Identomat

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in Brazil

COUNTRY Brazil

INDUSTRY Telecom & Mobile Services

LAST UPDATED 11 November 2026

KEY REGULATORS Agência Nacional de Telecomunicações (ANATEL) · Ministério das Comunicações · Autoridade Nacional de Proteção de Dados (ANPD)

Key takeaways

- Mobile operators in Brazil are not covered by the anti-money laundering (AML) law. Their identity duties come from telecom law: operators must keep an up-to-date register of their users, and for prepaid lines the law requires the holder's name, address and an identity document or taxpayer (CPF) number.
- Biometric checks are coming. The national telecom regulator (ANATEL) has approved mandatory face matching with a liveness check for new prepaid lines by 30 September 2027, and for postpaid lines, number transfers, SIM replacements and account changes by 31 December 2027.
- Existing customers who have not passed the biometric check must be re-registered by 31 December 2028. Lines not regularised can be suspended and then cancelled from January 2029.
- Online and in-store channels carry the same duties. The biometric check must be offered in shops and on operators' websites and apps, and every number transfer must be confirmed by the customer by text message within six hours, whatever the sales channel.
- Operators also answer for fraud prevention more broadly: keeping the subscriber register accurate, letting people see and cancel prepaid lines opened in their name, and securing business text messages used for one-time passwords.

The Brazilian mobile market is open to new entrants, including virtual operators, under authorisations issued by ANATEL. There is no AML licence or financial-crime reporting duty for a pure telecom business, but the identity burden is rising quickly because phone lines and text messages are widely used in fraud and scams.

The principal authorities are ANATEL, which licenses and supervises operators and sets the registration and anti-fraud rules, the Ministry of Communications, which sets policy, and the National Data Protection Authority (ANPD), which supervises the handling of the biometric and identity data that the new checks generate.

The biggest obstacle for a new entrant is the biometric validation timetable: any operator activating lines from late 2027 needs face matching with liveness detection against an existing biometric database in every sales and service channel, plus an alternative procedure for customers who cannot complete it.

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
Agência Nacional de Telecomunicações (ANATEL, National Telecommunications Agency)	Authorisations, consumer rules, subscriber registration, number portability, anti-fraud measures, sanctions	Federal	gov.br/anatel
Ministério das Comunicações (Ministry of Communications)	National telecommunications policy; ANATEL is linked to the ministry	Federal	gov.br/mcom
Autoridade Nacional de Proteção de Dados (ANPD, National Data Protection Authority)	Supervision of personal and biometric data processing under the LGPD	Federal	gov.br/anpd
Courts, Public Prosecution Service and police authorities	Access to subscriber data and call records under the laws described in section 7	Federal and state	n/a

The financial intelligence unit (COAF) has no supervisory role over telecom operators (section 3).

2 Licensing and authorisation

Under the General Telecommunications Law (Lei nº 9.472, de 16 de julho de 1997), providing a telecommunications service in the private regime requires prior authorisation from ANATEL, which also confers the right to use the radio frequencies needed (art. 131). An authorisation is a binding administrative act granted when the applicant meets objective and subjective conditions (art. 131, § 1), and ANATEL defines the cases that need no authorisation (art. 131, § 2). Mobile services are provided as the Serviço Móvel Pessoal (SMP, Personal Mobile Service).

Under the General Licensing Regulation (ANATEL Resolution 720/2020), an applicant must be a company incorporated and managed in Brazil, not barred from bidding or contracting with ANATEL, with legal and technical qualification, financial capacity and tax regularity (Annex, art. 5, as amended by Resolution 781/2025), and applies on ANATEL's electronic system (art. 7).

