use document capture with face matching, a qualified electronic signature, national e-identification or another method. For eSIM activation and switching, point 5 of order No 1V-277 sets the outcome instead: remote identification must leave no doubt about identity and the authenticity of the data. Because service must be refused where identity is not established, the provider bears the risk of a method that can be defeated.

Same-channel exit

Point 27[2] of the Rules, in force since 1 May 2025, requires providers to let subscribers terminate a contract, or refuse services where the contract allows, by every means the provider uses for concluding contracts. An app-only or web-only operator must therefore offer online cancellation.

eSIM and remote switching

Art. 40(16) of the Law on Electronic Communications requires providers that give mobile numbers to end users to let them use devices with embedded SIMs and change provider, keeping their number, without changing the module and without physical access to the device. Order No 1V-277 requires providers to follow GSMA eSIM standards (point 6) and to publish their remote activation and switching procedure on their websites (point 12).

6 Data protection and biometrics

The GDPR applies to identity capture, with the Law on Legal Protection of Personal Data (No I-1374) adding national rules. Telecom-specific privacy rules sit in Chapter IX of the Law on Electronic Communications, supervised by VDAI (art. 5(2)).

- **Personal code:** may be processed only where a GDPR art. 6(1) condition applies, may never be published, and may not be processed for direct marketing (Law No I-1374, art. 3).
- **Biometrics:** face images processed to uniquely identify a person are special-category data under GDPR art. 9. Because Lithuanian law does not mandate a biometric method, an operator using face matching needs an art. 9(2) condition, typically explicit consent.
- **Data minimisation:** providers may generate and keep only the subscriber and traffic data needed to identify subscribers, provide services and bill (art. 77(1)), and must tell subscribers what is processed, why and for how long (art. 78(1)).

- **Retention:** billing traffic data may be kept for no more than 6 months, except for disputed bills or debt recovery (art. 78(3)).

7 Sector-specific obligations

Number portability and port-out fraud

Art. 40(9) gives end users the right to keep their number when changing provider. Under RRT's number portability procedure, the port request goes to the gaining provider (the recipient) on the form annexed to the procedure (point 21). If the requester is not the subscriber, the subscriber's consent must be attached, and **the recipient is responsible for there being a proper basis for the port**. The recipient may obtain from the donor the information needed to check the data supplied (point 22). The donor may refuse the port where number, name and personal code (or company name and code) do not match, or where an unidentified subscriber did not use a free online option to identify (point 14). Service may be interrupted for no more than one working day (point 26).

Data retention for law enforcement

Art. 77(2) requires providers to retain the data listed in Annex 1 and provide them free of charge to competent authorities. For prepaid mobile services, Annex 1 point 5.2.6 includes the date and time of first activation in Lithuania and the cell ID where the service was activated. Data are kept for 6 months, or 2 months for the category in Annex 1 point 6.3 (art. 78(5)).

Spoofed calls and fake SMS

RRT's access and interconnection procedure (Council Resolution TN-53), in force since 21 February 2026, requires operators to block calls from abroad using Lithuanian fixed numbers, calls from numbers RRT has not assigned, and roaming calls from numbers whose users have not left Lithuania (points 10.5 to 10.7), and to analyse incoming traffic for fraud indicators (point 12). Under art. 78(8^1) and RRT's procedure for identifying spoofed SMS (TN-64), providers must screen SMS against set criteria and let senders and SMS aggregators register identifying attributes, so that named SMS not matching them are not delivered (point 10).

8 Risk indicators and red flags

TELECOM FRAUD AND IDENTITY ABUSE INDICATORS (RRT)

- **Spoofed caller ID**: calls from abroad displaying Lithuanian, institutional or other residents' numbers.
- **Phishing SMS**: links to fake sites demanding fines or the renewal of Smart-ID, e-signature or phone services.
- **Foreign sender codes**: SMS from codes such as +44, +63, +91 and +212 written in Lithuanian.
- **Code harvesting**: requests to read out Smart-ID or mobile signature codes, PINs or card data.
- **Impersonation**: callers posing as banks, police, the tax authority, couriers or mobile operators.
- **Bulk SIM holding**: one identity approaching the 50 active prepaid SIM limit.
- **Mismatched port request**: name or personal code that does not match the donor's record, or a third-party port without valid consent.
- **Automated traffic**: high call volumes from one number to many, or auto-generated call patterns.

