



Identomat

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in Ukraine

COUNTRY **Ukraine**

INDUSTRY **Telecom & Mobile Services**

LAST UPDATED **16 October 2026**

KEY REGULATORS **National Commission for the State Regulation of Electronic Communications, Radio Frequency Spectrum and the Provision of Postal Services · Cabinet of Ministers of Ukraine · National Bank of Ukraine**

Key takeaways

- No licence is needed to sell mobile or internet services in Ukraine: a provider files an online notification with the telecoms regulator. Radio spectrum and phone numbers still need their own licences or permits.
 - Prepaid SIM and eSIM cards can still be sold and used anonymously. Customer identification is a right the customer may exercise, not a condition for getting service.
 - Identification becomes compulsory at specific moments: replacing a lost SIM or eSIM, refunding a prepaid balance, porting a number to another operator, and using a number for commercial calling.
 - Online, a SIM or eSIM may be replaced only after a high-assurance electronic identity check. Every customer must be offered the option to block remote replacement entirely, at sign-up and at any time.
 - Operators are not covered by anti-money laundering (AML) rules. Carrier billing and airtime transfers are allowed only within caps tied to the minimum wage and require registration with the National Bank of Ukraine.
-

The Ukrainian mobile market is open to new entrants, including virtual operators, and online and eSIM sales are permitted. The National Commission for the State Regulation of Electronic Communications (NCEC) licenses spectrum and numbering, sets the customer identification and number portability procedures, and fines operators. The Cabinet of Ministers sets the service rules that govern SIM replacement.

The main obstacle for a new entrant is that Ukraine regulates the moments of highest fraud risk rather than the point of sale. A provider must build a compliant remote identification channel, a high-assurance check for SIM replacement and a remote-replacement block, while still serving customers who choose to stay anonymous. All of this operates under martial law, which adds service obligations for users in combat and occupied areas.

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 identity	Level	Official site
National Commission for the State Regulation of Electronic Communications, Radio Frequency Spectrum and the Provision of Postal Services (NCEC)	Register of providers, spectrum and numbering, customer identification procedure, number portability, supervision and fines	National	nkek.gov.ua
Cabinet of Ministers of Ukraine	Rules for the provision and receipt of electronic communications services (contracts, SIM replacement, martial-law duties)	National	kmu.gov.ua
Ministry of Digital Transformation of Ukraine	Electronic communications and electronic identification policy; Diia state services portal	National	thedigital.gov.ua
National Bank of Ukraine (NBU)	Register of limited payment service providers (carrier billing, airtime transfers)	National	bank.gov.ua

Ukraine is a unitary state: every rule here applies nationally.

2 Licensing and authorisation

Electronic communications are provided under a general authorisation. Under Article 16 of the [Law of Ukraine on Electronic Communications No. 1089-IX of 16 December 2020](#), a provider files a notification through the NCEC's electronic regulatory platform, signed with a qualified electronic signature, within one month of starting activity. Continuing without one is prohibited. The NCEC enters the provider in the register of providers within five working days and charges no fee. Interpersonal communications services that do not use numbers, such as app-based messaging, are exempt from the notification duty.

Article 18 sets an exhaustive list of general authorisation conditions. For identity and fraud teams the relevant ones are protecting personal data and communications confidentiality, providing lawful interception access, blocking unlicensed gambling websites on instruction from the gambling regulator, and supplying the NBU with information it needs to police limited payment services.

Mobile network operators and virtual operators that use spectrum or numbers also need the corresponding spectrum licence or numbering permit (Articles 48 and 75). Operating without a notification exposes the provider to confiscation of the resulting income or, where income cannot be determined, a fine of 10,000 times the non-taxable minimum income of citizens (Article 126(1)(1)).

3 Identity framework (AML rules do not apply)

Telecom operators are not obliged entities under the [Law of Ukraine No. 361-IX of 6 December 2019 on prevention and counteraction to money laundering](#). Article 6(2) lists banks and other financial institutions, payment system operators, postal operators that provide payment services, and designated professions, but not providers of electronic communications. Operators therefore have no customer due diligence, beneficial ownership, transaction monitoring or suspicious activity reporting duties as telecom providers.

Customer identity is instead governed by three instruments:

Law on Electronic Communications

Article 104(5) gives every end user the right to receive services anonymously, and the right to identify themselves, including remotely with a medium- or high-assurance electronic identification means. Article 107(2) makes identification compulsory before restoring service to an anonymous user who has lost a SIM or eSIM.

Service Rules (Resolution No. 761)

Cabinet of Ministers Resolution No. 761 of 25 June 2025 sets how contracts are concluded, when identification is required and how a lost SIM or eSIM is replaced. It replaced the 2012 telecommunications rules.

