



Identomat

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in Poland

COUNTRY **Poland**

INDUSTRY **Telecom & Mobile Services**

LAST UPDATED **20 October 2026**

KEY REGULATORS **President of the Office of Electronic Communications (UKE) · President of the Personal Data Protection Office (UODO)**

Key takeaways

- Mobile and fixed telecom providers in Poland are not covered by the anti-money laundering (AML) law, but every subscriber, including prepaid and eSIM customers, must be identified before the service is switched on.
 - You must collect the customer's name and Polish national identification number (PESEL), or the details of an identity document, and confirm them before activating the line. A SIM bought anonymously stays inactive until that check is done.
 - Fully online activation is allowed, using one of six methods set out in the law: a selfie or video comparison against an identity document, the mObywatel government app, Trusted Profile (the free government e-signature), a bank login, a qualified or e-ID card signature, or an existing verified account with the same provider.
 - Before issuing a replacement SIM or a new eSIM profile on an existing number, you must check whether the customer has reserved their PESEL number in the national register and refuse if it is reserved.
 - Breaches can cost up to 3% of the previous year's revenue, and the regulator can suspend a provider's remote selfie or video checks if they are done carelessly.
-

The Polish market is open to new mobile operators and mobile virtual network operators (MVNOs). Entry is by a quick entry in a public register kept by the President of the Office of Electronic Communications (UKE), not by a licence, and EU providers can serve Polish customers on the same basis.

The principal authorities are UKE, which supervises the Electronic Communications Law, the President of the Personal Data Protection Office (UODO) for subscriber data, and the cybersecurity regime that since April 2026 treats most telecom providers as key or important entities.

The biggest practical obstacle for a digital entrant is identity: the service cannot start until the subscriber's data has been confirmed by one of the statutory routes, and SIM replacement carries a separate, mandatory register check.

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 telecom identity	Level	Official site
President of the Office of Electronic Communications (UKE)	Register of telecom undertakings, subscriber identification, number portability, anti-abuse rules, penalties	National	uke.gov.pl
President of the Personal Data Protection Office (UODO)	GDPR supervision; penalties for breaches of the telecom data-security duties	National	uodo.gov.pl
Minister of Digital Affairs	Implementing regulations under the Electronic Communications Law; national cybersecurity system	National	gov.pl/web/cyfryzacja
CSIRT NASK (national computer incident response team)	Smishing message patterns that operators must block; 8080 reporting number	National	Designated in the Act on Combating Abuse in Electronic Communications

Poland is a unitary state, so there is no regional layer. EU law applies directly, in particular the General Data Protection Regulation (GDPR), while EU directives such as the European Electronic Communications Code reach operators through the Polish acts that transpose them.

The governing statute is the Ustawa z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej [Act of 12 July 2024, Electronic Communications Law] (Dz.U. 2024 poz. 1221), in force since 10 November 2024, which replaced the 2004 Telecommunications Law.

In force

Telecommunications activity carried on as a business is a regulated activity requiring entry in the register of telecommunications undertakings kept by the President of UKE (art. 5). Providers from other EU or EEA states that temporarily serve Polish customers must also be entered. The application is filed electronically through UKE's e-services platform and signed with a qualified electronic signature, Trusted Profile or e-ID card signature (art. 17). UKE must make the entry within 3 working days; if it does not, the applicant may start operating (art. 8). An applicant that operated without an entry in the previous 3 years cannot be registered (art. 16(2)).

There is no capital requirement for an MVNO. Spectrum and numbering are separate: radio frequencies require a reservation or radio permit, and numbers are assigned by UKE decision, each with annual fees capped in the act (arts. 24 and 25). An annual telecommunications fee of at most 0.15% of telecom revenue applies only above a revenue threshold that UKE publishes each year (art. 23).

Over-the-top messaging and calling apps that do not use telephone numbers are electronic communications providers under the act, but they are expressly excluded from the subscriber identification duty in art. 296.