Mobile virtual network operators have two routes under the General Regulation of Telecommunications Services (RGST, ANATEL Resolution 777/2025). A credenciado represents a host operator and offers the service jointly with it (Annex, art. 216); the host must keep the register of those users updated and intact for security and anti-fraud purposes (art. 227, V). An authorised virtual network operator is itself an SMP provider subject to the RGST (art. 239) and needs a network-sharing contract with a host operator (art. 241). Virtual network authorisations are issued for an indefinite term and against payment (art. 251, sole paragraph); from 14 November 2026 the fee is set under the General Licensing Regulation (Resolution 792/2026).

3 Identity framework (AML rules do not apply)

The AML law, Lei nº 9.613, de 3 de março de 1998, applies customer identification, record-keeping and suspicious-transaction reporting duties only to the persons listed in its art. 9, which covers financial, securities, insurance, payment, lottery and betting, real estate, precious metals and high-value goods, virtual asset and certain advisory businesses, among others. Telecommunications operators are not on the list, so a mobile operator has no customer due diligence programme, beneficial ownership check or COAF reporting duty in that capacity.

Identity in the telecom sector is governed instead by four layers:

Prepaid registration law

Lei nº 10.703/2003 requires prepaid providers to keep an updated register with full name, address and an identity document number or CPF for individuals, or the company taxpayer number (CNPJ) for legal persons (art. 1, § 1).

Subscriber register and subscription fraud

The RGST requires providers to keep an updated register of their users (Annex, art. 119, XIV) and, in its portability chapter, to adopt preventive measures against subscription fraud (art. 69, VII), and to take the necessary and available technical and administrative measures to prevent and stop fraud and to reverse or mitigate its effects (art. 137)

`In force since 27 Oct 2025`.

Biometric validation standard

ANATEL's Technical Standard GT-SEG.2026.11 requires face recognition with proof of life for individuals and individual micro-entrepreneurs (MEI), phased in from 2027. It comes from GT-Seg, the technical group that the RGST empowers to set actions and deadlines (Annex, art. 140, II)

`Adopted, phased from 30 Sep 2027`

Law enforcement access

Registration data must be available to courts, and registration data and call records to police and prosecutors, under Lei nº 10.703/2003 and Lei nº 12.850/2013 (section 7).

4 Identity verification and onboarding

Data to collect

For an individual, the minimum register is full name, full address and either an identity document number or the CPF number; for a legal person, name, address and CNPJ (Lei nº 10.703/2003, art. 1, § 1). The national identity card uses the CPF as its national registration number (Decreto nº 10.977/2022, art. 3) and is issued on security paper or polycarbonate and in digital form (art. 5), carrying a QR code and an ICAO machine-readable zone (art. 11).

Biometric validation

On 28 October 2026 ANATEL announced Technical Standard GT-SEG.2026.11, issued by its Planning and Regulation Superintendence. Mobile operators must identify individuals and individual micro-entrepreneurs by facial recognition with proof of life, compared against

pre-existing biometric databases, public or from private suppliers. The check must be available in physical service channels and on operators' official websites and apps, alternative procedures must exist where biometric validation is not possible, and personal data protection must follow the LGPD. GT-Seg members approved it by consensus `Adopted, phased 2027 to 2029`. ANATEL's supporting technical report (Informe nº 154/2026/PRRE/SPR) states that the procedure requires liveness detection meeting ISO/IEC 30107-3 at presentation attack detection (PAD) level 2 or higher, lets operators contract private identity providers for the reference comparison, and covers every SMP provider, including virtual network operators. Legal persons other than MEI are exempt in this phase, but corporate contracts must record the purpose and actual user of each line.

Event	Biometric validation required by
New prepaid activations	30 September 2027
New postpaid activations, portability, SIM replacement, registration or contract changes requested by the customer	31 December 2027
Re-registration of existing users not yet validated	31 December 2028
Lines not regularised	Subject to suspension, then cancellation, from January 2029, after notice

Retail and third-party capture

Shops that sell prepaid mobile handsets must pass the buyer's registration data to the operator within 24 hours of the sale (Lei nº 10.703/2003, art. 2).