Identification Procedure (Resolution No. 235)

NCEC Resolution No. 235 of 7 December 2022 fixes the data an operator may collect, the paper, remote and video channels, and record retention.

Where telecoms touch payments

Article 8 of the [Law of Ukraine on Payment Services No. 1591-IX](#) treats certain operator payments as limited payment services: paying for digital content, mobile tickets, charitable donations by text, transfers between subscribers, withdrawing a mobile balance to a payment account, and paying for utilities, taxes and fines. A single operation may not exceed 37% of the statutory minimum wage, and an individual subscriber's monthly total may not exceed one minimum wage. A subscriber's operations below 37% of the minimum wage in a month fall outside the regime. Above that, the operator must be included in the NBU's register of limited payment service providers. An operator that exceeds the caps must stop and apply for a full payment licence (Article 8(6)), at which point AML obligations follow.

4

Identity verification and onboarding

A customer can activate and use a prepaid SIM or eSIM without giving any personal data. Resolution No. 761 (paragraph 7) prohibits discriminatory conditions for anonymous users unless the law or the Rules provide for them. When a customer does identify, Resolution No. 235 controls the process.

Data set and documents

For an individual, the application contains full name, the series and number of an identity document listed in Article 13 of the Law on the Unified State Demographic Register, the taxpayer registration number and register record number if the person has them, and the phone number or account being identified. Non-residents give a passport or another document valid for transactions in Ukraine. Legal entities give their name and state registry code. An operator may not demand any other document or data (section II, point 10), may not refuse identification when the application is complete (point 11) and may not charge for it (point 12). Only individuals aged 14 or over can be identified. Customers may submit an electronic copy of their e-passport through the Diia portal or app.

Proving control of the SIM

Every channel requires proof that the applicant controls the active SIM: presenting the card, quoting a one-time password sent to the number, or giving a secret word agreed with the operator. For M2M and Internet of Things cards the operator sets its own procedure.

Remote and video channels

Remote applications are filed on the operator's website, customer account or app, signed with a qualified electronic signature or an advanced electronic signature based on a qualified certificate. An operator may also accept another electronic identification means that belongs to a scheme approved by the Cabinet of Ministers. Where an operator offers video verification, the session must be real-time and uninterrupted, recorded in full with the customer's consent, and opened with the customer quoting a one-time password sent to the number. The operator is responsible for the identification, must record it within one working day and must keep the record for the life of the contract plus the statutory limitation period.