Telecom providers are not obliged institutions under the Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu [Act on Counteracting Money Laundering and Terrorist Financing] (consolidated text Dz.U. 2025 poz. 644). Its list of obliged institutions in art. 2(1) covers banks, payment and e-money institutions, insurers, virtual asset providers, gambling operators and others, but not electronic communications providers. A telecom group comes within the AML Act only for a separate regulated activity, for example if it holds a payment or e-money authorisation, or as a trader accepting cash payments for goods of EUR 10,000 or more (art. 2(1)(3) and (23)).

Identity in the sector is instead governed by the Electronic Communications Law. Its core is art. 296, a registration rule that applies to postpaid and prepaid customers alike.

Who must be identified

Every subscriber, except users of number-independent apps, payphone and dial-in voice users, and prepaid broadcast TV subscribers (art. 296(1)).

Data for individuals

Full name and PESEL number, or the name, series and number of an identity document. Foreigners from outside the EU and Switzerland give a passport or residence card number.

Data for businesses

Name, plus REGON, NIP, National Court Register number or another register entry; on request, details of representatives sufficient to verify them.

Activation gate

The provider may start the service only after confirming the data, either against the identity document or company register, or through an approved electronic route (art. 296(3)).

There is no risk-based customer due diligence, beneficial ownership check or suspicious activity reporting in this regime. Separate obligations to retain traffic and subscriber data and make them available to authorised bodies are covered in section 7.

4

Identity verification and onboarding

Art. 296(3) gives two ways to confirm a subscriber's data before service starts.

Document or register check

The provider confirms that the data given match an identity document (for individuals) or the relevant register (for businesses). This is the in-store route. The law lists the data to be recorded, not a copy of the document.

Electronic confirmation

The subscriber gives the data and confirms them electronically using one of the following:

- electronic identification means used to log in to a Polish bank, credit union or Polish payment institution;
- data verified with a qualified electronic signature certificate or an e-ID card personal signature;
- the provider's own login, if the subscriber's data were already verified under another contract;

- remote biometric comparison: the subscriber's live image, including over an audio-video link, is compared with the photo and data on the identity document shown during the session;
- Trusted Profile, which the provider may use only to confirm subscriber data (art. 296(5));
- a mObywatel app user certificate, where the user consents to that form of providing data.

Confirmation may be carried out by a third party acting for the provider (art. 296(4)), which allows outsourced identity verification, but the provider remains the party bound by the duty and the penalty.