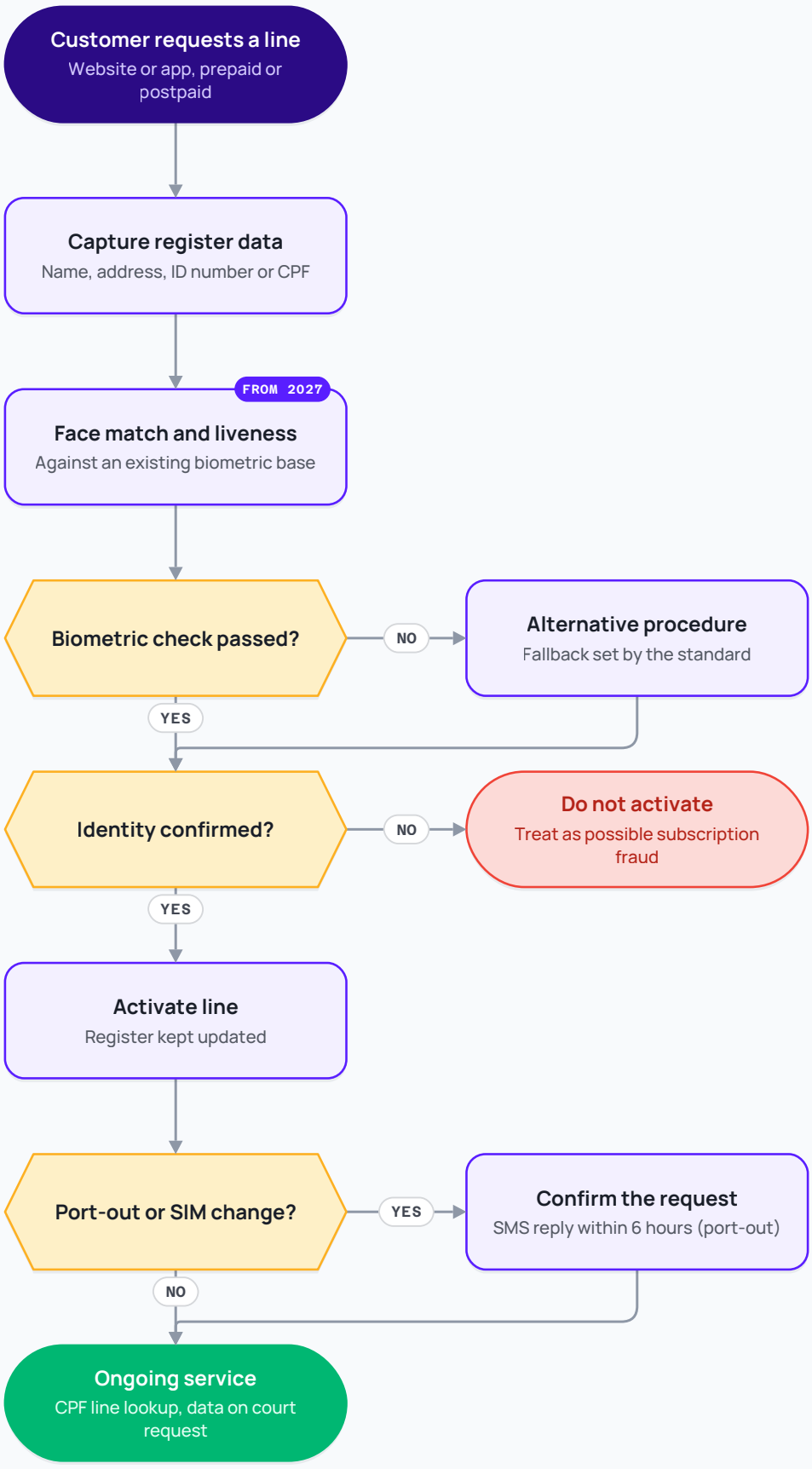


Figure 1. Remote mobile line activation and high-risk line changes in Brazil, with biometric validation as phased in by ANATEL.

