



Identomat

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in Bulgaria

COUNTRY **Bulgaria**

INDUSTRY **Telecom & Mobile Services**

LAST UPDATED **21 October 2026**

KEY REGULATORS **Communications Regulation Commission · Commission for Personal Data Protection**

Key takeaways

- No licence is needed to sell mobile or internet services in Bulgaria. A provider files a notification with the Communications Regulation Commission (the telecom regulator) and needs a separate permit only to use phone numbers or radio spectrum.
- Every SIM, prepaid ones included, must be tied to an identified person: full name, Bulgarian personal number (EGN, or a personal number for foreigners) and permanent address. Anonymous prepaid SIMs have not been allowed since 1 January 2010.
- Telecom providers are not covered by the anti-money laundering law, so no bank-style due diligence applies. A provider may ask for an identity document and check it, including its photo, against the national identity document records, but it may not ask for more personal data than the law sets out.
- Online sign-up is allowed. The contract can be signed electronically where this is technically possible, and a number can be ported with an application signed by qualified or agreed electronic signature, with an eSIM delivered over the air.
- Do not store photocopies or scans of identity documents unless a law allows it. Selfie face matching counts as biometric processing and needs its own legal basis under EU data protection law.

The Bulgarian market is open to new mobile, internet and virtual network operators, including fully digital ones. Entry works on a general authorisation: notification to the Communications Regulation Commission, plus individual permits for numbering resources and spectrum where these are needed. The Commission regulates contracts, number portability and consumer protection in the sector and, since February 2026, also supervises telecom cybersecurity.

The obstacle for a digital entrant is not licensing but identification design. Bulgarian law requires a verified identity behind every prepaid and postpaid line, limits the personal data a provider may request, restricts copying of identity documents and gives the regulator detailed rules on porting that apply equally to app-based and in-store channels.

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

Electronic communications are governed by the Electronic Communications Act (Закон за електронните съобщения, ECA), promulgated in State Gazette (ДВ) No. 41 of 2007 and last amended by State Gazette No. 17 of 2026. Bulgaria is a unitary state, so all authorisations are national.

Regulator	Remit for telecom	Level	Official site
Communications Regulation Commission (Комисия за регулиране на съобщенията, CRC)	Notifications, numbering and spectrum permits, contracts and end-user protection, number portability, inspections and fines; supervisory body for trust service providers under eIDAS; national competent authority under the Cybersecurity Act for communications providers; Digital Services Coordinator	National	crc.bg
Commission for Personal Data Protection (Комисия за защита на личните данни, CPDP)	GDPR supervision; monitoring authority for the security and destruction of retained traffic data	National	cpdp.bg
Consumer Protection Commission (Комисия за защита на потребителите)	Hosts, with the CRC, the sectoral conciliation commission for consumer disputes in electronic communications	National	kzp.bg

European Union
(EUR-Lex)

Directly applicable regulations:
GDPR, eIDAS as amended in 2024,
Digital Services Act, Open Internet
Regulation

Supranational

[eur-
lex.europa.eu](https://eur-lex.europa.eu)

2

Licensing and authorisation

Under Article 66(1) ECA, public electronic communications networks or services are provided after a notification to the CRC. No notification is required for number-independent interpersonal communications services (for example app-based messaging that does not use phone numbers) or for certain non-commercial local radio access (Article 66(2)). Only sole traders and legal entities may provide public electronic communications (Article 69).

Two scarce resources need individual permits. Rights to use numbering resources are granted only by permit (Article 67b), and individual rights to use radio spectrum are granted by registration or permit (Article 66a). A spectrum or numbering permit runs for an initial term of up to 20 years (Article 71(1)). A mobile virtual network operator that uses its own numbers therefore needs a notification plus a numbering permit, but no spectrum permit.

Once notified, a provider must comply with the CRC's General Requirements for Public Electronic Communications (State Gazette No. 108 of 2021, last amended by State Gazette No. 113 of 2025), which cover annual reporting, publication of terms and coverage maps, notices of contract changes and electronic signature of contracts.