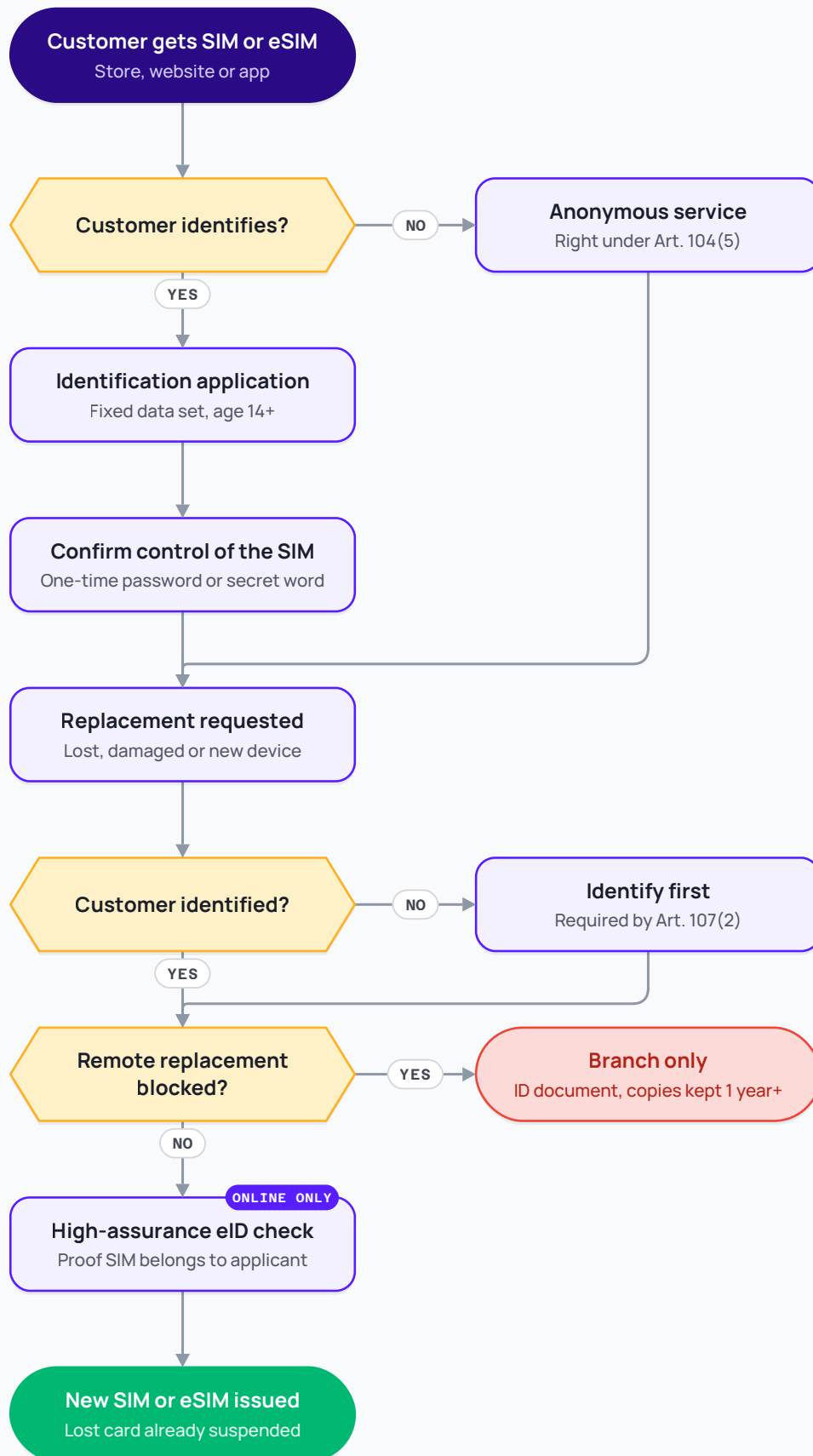


Figure 1. SIM or eSIM activation and remote replacement under Ukrainian rules.

Bottom line: Selling and activating a SIM or eSIM online is treated like a store sale and can stay anonymous, but replacing a SIM or eSIM remotely requires a high-assurance electronic identity check, and customers can switch remote replacement off altogether.

Requirement	In person (store)	Online / remote	Difference
Anonymous activation	Permitted	Permitted	Same
Concluding the contract	Written, oral, public or accession contract	Consent by electronic identification or an active recorded action	Differs
Voluntary identification	Paper application, identity document shown	Qualified or advanced signature, approved eID scheme, or recorded video	Differs
Data an operator may collect	Fixed list in Resolution No. 235	Same fixed list	Same
SIM or eSIM replacement	Identity document; signed copies kept at least one year	High-assurance electronic identification only	Differs
Option to block replacement	Branch replacement always available	Customer may block remote replacement	Differs
Number porting by an anonymous user	Identification application plus SIM control	One-time password plus live confirmation call; Diia channel available	Differs
Record retention	Contract term plus limitation period	Same; video recordings stored under data protection rules	Same

Remote SIM and eSIM replacement

Paragraph 63 of the [Rules approved by Cabinet of Ministers Resolution No. 761 of 25 June 2025](#) allows only two routes for replacing or restoring a SIM or eSIM: a visit to the provider's

office with an identity document, or a remote application using electronic identification at the high assurance level under the [Law on Electronic Identification and Electronic Trust Services No. 2155-VIII](#). In both cases the provider must establish, on evidence, that the lost card belongs to the applicant. Medium-assurance means, which are enough for voluntary identification, are not enough for replacement. At contract signing, and at any time afterwards including through electronic channels, the customer must be offered the option to block remote replacement.

Assurance levels

The levels are defined in the [Technical Regulation approved by Cabinet of Ministers Resolution No. 577 of 16 May 2025](#), in force since 22 November 2025. It is based on Commission Implementing Regulation (EU) 2015/1502, defines low, medium and high levels, requires at least two authentication factors from the medium level, and refers to the national adoptions of the ISO/IEC 30107 standards on biometric presentation attack detection. A provider designing a remote replacement flow should confirm that the identification means it relies on has been assessed at the high level under this regulation.

Remote contracts and porting

Article 112(1) of the Law allows a contract to be concluded remotely by consent given through electronic identification, or by an active action of the user recorded by the provider's equipment, and the user may demand evidence of that consent. Number porting applications can be filed remotely, including through the Diia portal and app, since NCEC Resolution No. 417 of 2 July 2025 amended the porting procedure.

6 Data protection and biometrics

The [Law of Ukraine on Personal Data Protection No. 2297-VI](#) applies to all subscriber data, and protecting personal data is itself a general authorisation condition (Article 18(3)(3) of the Law on Electronic Communications). Resolution No. 235 requires operators to tell identified customers who controls their data, what is collected, why, and to whom it is passed, and to publish directory entries only with consent.