5 Digital channels: what's different

> **Bottom line:** the rules are channel-neutral, but the new biometric standard must be offered on websites and apps as well as in shops, so a digital-only operator needs remote face matching with liveness detection by 2027.

Requirement	In person / retail	Online / remote	Difference
Register data (name, address, ID or CPF)	Required	Required	`Same`
Who captures the data	Retailer passes it to the operator within 24 hours	Operator captures it directly	`Differs`
Biometric validation (from 2027)	Required in physical channels	Required on websites and apps	`Same`
Fallback when biometrics fail	Alternative procedure	Alternative procedure	`Same`
Port-out confirmation	SMS reply within 6 hours	SMS reply within 6 hours	`Same`
Activation of a ported number	In person	Other secure identification method that proves the request data	`Differs`
Prior identification to reach customer service	Not addressed	Permitted for digital service channels	`Differs`
Legal basis for biometric processing	LGPD art. 11	LGPD art. 11	`Same`

Remote biometric capture is mandatory, not optional

An online-only operator cannot send customers to a shop; it needs its own remote capture with proof of life, database comparison and fallback `Adopted, phased from 30 Sep 2027`.

Number portability is authenticated the same way in every channel

Under an ANATEL determination in force since 28 August 2023, a customer moving a number must reply "SIM" (yes) to a text message within six hours, or the request is cancelled; it applies in shops, online and by phone. Portability rules now sit in the RGST. Activation at the receiving operator must be done in person or by other secure identification methods, through procedures that prove the data given in the portability request (Annex, art. 100, § 3), so a remote port-in needs a method strong enough to tie the applicant to the request.

Digital service channels may require identification

The General Regulation on Consumer Rights for Telecommunications Services (RGC), in force since 1 September 2025, prohibits conditions that restrict access to digital customer service, but states that requiring prior identification of the consumer to use digital service is not such a restriction (Annex, art. 14, sole paragraph).

Pending

The biometric deadlines, the text-message rules (section 7) and two bills (section 10) will change digital journeys in 2027.

6 Data protection and biometrics

The General Personal Data Protection Law (Lei nº 13.709/2018, LGPD) applies to all subscriber data. Biometric data linked to a natural person is sensitive personal data (art. 5, II). It may be processed with the holder's specific and highlighted consent for specific purposes (art. 11, I) or, without consent, where indispensable to guarantee fraud prevention and the holder's security in identification and authentication processes in electronic systems, unless the holder's fundamental rights prevail (art. 11, II, g). That basis can support the telecom biometric check, which targets lines activated with false or third-party data.

How long biometric data may be kept is governed by the LGPD's general rules. LGPD fines reach 2% of the group's revenue in Brazil in the previous financial year, net of taxes, capped at R$ 50 million per infringement (art. 52, II).

7 Sector-specific obligations

Keeping the prepaid register accurate

Under ANATEL's Projeto Cadastro Pré-Pago, anyone can see on the operators' portal which prepaid lines are linked to their CPF and have unknown lines cancelled (within 24 hours via an attendant, 48 hours automatically); lines without a recognised holder may be cancelled if not updated. Users must report theft or loss of a device, transfer of ownership and any change in their registration data (Lei nº 10.703/2003, art. 4; RGC Annex, art. 6), and the RGC gives consumers the right to transfer a contract to a new holder only if the new holder meets the requirements for an initial contract (Annex, art. 4, XVIII).

Data for criminal investigations

Registration data must be given immediately to a judicial authority on request (Lei nº 10.703/2003, art. 1, § 3). Police and prosecutors may obtain basic registration data without a court order (Lei nº 12.850/2013, art. 15). Telephone operators must keep call origin and destination records for five years (art. 17).