Providing public services without a notification is punishable by a fine of 3,000 to 15,000 leva (Article 324(6) ECA). Using numbers or spectrum without the required permit carries 30,000 to 300,000 leva (Article 324(1)).

3

Identity framework (AML rules do not apply)

Telecom providers are not obliged entities under the Measures Against Money Laundering Act (Закон за мерките срещу изпирането на пари, State Gazette No. 27 of 2018, consolidated to State Gazette No. 51 of 2026). Article 4 lists the obliged entities, from credit institutions and payment service providers to gambling organisers and crypto-asset service providers, and electronic communications providers are not among them. A telecom group that provides payment services in its own right is covered for that activity as a payment service provider under Article 4, item 2, not as a telecom operator.

Identification in the sector is governed by the ECA instead, through four provisions that work together:

Mandatory identification of prepaid users

Since 1 January 2010, providers must collect the data needed to identify every user of prepaid services (§ 80(1) of the transitional provisions to the 2009 amending act, as amended in 2015). Postpaid customers are identified as parties to the contract under Article 227.

What "identification data" means

For individuals: full name, personal number (EGN) and permanent address; for foreigners, the personal number. For companies and sole traders: name, seat, registered address and identification code (§ 1, item 83 of the Supplementary Provisions).

A ceiling on data collection

Providers may not require more data than the identification data in Article 248(2)(2)(a), unless a law provides otherwise or the service cannot be provided without it (Article 249(1)). Service may not be made conditional on consent to other uses of the data (Article 249(2)).

Document and register checks

To identify the customer or a representative, ensure accuracy and prevent abuse, a provider may require an identity document, record its type, number, date and place of issue and issuer, and verify the data and the document photo against the national records of Bulgarian identity documents (fingerprints excluded) and the unified register of foreigners (Article 249(6)).

There is no transaction monitoring or suspicious activity reporting duty for telecom providers. The relevant record-keeping duty is data retention: traffic, location and subscriber identification data needed to trace and identify communications are kept for six months for national security and serious crime purposes and then destroyed (Article 251b). For prepaid services this includes the date and time of initial activation and the cell from which the service was activated (Article 251i(5)(2)).

4

Identity verification and onboarding

The ECA prescribes what must be known about a customer, not how it must be proved. It sets no identity assurance level, no list of accepted remote methods and no liveness standard. Three rules shape the verification step in practice.

Accepted documents and register checks

Article 249(6) refers to a "personal document" (личен документ), meaning a Bulgarian or foreign identity document. For Bulgarian documents the provider may confirm the name, EGN, address and document details, and compare the holder against the document photo held in the national records; foreign nationals can be checked against the unified register of foreigners. Access to these checks must be limited to staff the provider has expressly designated.

No photocopies unless a law allows it

Article 25g of the Personal Data Protection Act (Закон за защита на личните данни) allows a controller or processor to copy an identity document, driving licence or residence document only where a law provides for it. Article 249(6) ECA permits recording the document's details and checking it against official records, but it does not provide for copying the document. Onboarding flows that capture document images should be designed around data extraction and verification rather than retention of the image, and any retention needs a specific legal basis.