Biometric data is a special category: Article 7 of the data protection law prohibits processing it unless an exception applies, the most relevant being the data subject's unambiguous consent. A telecom operator that adds face matching or liveness to identification or replacement therefore needs explicit consent, because no telecom rule requires biometrics. Video verification under Resolution No. 235 already requires consent

to record the session in full, and the recording must be stored under the data protection rules.

Article 119 of the Law on Electronic Communications makes providers responsible for keeping subscriber data, traffic data and location data confidential. Article 121 allows access to subscriber information and traffic facts only on a decision of a prosecutor, a court or an investigating judge.

7 Sector-specific obligations

Number portability

Porting is governed by the [Procedure approved by NCEC Resolution No. 181 of 10 April 2024](#), as amended. Only contract customers or identified customers can port (Article 113(2) of the Law), so an anonymous customer files an identification application with the receiving operator together with the porting request. An anonymous mobile subscriber must also confirm control of the number by quoting a one-time password sent to it, and confirm consent during a live call from the receiving operator. A port is refused if the right to the number belongs to someone else, if fewer than 30 days have passed since the last port, or if the data is incomplete or false. The customer may withdraw until four working hours before the scheduled port.

Lost cards, refunds and anonymous balances

An anonymous customer must identify to recover unused funds, which is possible for two months after the prepaid card expires (Article 106(4)), and to restore service after losing a SIM, eSIM or router settings (Article 107(2)). On a report of loss the provider must suspend service promptly, free of charge, after checking the card belongs to the reporter (paragraph 63 of the Rules).

Commercial calling and fraud blocking

A user who makes commercial calls must sign a separate contract and be identified. A provider that detects commercial calls without one must curtail service on the number until the user is identified and contracted (paragraph 58). Providers must block individual numbers and services where fraud or unauthorised interference has been confirmed (paragraph 57).

Martial-law duties

For the duration of martial law, paragraph 48 of the Rules prohibits providers from cutting service for lack of funds to users in combat or occupied areas listed by the Ministry of Development, and from deactivating SIMs or eSIMs last connected in those areas. When such a card first reconnects, the provider must give at least two months of free mobile voice, text and internet within the user's tariff. Under Article 115 of the Law, all networks serve national security, defence and law-enforcement needs during martial law.

8

Risk indicators and red flags

IDENTITY AND FRAUD INDICATORS NAMED IN UKRAINIAN RULES

- **SIM swap for account takeover:** SIM reissue used to take over financial, document and communication accounts, identified in the Cabinet's 2030 electronic communications strategy.
- **Replacement request on an anonymous number:** no identification on file, so the applicant must identify before any reissue.
- **Remote replacement despite a block:** any remote request on a number whose holder has disabled remote replacement.
- **Unproductive calling patterns:** under paragraph 4(19) of the Rules, mostly short or unanswered calls, half or more of calls to different numbers within seven days, or autodialling.
- **Complaint spikes:** more than 0.05% of a number's outgoing calls drawing complaints within seven days.
- **Voice-only numbers:** a mobile number used only for outgoing calls, with no texts or data and almost no answered incoming calls.
- **Commercial calls without a contract:** advertising calls from a number with no commercial calling contract or identification.
- **Refiling and anomalous traffic:** traffic disguised as another type, or calls atypical for the user's profile, listed as unauthorised interference.

Enforcement and penalties

The NCEC imposes administrative and economic sanctions on providers under Article 126 of the Law on Electronic Communications. Fines are set as multiples of the non-taxable minimum income of citizens or as a percentage of revenue:

Breach	Sanction	Basis
Breach of rules on services to end users (including identification and SIM replacement)	1,000 to 5,000 times the non-taxable minimum, per breach, under an NCEC methodology	Art. 126(1) (5)
Operating without a notification; unlicensed spectrum use	Confiscation of income, or 10,000 times the minimum if income cannot be determined	Art. 126(1) (1)
Missing or false reporting	1,000, 2,000 or 5,000 times the minimum for small, medium and large firms; doubled tiers for repeat breaches in a year	Art. 126(1) (3)
Failing to obey an NCEC order or obstructing an inspection	0.1% to 0.3% of the previous year's revenue from the services concerned	Art. 126(1) (6)
Failing to block unlicensed gambling sites	2,000 times the minimum; 4,000 for a repeat in a year	Art. 126(1) (12)

Before sanctioning, the NCEC must notify the provider, hold a meeting and allow it to respond or fix the breach. Sanctions may be imposed within six months of detection and no later than one year after the breach, and can be appealed to court (Article 127).