Caller authentication and abusive calls

Provisional Measure (Medida Provisória) nº 1.396/2026, published on 13 October 2026, has force of law but lapses unless Congress converts it (deliberation period to 11 December 2026, extendable) `In force, not yet converted`. Originating operators must authenticate calls and terminating operators must verify them (art. 2); calls from companies must display the business name and logo held in a central numbering database that records number holders and their CNPJ (arts. 4 and 5); and operators must block calls using irregular numbers and suspend abusive callers for 15 days (arts. 3 and 6). From 12 November 2026, ANATEL superintendence decision (Despacho Decisório) nº 100/2026 applies the abuse test across all lines linked to the user's CPF or CNPJ, blocks outgoing calls on all of them and bars new numbers during the block (arts. 1 and 2).

Securing authentication messages

ANATEL Board Decision (Despacho Decisório) nº 2/SCD of 3 November 2026, published on 4 November, sets rules for application-to-person (A2P) text messages `Adopted, deadlines Jan to Feb 2027`. Within 60 days, extendable once, mobile operators must give each short code to a single company, adopt an internal SMS security policy and run automated monitoring for anomalous traffic and identity spoofing (art. 2). Within 90 days they must run a public central directory of short codes, restrict A2P sending to companies identified in it (art. 1) and block messages from unregistered codes (art. 3).

Within 90 days, aggregators and other intermediaries must verify their customers' identity in proportion to risk (art. 6), and platforms used for authentication or transaction authorisation must reach equivalent security outcomes (arts. 7 and 9).

8 Risk indicators and red flags

IDENTITY ABUSE IN MOBILE SERVICES (FROM ANATEL ALERTS AND MEASURES)

- **Line hijacking**: a port-out or SIM change requested by someone posing as the holder.
- **Third-party registration**: activation with another person's CPF or with false data.
- **Unknown lines on a CPF**: a person finds prepaid lines they never opened on the consultation portal.
- **Defective register entries**: lines with no CPF, invalid CPFs, deceased holders or impossible ages.
- **Document workarounds**: lines registered with a passport or foreign document and no further identity data.
- **Spoofed caller ID**: calls carrying an altered originating number.
- **Shared or opaque short codes**: A2P messages whose sender cannot be traced to a verified brand.

9 Enforcement and penalties

ANATEL imposes the sanctions in the General Telecommunications Law: warning, fine, temporary suspension, forfeiture and declaration of unfitness (art. 173). A fine may be imposed alone or with another sanction and may not exceed R$ 50 million per infringement, taking into account the offender's economic condition and proportionality between the seriousness of the fault and the sanction (art. 179). Temporary suspension applies to serious infringements that do not justify forfeiture and lasts no more than 30 days (art. 180).

Lei nº 10.703/2003 adds fines imposed by ANATEL (art. 5): up to R$ 10,000 per infringement for withholding register data from a court (art. 1, § 3), up to R$ 500 for retailers that miss the 24-hour deadline (art. 2), R$ 100,000 for failing to provide stolen-handset lists (art. 3, § 2) and up to R$ 50 for users, with line blocking (art. 4).

In Board decision (Acórdão) nº 207 of 10 August 2026, ANATEL partly upheld an appeal by Claro S.A. and set a total fine of R$ 6,451,430.40 for breaches of rules then in force, including the former General Portability Regulation (Resolution 460/2007, revoked from 3 October 2022 by Resolution 749/2022).

In September 2026 ANATEL also issued six precautionary measures against companies identified as originating or carrying significant volumes of calls showing signs of spoofing.