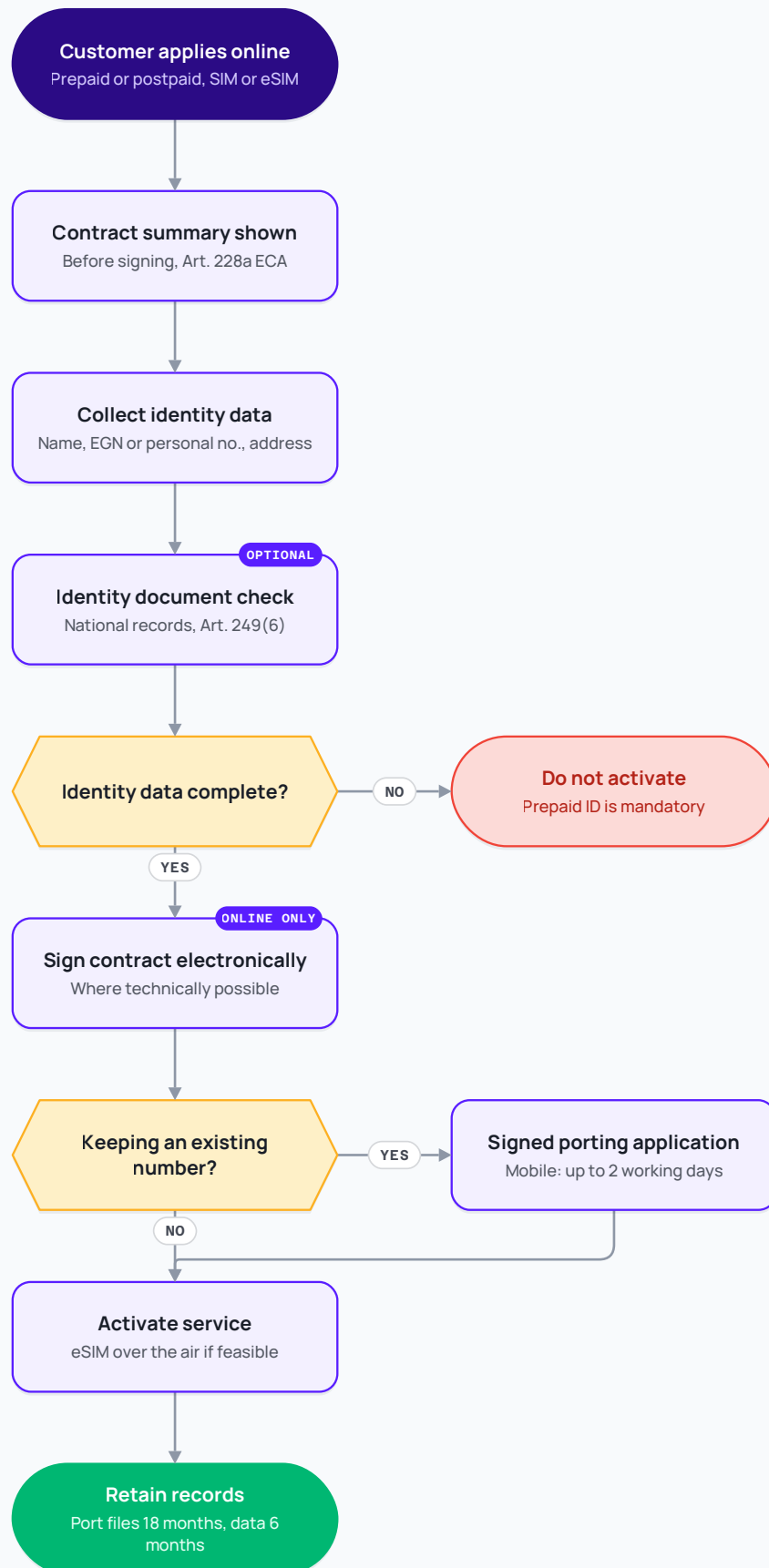


Figure 1. Online SIM or eSIM activation in Bulgaria, with optional number porting.

Bottom line: the identification duties are channel-neutral, but Bulgarian rules expressly accommodate online sales: contracts and porting requests may be signed electronically, and a ported number can be activated on an eSIM over the air without the customer visiting a shop.