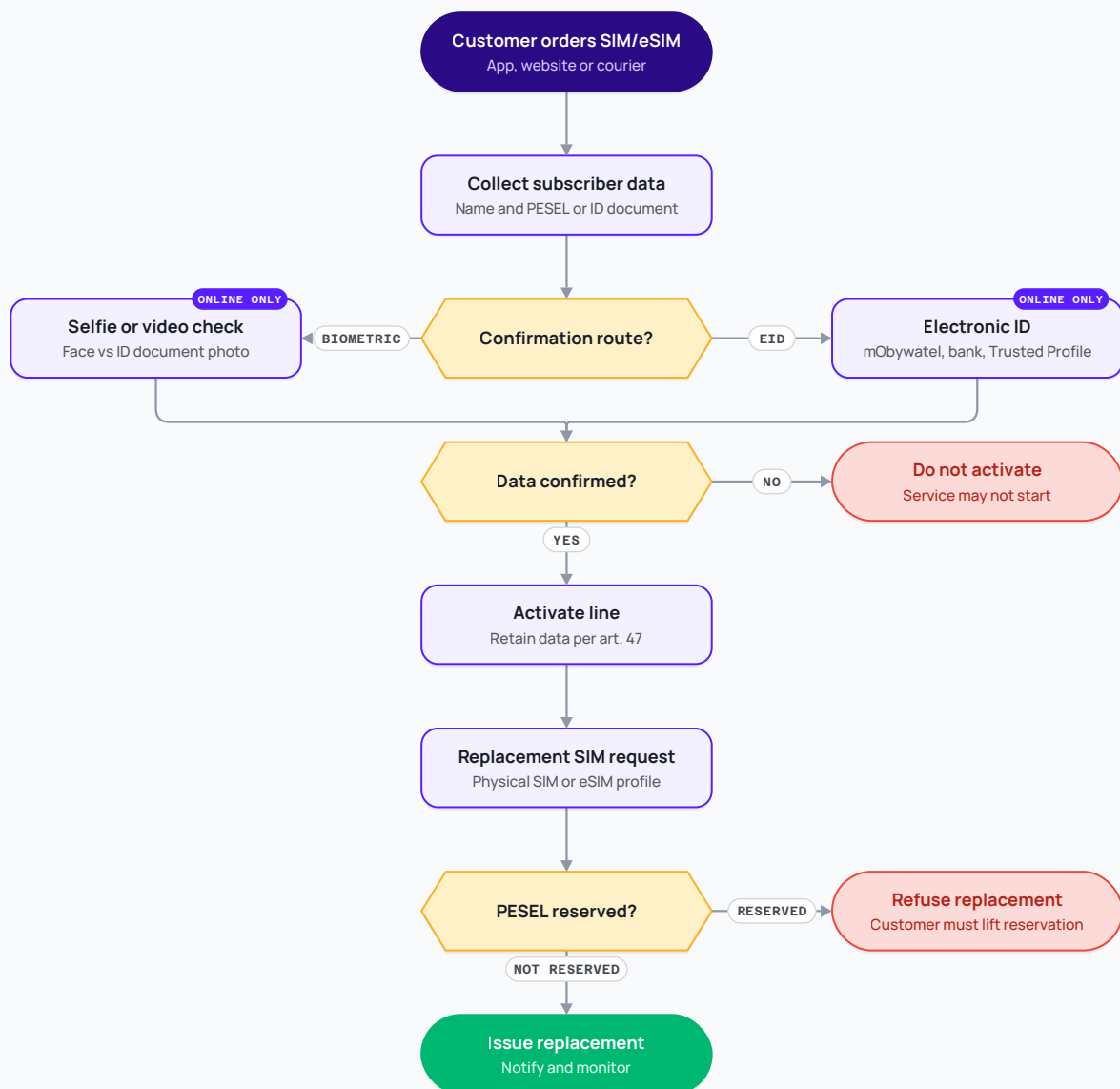


Figure 1. Online SIM or eSIM activation and SIM replacement under the Polish Electronic Communications Law.

The law does not specify a liveness standard, presentation-attack testing or an identity assurance level for the biometric route. Instead, UKE polices it after the fact: if UKE finds that a provider carries out remote image comparison contrary to the act or without due care, it suspends that method by an immediately enforceable decision and sets conditions for resuming it, and the provider must report the measures it has taken before restarting (art. 296(6) and (7)).

5 Digital channels: what's different

Bottom line: the data and the activation gate are the same in a shop and in an app; what changes online is the confirmation method, which must be one of the statutory electronic routes, and the remote biometric route can be suspended by UKE.

Requirement	In person / point of sale	Online / remote	Difference
Data collected	Name and PESEL or ID document details	Same data	Same
When service may start	Only after the data are confirmed	Only after the data are confirmed	Same
How data are confirmed	Against the identity document or company register	One of six electronic routes in art. 296(3)(2)	Differs
Biometric face comparison	Not required	Permitted against the ID document; UKE can suspend it	Differs
Use of a third party to verify	Permitted	Permitted	Same
Replacement SIM or eSIM profile	PESEL reservation check first	PESEL reservation check first	Same
Data retention	12 months, in Poland	12 months, in Poland	Same

Choosing the remote route

The electronic routes rely on identity that someone else has already verified: a bank, a qualified trust service provider, the State (mObywatel, Trusted Profile, e-ID card) or the provider itself. The selfie or video route is the only one in which the provider performs the verification itself, which is why it carries the specific suspension power in art. 296(6). For customers without a PESEL number, typically foreign nationals, the eID routes are usually unavailable, so document-based biometric comparison or in-person checks become the practical options.

eSIM and SIM replacement

Art. 297 expressly covers the "digital representation" of a SIM, so issuing an eSIM profile on an existing number triggers the same PESEL reservation check as a plastic duplicate. There is no separate, more lenient regime for eSIM.

Prepaid sold through retailers

For prepaid contracts, the subscriber may give the data to the provider electronically or in another way the provider specifies (art. 296(2)), so a starter pack can be sold anonymously and registered later in an app, provided the line is not activated until confirmation.