10 Recent changes and what to watch

- **4 Nov 2026**: ANATEL Board Decision nº 2/SCD on A2P text messages `Adopted, deadlines Jan to Feb 2027`. Firms that send SMS one-time passwords need a registered, exclusive short code and must meet equivalent security outcomes on other channels.
- **28 Oct 2026**: Technical Standard GT-SEG.2026.11 on mandatory biometric validation `Adopted, phased from 30 Sep 2027`. Operators need face matching with liveness in every channel and a re-registration plan for the existing base by the end of 2028.
- **13 Oct 2026**: Provisional Measure nº 1.396/2026 on call authentication, caller identification and a central numbering database `In force, not yet converted`. Abusive-caller blocks, linked to the caller's CPF or CNPJ, apply from 12 November 2026; call authentication and caller identification await ANATEL regulation.
- **Aug 2026**: the Senate approves Bill PL 2.616/2025 (a national register of numbers by CPF and identity validation for SIM activation, portability and ownership transfer) and sends it to the Chamber of Deputies; PL 352/2025, with similar rules, passed the Chamber on 28 October 2025 and awaits the Senate `Bills, not enacted`.
- **10 Aug 2026**: ANATEL Board sets a R$ 6.45 million fine on Claro S.A. for portability and customer-service breaches `Decided on appeal`. Portability failures are enforced with multi-million fines.
- **Sep to Oct 2025**: the new General Regulation on Consumer Rights (RGC, from 1 September) and the RGST (from 27 October) take effect `In force`. Digital channels may require prior identification, and subscription fraud prevention is an explicit duty.

11 What this means for identity verification

- **Data**: capture name, address and CPF (or identity document number) for individuals and CNPJ for companies; validate the CPF, since it is the national key for line lookups.

- **Biometrics**: plan for face matching with liveness at ISO/IEC 30107-3 PAD level 2 or higher against a public or private reference database, in shops, on the web and in apps, by 30 September 2027 for prepaid and 31 December 2027 for everything else.
- **Re-verification triggers**: portability, SIM replacement, ownership transfer and customer-requested registration or contract changes all require biometric validation by 31 December 2027.
- **Fallback**: build an alternative path for customers who cannot complete the biometric check, as the standard requires.
- **Legal basis**: fraud prevention in identification and authentication (LGPD art. 11, II, g) supports biometric processing; document the assessment and limit retention.
- **Back book**: schedule re-registration of every unvalidated user before 31 December 2028 to avoid suspensions from January 2029.

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 face match with biometric liveness detection for line activation, available in apps and on the web as ANATEL's standard requires.
- ID document capture and verification, including the new national identity card with its QR code and machine-readable zone.
- Re-verification flows for portability, SIM replacement and account changes, built in the no-code workflow builder.
- Phone and email verification plus an audit trail for every check, supporting register accuracy and data requests.