Requirement	In person / land-based	Online / remote	Difference
Identification data for prepaid and postpaid	Name, EGN, permanent address	Name, EGN, permanent address	Same
Document and register check	Permitted, not mandatory	Permitted, not mandatory	Same
Copying the identity document	Only if a law provides for it	Only if a law provides for it	Same
Signing the contract	Written signature	Electronic signature where technically possible	Differs
Contract summary	Free, before conclusion	Free, before conclusion, including distance contracts	Same
Porting application	Signed standard form at the shop or dealer	Qualified or agreed electronic signature, by agreement	Differs
SIM delivery when porting	SIM cards handed over	No handover duty for distance contracts; over-the-air provisioning where feasible	Differs
Data the provider may request	Identification data only	Identification data only	Same

Electronic contracts

Article 17(1) of the CRC General Requirements allows any end-user contract under Chapter 14 ECA to be signed under Article 13 of the Electronic Document and Electronic Trust Services Act "where technically possible". The ECA requires the contract summary to be

provided free of charge before conclusion, including for distance contracts (Article 228a(2)); if that is technically impossible, the summary follows within seven days and the contract takes effect only once the customer confirms (Article 228a(3)).

Remote porting and eSIM

Under Article 33(3) of the CRC Functional Specifications for number portability, a porting application may be filed electronically, signed with a qualified electronic signature or another type of electronic signature agreed between the recipient provider and the customer, where this is technically possible and agreed. The application must state that porting will be completed by over-the-air provisioning where technically feasible (Article 33(2)(8)), and the duty to hand over SIM cards does not apply when the application and contract are concluded without the simultaneous physical presence of the parties (Article 35(2)).

Same data, same ceiling

The data minimisation rules bind both channels: a provider may not ask for more than the identification data (Article 249(1) ECA), and porting providers may not request more data than the application form lists (Article 33(9) of the Specifications).

6 Data protection and biometrics

The GDPR applies directly, supervised by the CPDP, and the ECA states that providers process customers' personal data under the ECA and, for matters it does not regulate, under the GDPR (Article 249(5)).

Biometric data, defined in Article 4(14) GDPR to include facial images processed to uniquely identify a person, is special category data under Article 9(1). A selfie-to-document face match therefore needs an Article 9(2) condition, usually explicit consent (Article 9(2)(a)). Article 249(2) ECA separately bars making service conditional on consent to other uses of data, so a non-biometric alternative is the safer design. The photo comparison against national records in Article 249(6) ECA is a statutory check of the document photo, not a general authorisation for biometric templates.

Retained traffic data is subject to its own regime. The CPDP is the monitoring authority for the security of data retained under Article 251b (Article 261a), and by the 5th of each month providers must send the CPDP a record of data destroyed in the previous month (Article 251zh(1)). Providers and their staff must keep communications, traffic and location data and customer identification data confidential (Article 245).

Number portability and port-out fraud controls

End users have the right to keep their numbers when changing provider (Article 134 ECA). The recipient provider leads the process, and providers must not port numbers without the end user's express consent (Article 134a(1)). The application must carry the customer's full name, EGN (or name and personal number for foreigners), the numbers, signature and the date and time of filing (Article 33(2) of the Specifications). The donor provider may refuse only on listed grounds, including incomplete or inaccurate name and EGN data (Article 36(1)), and the recipient must refuse applications filed by an unauthorised third party (Article 36(2)). Mobile numbers must be ported within two working days with a porting window of up to five hours (Article 38(1)). Providers keep every application and related message for at least 18 months (Article 33(10)). Delay or porting without consent entitles the customer to compensation of at least EUR 1.02 per day per number from 1 January 2026 (Article 40(3)). Porting is free to end users (Article 136a ECA).

Unpaid debt checks when devices are sold

When a contract includes a handset or other terminal device, a provider may ask other providers whether the customer owes them more than 15 per cent of the national minimum wage for at least 30 days, under the conditions in Article 249(3) ECA and joint CRC and CPDP guidelines adopted under Article 249(4), which require a secure, encrypted channel.