RRT reports that operators blocked more than 13.1 million spoofed calls and 5.73 million SMS in 2025, and about 13.8 million calls and 2.12 million SMS in the first quarter of 2026.

9 Enforcement and penalties

RRT imposes economic sanctions under arts. 90 to 92 of the Law on Electronic Communications, set as a share of gross annual revenue from electronic communications activity, with fixed caps where that revenue is hard or impossible to calculate:

Breach	Maximum sanction	Provision
Breach of the conditions for electronic communications activity and related duties	3% of gross annual revenue, or EUR 86,900	Art. 90(1)

Repeat breach within a year of a sanction	5% of gross annual revenue, or EUR 144,800	Art. 90(2)
Business with gross annual revenue below EUR 86,900	EUR 2,900 (EUR 5,800 for a repeat)	Art. 90(3)
Failing to stop unlawful activity, supply information or follow RRT requirements; obstructing inspectors	EUR 14,500, or EUR 1,500 per day for a continuing breach	Art. 90(4)
Serious or systematic breach	Ban on providing networks or services, or suspension of number and frequency rights, for up to 3 years	Art. 90(5)

A breach must be examined within 3 months of the start of proceedings, and no sanction may be imposed more than 5 years after the breach (3 years from detection for a continuing breach) (art. 87). Data protection breaches fall to VDAI under the GDPR.

Recent RRT action has focused on consumer transparency: in March 2026 RRT found that UAB Cgates had notified price changes in a misleading way and ordered it to re-notify customers with a free right to terminate.

10 Recent changes and what to watch

- **By 24 December 2027** `Adopted, applies by 24 Dec 2027` : under Regulation (EU) 2024/1183, art. 5f(2), telecom providers other than micro and small enterprises that are required by law or contract to use strong user authentication for online identification must accept European Digital Identity Wallets at the user's request, no later than 36 months after the wallet implementing acts under arts. 5a(23) and 5c(6) (Implementing Regulations (EU) 2024/2977, 2024/2979, 2024/2980, 2024/2981 and 2024/2982) entered into force on 24 December 2024.
- **1 November 2026** `In force` : RRT's Council Resolution TN-320 requires providers to inform users of outages without delay and free of charge, and to report outages meeting set criteria to RRT within 2 hours; continuity rules follow from 1 August 2028 `Adopted, effective 1 Aug 2028` .
- **1 July 2026** `In force` : amending Law No XV-815 extends art. 90(1) fines to breaches of the Gigabit Infrastructure Act (Regulation (EU) 2024/1309).
- **21 February 2026** `In force` : TN-53 replaces RRT's access rules and sets the current call-blocking and fraud-analysis duties.

- **6 February 2026** `In force`: 50-card cap on active prepaid SIMs per person (for prepaid contracts concluded from 6 February 2026) and activation only from the EU, EEA, UK or Switzerland.
- **1 January 2025** `In force`: prepaid customers must be identified before service; applies only to prepaid contracts concluded from 1 January 2025, when the amending law took effect (art. 3(1) and (4)).

11 What this means for identity verification

- **Choose and document a method:** a published identification procedure is the operator's main evidence that identity was established; for remote channels it should show why no doubt about identity remains.
- **Capture the right fields:** name and personal code for individuals, company name and code for businesses, to support de-duplication, port-out matching and retention requests.
- **Count and locate:** link each prepaid SIM to a verified identity to enforce the 50-card cap, and check the customer's location at activation.
- **Biometrics need a legal basis:** plan explicit consent and an alternative route when using face matching.
- **Legacy base:** pre-2025 prepaid customers may be unidentified; a free online self-identification route also protects the donor's right to refuse mismatched ports.
- **Port-in verification:** the gaining operator is responsible for the basis of each port, so verify the requester and any consent before submitting.

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 identification of prepaid and eSIM customers before activation, with ID document capture and verification (including NFC), face match and biometric liveness.
- A no-code workflow builder to document and publish the provider's chosen identification procedure and offer non-biometric alternatives.
- Verification of the requester before submitting number port-in requests, including phone and email verification.
- KYB checks for business subscribers, keyed on company name and code.
- Cloud, on-premises or hybrid deployment to keep identity data within the operator's own retention and minimisation controls.