Recent changes and what to watch

- **September 2026:** Law No. 4986-IX of 16 September 2026 added Article 255-4 to the Criminal Code on organised electronic-communications fraud groups. **In force** Expect closer law-enforcement interest in SIM misuse and call-centre traffic.
- **July 2026:** the last provisions of Resolution No. 761 took effect one year after publication, including advance notice of contract expiry. **In force** Update customer notification templates.

- **May 2026:** Cabinet Resolution No. 635 of 20 May 2026 amended the martial-law service duties in paragraph 48 of the Rules. **In force** Recheck free-service and non-deactivation logic for users returning from affected areas.
- **March 2026:** the number portability procedure was amended again (edition of 2 March 2026). **In force** Review porting flows against the current text.
- **November 2025:** the eID assurance level Technical Regulation (Resolution No. 577) took effect. **In force** Confirm the assurance level of any eID used for remote SIM replacement.
- **October 2025:** the new Service Rules (Resolution No. 761) replaced the 2012 rules, introducing high-assurance remote SIM replacement and the remote-replacement block. **In force** Remote replacement flows built on weaker checks must be rebuilt.
- **July 2025:** NCEC Resolution No. 417 allowed porting applications through the Diia portal. **In force** Receiving operators must accept this channel.

11 What this means for identity verification

Identification is not a gate at activation, so the critical identity events are later in the customer lifecycle: voluntary identification, SIM or eSIM replacement, porting, refunds and commercial calling. Each needs its own verified flow.

Collect only the fixed data set, from customers aged 14 or over, free of charge, and prove control of the active SIM in every channel. Remote SIM or eSIM replacement needs high-assurance electronic identification and a per-customer block flag checked by every remote channel; in-store replacement needs signed document copies kept for at least one year. Biometric checks need explicit consent, video sessions must be recorded with consent, and identification records are kept for the contract term plus the limitation period.

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 subscriber identification with ID document capture and verification, including NFC reading of e-passports, collecting only the data fields the operator needs.
- Video KYC sessions with full recording and an audit trail for operators that offer video verification.
- Biometric liveness and face match as an added step before remote SIM or eSIM replacement, with consent capture.
- Phone verification by one-time password to confirm control of the active number before identification or porting.
- No-code workflows that route replacement requests to in-store handling when a customer has blocked remote replacement.

[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 України «Про електронні комунікації» № 1089-IX від 16.12.2020 [Law on Electronic Communications], edition of 30 May 2026, Articles 16, 18, 104, 106, 107, 112, 113, 115, 119, 121, 125 to 127, zakon.rada.gov.ua
- Постанова КМУ № 761 від 25.06.2025 «Про затвердження Правил надання та отримання електронних комунікаційних послуг» [Service Rules], edition of 22 May 2026, paragraphs 4, 7, 48, 50, 51, 55 to 58, 63, 64, zakon.rada.gov.ua

- Постанова НКЕК № 235 від 07.12.2022 «Про затвердження Порядку ідентифікації кінцевих користувачів послуг» [Identification Procedure], registered with the Ministry of Justice No. 25/39081, zakon.rada.gov.ua
- Постанова НКЕК № 181 від 10.04.2024 «Про затвердження Порядку надання послуг перенесення номерів» [Number Portability Procedure], edition of 2 March 2026, as amended by Resolution No. 417 of 2 July 2025, zakon.rada.gov.ua
- Постанова КМУ № 577 від 16.05.2025 [Technical Regulation on requirements for electronic identification means and assurance levels], zakon.rada.gov.ua
- Закон України «Про електронну ідентифікацію та електронні довірчі послуги» № 2155-VIII [Law on Electronic Identification and Electronic Trust Services], edition of 18 December 2024, zakon.rada.gov.ua
- Закон України № 361-IX від 06.12.2019 [Law on prevention and counteraction to money laundering], edition of 26 June 2026, Article 6, zakon.rada.gov.ua
- Закон України «Про платіжні послуги» № 1591-IX [Law on Payment Services], edition of 26 June 2026, Article 8, zakon.rada.gov.ua
- Закон України «Про захист персональних даних» № 2297-VI [Law on Personal Data Protection], edition of 14 June 2025, Articles 7 and 11, zakon.rada.gov.ua
- Розпорядження КМУ № 546-р від 04.06.2025 [Strategy for the development of electronic communications to 2030], zakon.rada.gov.ua
- Кримінальний кодекс України № 2341-III [Criminal Code], edition of 18 September 2026, Article 255-4 as added by Law No. 4986-IX, zakon.rada.gov.ua