Network security and incident reporting

Since the Cybersecurity Act amendments of February 2026, security obligations for communications providers sit in the Cybersecurity Act rather than the ECA. Providers of public networks or publicly available services that are at least medium-sized are essential entities, the CRC is their national competent authority, and significant incidents require an early warning within 24 hours and an incident notification within 72 hours.

8 Risk indicators and red flags

IDENTITY-ABUSE PATTERNS THE BULGARIAN RULES TARGET

- **Port-out without consent:** a porting request the customer did not make, which Article 134a(1) ECA prohibits.
- **Third-party porting application:** a request filed by someone not authorised by the customer or an heir (Specifications Article 36(2)).
- **Mismatched identity data:** name or EGN that does not match the donor provider's records (Specifications Article 36(1)).
- **Document details that fail the register check:** data or photo that does not match national identity document records (Article 249(6) ECA).
- **Prepaid activation without identification:** a SIM activated before identification data is captured, contrary to § 80 ECA.
- **Unidentified marketing senders:** messages whose sender cannot be identified, which Article 261(5) ECA prohibits.
- **Unlawful use of the network for gain:** use of a network without a legal basis causing damage to the operator (Article 328(2) ECA).

9 Enforcement and penalties

CRC inspectors establish violations of the ECA with written acts, and fines follow the Administrative Violations and Sanctions Act procedure (Article 337). Penalties are fixed ranges per violation. For most listed violations, fines set for individuals apply to companies as pecuniary sanctions of the same amounts (Article 336). Amounts below are stated in leva, as in the Act; under § 5 of the Euro Introduction Act, acts that set fines in leva continue to apply under its conversion rules after the euro changeover.

Violation	Provision	Range (leva)
Providing services without notification	Art. 324(6)	3,000 to 15,000
Breach of the General Requirements	Art. 326	3,000 to 15,000
Breach of portability rules or Specifications	Art. 326a(1)-(2)	5,000 to 60,000

Breach of end-user protection rules (Chapter 14)	Art. 326a(3)	5,000 to 100,000
Failure to retain data under Article 251b	Art. 327(4)	3,000 to 25,000
Any other breach of the ECA or its implementing acts	Art. 335	500 to 5,000

Data protection breaches, including unlawful document copying or biometric processing, are sanctioned by the CPDP under the GDPR. In 2025 the CRC issued 92 acts establishing violations of the ECA: 20 for breaches of Chapter 14 (end-user contracts), 19 for Chapter 15 (confidentiality and data protection) and 6 for breaches of the portability Specifications after 95 portability inspections. Courts confirmed 25 CRC penalty decisions issued in 2025 and annulled none, according to the CRC's 2025 annual report.

10 Recent changes and what to watch

- **Applies from December 2027** Private relying parties that are required by law or contract to use strong user authentication for online identification must accept European Digital Identity Wallets on request within 36 months of the implementing acts (Regulation (EU) 2024/1183, Article 5f(2)); micro and small enterprises are exempt.
- **Member State deadline December 2026** Bulgaria must provide at least one European Digital Identity Wallet within 24 months of the implementing acts, which entered into force on 24 December 2024 (Article 5a(1)). Telecom onboarding flows should plan to accept it.
- **In force** 13 February 2026: the Cybersecurity Act amendments (State Gazette No. 17 of 2026) make the CRC the national competent authority for communications providers and repeal the ECA's network security section.
- **In force** 1 January 2026: CRC amendments to the portability Specifications and General Requirements (State Gazette No. 113 of 2025) restate amounts in euro, including minimum porting compensation of EUR 1.02 per day.
- **In force** 21 November 2025: ECA amendments (State Gazette No. 99 of 2025) designate the CRC as Digital Services Coordinator under the Digital Services Act.
- **In force** 7 November 2025: State Gazette No. 95 of 2025 adds further purposes for which retained data may be used under Article 251b(2) ECA; the six-month retention period is unchanged.