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

- **Lei nº 9.472, de 16 de julho de 1997 [General Telecommunications Law]**, arts. 131, 173, 179, 180, Planalto, planalto.gov.br
- **Lei nº 10.703, de 18 de julho de 2003 [Prepaid mobile user registration law]**, arts. 1 to 5, Planalto, planalto.gov.br
- **Lei nº 9.613, de 3 de março de 1998 [Anti-money laundering law]**, art. 9, Planalto, planalto.gov.br
- **Lei nº 13.709, de 14 de agosto de 2018 [General Personal Data Protection Law, LGPD]**, arts. 5, 11, 52, Planalto, planalto.gov.br
- **Lei nº 12.850, de 2 de agosto de 2013 [Criminal organisations law]**, arts. 15 and 17, Planalto, planalto.gov.br
- **Decreto nº 10.977, de 23 de fevereiro de 2022 [National identity card decree]**, arts. 3, 5, 11, Planalto, planalto.gov.br
- **Resolução Anatel nº 765, de 6 de novembro de 2023 [General Regulation on Consumer Rights for Telecommunications Services, RGC]**, Annex arts. 4, 6, 14, Diário Oficial da União, 10 November 2023, in.gov.br
- **Resolução Anatel nº 777, de 28 de abril de 2025 [General Regulation of Telecommunications Services, RGST]**, arts. 2 and 28; Annex arts. 69, 100, 119, 137, 140, 216, 227, 239, 241, Diário Oficial da União, 30 April 2025, in.gov.br
- **Resolução Anatel nº 792, de 14 de outubro de 2026 [Regulatory guillotine; amends RGST art. 251]**, arts. 4 and 7, Diário Oficial da União, 15 October 2026, in.gov.br
- **Resolução nº 720, de 10 de fevereiro de 2020 [General Licensing Regulation]**, Annex arts. 5 and 7, Diário Oficial da União, 12 February 2020, in.gov.br
- **Despacho Decisório nº 100/2026 [ANATEL consumer relations and obligations superintendences; abusive-call blocking under MP 1.396/2026, in force 12 November 2026]**, arts. 1 to 4 and 8, Diário Oficial da União, 19 October 2026, in.gov.br
- **Resolução Anatel nº 781, de 15 de agosto de 2025 [amends General Licensing Regulation art. 5]**, art. 2, Diário Oficial da União, 18 August 2025, in.gov.br
- **Despacho Decisório nº 2/SCD, de 3 de novembro de 2026 [A2P SMS measures]**, arts. 1 to 9, Diário Oficial da União, 4 November 2026, in.gov.br
- **Resolução Anatel nº 749, de 15 de março de 2022 [Numbering Regulation; revokes Resolution 460/2007 from 3 October 2022]**, arts. 2 and 4, Diário Oficial da União, 18 March 2022, in.gov.br
- **Acórdãos de 10 de agosto de 2026, Acórdão nº 207 [ANATEL Board decision, Claro S.A., Process 53500.024931/2020-81]**, Diário Oficial da União, 17 August 2026, in.gov.br
- **"Competências" [Ministry of Communications remit]**, Ministério das Comunicações, updated 19 November 2025, gov.br/mcom
- **"Anatel atualiza Regulamento Geral de Direitos do Consumidor..." [RGC in force]**, ANATEL, 1 September 2025, gov.br/anatel

- **"Anatel aprova validação biométrica obrigatória para usuários de telefonia móvel" [Technical Standard GT-SEG.2026.11]**, ANATEL, 28 October 2026, gov.br/anatel
- **"Conselho Diretor prorroga a entrada em vigor do Novo Regulamento Geral de Direitos do Consumidor..." [RGC postponed to 1 September 2025]**, ANATEL, 29 August 2024, gov.br/anatel
- **PL 2.616/2025 [CadÚnico Telefônico bill]**, Federal Senate, status "remetida à Câmara dos Deputados" (August 2026), senado.leg.br
- **PL 352/2025 [Call identification and SIM activation bill]**, Chamber of Deputies, "Câmara aprova critérios mais rígidos para identificação de chamadas de celular", 28 October 2025, camara.leg.br; Federal Senate record, senado.leg.br
- **Informe nº 154/2026/PRRE/SPR [ANATEL technical report on mandatory biometric validation for SMP users]**, 26 October 2026, Process 53500.000279/2021-90, SEI nº 16481047, ANATEL public document search, sei.anatel.gov.br
- **Medida Provisória nº 1.396, de 9 de outubro de 2026 [Call authentication, identification and blocking; central numbering database]**, arts. 1 to 10, Planalto, planalto.gov.br; Congresso Nacional, deliberation period 13 October to 11 December 2026, congressonacional.leg.br
- **Acórdão nº 310, de 3 de novembro de 2026 [ANATEL Board decision approving the A2P SMS measures]**, Process 53500.104806/2025-68, SEI nº 16533364, ANATEL public document search, sei.anatel.gov.br
- **"Medidas cautelares estabelecem providências sobre chamadas com identificação de origem alterada" [Spoofing precautionary measures]**, ANATEL, 17 September 2026, gov.br/anatel
- **"Portabilidade numérica tem novos procedimentos" [Portability SMS confirmation]**, ANATEL, 28 August 2023, gov.br/anatel
- **"Consumidor pode consultar celulares pré-pagos ligados ao seu CPF" [Projeto Cadastro Pré-Pago]**, ANATEL, 22 January 2020 (modified 17 November 2022), gov.br/anatel