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

- **Lietuvos Respublikos elektroninių ryšių įstatymas Nr. IX-2135 [Law on Electronic Communications]**, consolidated version from 1 July 2026, arts. 4, 5, 35, 40, 57, 61, 77, 78, 87, 90 and Annex 1, e-seimas.lrs.lt
- **Law No XIV-2386 of 19 December 2023 amending arts. 40 and 78 of the Law on Electronic Communications**, art. 3(1), (2) and (4), e-seimas.lrs.lt
- **Law No XV-815 of 16 April 2026 amending the Law on Electronic Communications**, arts. 12 and 14, e-seimas.lrs.lt

- **Elektroninių ryšių paslaugų teikimo taisyklės [Rules for the Provision of Electronic Communications Services]**, RRT order No 1V-1160, consolidated version from 6 February 2026, points 4.9, 20[1], 23.3, 27[2], 29, e-tar.lt
- **RRT Council Resolution No TN-43 of 5 February 2026** (prepaid SIM limits), points 1 and 2, in force 6 February 2026, e-tar.lt; **No TN-850 of 19 December 2024**, e-tar.lt
- **Viešųjų mobiliojo ryšio paslaugų aktyvavimo ir viešųjų mobiliojo ryšio paslaugų teikėjo keitimo nuotoliniu būdu tvarkos aprašas [Procedure for Remote Activation of Public Mobile Services and Remote Change of Provider]**, RRT order No 1V-277 of 12 April 2022, in force 1 January 2023, points 5, 6, 12, e-tar.lt
- **Galutinio paslaugų gavėjo teisės išlaikyti abonentinį numerį užtikrinimo sąlygų ir tvarkos aprašas [Procedure for Ensuring the End User's Right to Retain a Subscriber Number]**, RRT order No 1V-460, consolidated version from 9 April 2022, points 14, 21, 22, 26, e-seimas.lrs.lt
- **RRT Council Resolution No TN-53 of 20 February 2026 (access and interconnection procedure)**, points 10 to 12, e-tar.lt
- **Apsimestinių trumpųjų žinučių identifikavimo tvarkos aprašas [Procedure for Identifying Spoofed SMS]**, RRT Council Resolution No TN-64, consolidated version from 10 April 2025, points 3 and 10, e-tar.lt
- **RRT Council Resolution No TN-320 of 21 July 2026** (service interruption information and continuity rules), points 1 and 6, rules points 3 and 8, e-tar.lt; RRT, "RRT: nuo lapkričio 1 d. apie ryšio paslaugų sutrikimus privaloma informuoti vartotojus" [Outage information mandatory from 1 November], 30 October 2026, rrt.lt
- **Law on the Prevention of Money Laundering and Terrorist Financing (No VIII-275)**, consolidated version 30 June to 31 December 2026, arts. 2(10) and 5, e-seimas.lrs.lt
- **Law on International Sanctions (No IX-2160)**, consolidated version from 30 June 2026, e-seimas.lrs.lt
- **Law on Legal Protection of Personal Data (No I-1374)**, consolidated version from 30 June 2026, arts. 3 and 7, e-seimas.lrs.lt
- **Law on Electronic Identification and Trust Services for Electronic Transactions (No XIII-1120)**, consolidated version from 18 October 2024, art. 3, e-seimas.lrs.lt
- **Regulation (EU) 2016/679 (General Data Protection Regulation)**, art. 9, eur-lex.europa.eu
- **Regulation (EU) 2024/1624 (Anti-Money Laundering Regulation)**, arts. 3 and 90, eur-lex.europa.eu
- **Regulation (EU) 2024/1183 (European Digital Identity Framework)**, art. 5f(2), eur-lex.europa.eu; Commission Implementing Regulations (EU) 2024/2977, 2024/2979, 2024/2980 and 2024/2982 (art. 5a(23)) and 2024/2981 (art. 5c(6)), all of 28 November 2024, OJ L of 4 December 2024, in force 24 December 2024
- **RRT, "Naujos taisyklės stiprina vartotojų teises ryšių sektoriuje nuo 2025 metų" [New rules strengthen consumer rights from 2025]**, 30 December 2024, rrt.lt
- **RRT, "Apsisaugok nuo sukčiavimo" [Protect yourself from fraud]**, rrt.lt; first-quarter 2026 blocked calls and SMS, 28 May 2026, rrt.lt

- **RRT, Cgates price-change notification decision**, 10 March 2026, rrt.lt