- **Capture exactly the statutory data set:** full name, EGN or foreign personal number and permanent address for individuals; name, seat, address and code for companies. Asking for more needs a legal reason.
- **Verify against national records where possible:** Article 249(6) ECA permits checking Bulgarian document data and photo, and foreigners' data, against official registers through designated staff.
- **Extract, verify, do not keep scans:** Article 25g of the Personal Data Protection Act restricts copying identity documents to cases a law provides for.
- **Treat face matching as optional and consent-based:** biometric matching is special category processing under the GDPR; offer an alternative route.
- **Use electronic signatures for contracts and porting:** qualified or agreed signatures are recognised, and eSIM over-the-air delivery removes the need for a shop visit.
- **Re-verify at port-out:** match name and EGN before porting, refuse unauthorised third-party requests and keep porting records for 18 months.
- **Prepare for digital identity wallets:** Bulgaria's wallet is due by December 2026, with acceptance duties for some private relying parties from December 2027.

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:

- Online SIM and eSIM onboarding that captures the statutory identity data set, with ID document capture and verification, including NFC chip reading.
- Optional face match and biometric liveness, configured as a consent-based step with a non-biometric alternative route.
- E-signatures for end-user contracts and porting applications completed remotely.
- Phone and email verification and a no-code workflow builder to re-verify customers before port-out or SIM replacement.
- Cloud, on-premises or hybrid deployment to fit data retention and data minimisation requirements.

[Request a meeting](#)

DISCLAIMER

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

Sources

- **Закон за електронните съобщения (Electronic Communications Act)**, State Gazette No. 41 of 2007, consolidated text as amended to State Gazette No. 100 of 25 November 2025 (text dated 26 November 2025), Articles 66 to 71, 134 to 136a, 227 to 228a, 245, 248 to 251i, 261, 261a, 324 to 337, § 1 item 83 of the Supplementary Provisions and § 80 of the 2009 transitional provisions, published by the Communications Regulation Commission, crc.bg
- **Закон за изменение и допълнение на Закона за киберсигурност (Act amending the Cybersecurity Act)**, State Gazette No. 17 of 13 February 2026, including § 52 amending the Electronic Communications Act, dv.parliament.bg; adoption record, parliament.bg

- **Общи изисквания при осъществяване на обществени електронни съобщения (General Requirements for Public Electronic Communications)**, CRC, State Gazette No. 108 of 2021, as amended to State Gazette No. 113 of 23 December 2025, Articles 1, 2, 15 to 17, crc.bg
- **Функционални спецификации за осъществяване на преносимост на национално значими номера (Functional Specifications for number portability)**, CRC, State Gazette No. 101 of 2021, as amended to State Gazette No. 113 of 23 December 2025, Articles 33 to 40, crc.bg
- **Указания относно предоставяне на информация за неплатени задължения на крайния ползвател (Guidelines on information about end users' unpaid obligations under Article 249(3) ECA)**, CRC and CPDP, crc.bg
- **CRC subordinate acts under the Electronic Communications Act (list of current rules)**, crc.bg
- **Годишен доклад на КРС за 2025 г. (CRC Annual Report 2025)**, 2026, control and enforcement chapter, crc.bg
- **Закон за мерките срещу изпирането на пари (Measures Against Money Laundering Act)**, State Gazette No. 27 of 2018, consolidated to State Gazette No. 51 of 5 June 2026, Article 4, published by the Financial Supervision Commission, fsc.bg
- **Закон за защита на личните данни (Personal Data Protection Act)**, State Gazette No. 1 of 2002, as amended to State Gazette No. 70 of 2024, Article 25g, cpdp.bg
- **Regulation (EU) 2016/679 (General Data Protection Regulation)**, Articles 4(14) and 9, eur-lex.europa.eu
- **Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 (European Digital Identity Framework)**, Articles 5a and 5f, eur-lex.europa.eu
- **Commission Implementing Regulation (EU) 2024/2977 on person identification data and electronic attestations of attributes for European Digital Identity Wallets**, entry into force 24 December 2024, eur-lex.europa.eu