6 Data protection and biometrics

The GDPR (Regulation (EU) 2016/679) applies directly, supplemented by the Ustawa o ochronie danych osobowych [Act on the Protection of Personal Data] of 10 May 2018. For registration itself, the legal basis is the statutory duty in art. 296, which also sets the data that may be collected: the list does not include a copy or scan of the identity document.

The remote face comparison route processes biometric data. Where a facial image is processed by specific technical means to identify a person uniquely, it is special category data under art. 9 GDPR, so providers should document the condition relied on, run a data protection impact assessment and keep templates and images no longer than needed to evidence the check. The statute authorises the comparison but does not itself set a retention period for the images.

Separately, the Electronic Communications Law contains its own data security and breach-handling duties for providers, enforced by the President of UODO with penalties of up to 3% of the previous year's revenue (art. 445). The Act on Combating Abuse in Electronic Communications allows telecom operators to process personal data to identify and

prevent abuse and limits certain GDPR transparency and access rights to the extent necessary for that purpose (art. 26).

7 Sector-specific obligations

SIM swap protection through the PESEL reservation register

Before issuing a copy or duplicate of a SIM card or other subscriber identification device, or its digital representation, the provider must check in the register of PESEL reservations whether the number given by the subscriber is reserved (art. 297(1)). If it is reserved, or the register is unavailable for reasons announced under the Population Records Act, the provider must refuse. If the register is down for more than 15 minutes for other reasons, the provider may, after a second failed attempt, refuse until it is back or issue the replacement with due care and document the identity check; in that case no penalty applies (art. 297(3) and (4)).

Number portability

Mobile and fixed numbers move between providers free of charge within 1 working day of the agreed start date, with the process led by the new provider through UKE's system (art. 325). If a number is ported without the subscriber's consent, the new provider owes daily compensation of half the average monthly charge, or for prepaid half the top-ups of the last 3 months (art. 326(5)). Port-out is therefore an identity event as well as a consumer right.

Anti-abuse duties

The Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej [Act on Combating Abuse in Electronic Communications] (consolidated text Dz.U. 2024 poz. 1803) prohibits smishing, caller line identification (CLI) spoofing, artificial traffic generation and unlawful alteration of sender information (art. 3). Operators must block SMS messages matching patterns supplied by CSIRT NASK (art. 6), offer the free 8080 number for reporting suspicious messages (art. 5) and block or hide spoofed calls (art. 16).

Data retention and cybersecurity

Providers must retain traffic and location data in Poland for 12 months from the call or attempted call and provide them to authorised bodies, courts and prosecutors (art. 47), with prepaid services expressly covered. Under the amended Act on the National Cybersecurity System, in force since 3 April 2026, medium and large electronic

communications providers are key entities and micro and small ones are important entities, each subject to risk management and incident reporting duties.

8 Risk indicators and red flags

TELECOM IDENTITY-ABUSE INDICATORS DRAWN FROM POLISH LAW

- **Replacement SIM on a reserved PESEL:** a request to issue a duplicate or eSIM where the holder has reserved their number.
- **Duplicate during register outage:** replacement requests concentrated in periods when the PESEL reservation register is unavailable.
- **Port-out without consent:** a porting request the subscriber did not initiate, followed by loss of service.
- **Smishing:** SMS impersonating a bank, courier or public body to obtain data, payments or app installation.
- **CLI spoofing:** calls presenting another person's or institution's number, such as a bank's receive-only number.
- **Artificial traffic:** automated calls or messages generated only to be counted in interconnection or billing.
- **Face mismatch or document presented on screen:** weak signals in remote image comparison that UKE may treat as a lack of due care.

9 Enforcement and penalties

Breach	Authority	Maximum penalty
Providing service without confirming subscriber data (art. 444(1)(42))	UKE	Up to 3% of previous-year revenue
Failing to run the PESEL reservation check before a replacement SIM (art. 444(2)(13))	UKE	Up to 3% of previous-year revenue
Managers of a telecom undertaking (art. 444(4))	UKE	Up to 300% of the manager's monthly salary

Smishing, CLI spoofing or artificial traffic by an operator (art. 27 and 28 anti-abuse act)	UKE	Up to 3% of previous-year revenue
Telecom data security and breach duties (art. 445)	UODO	Up to 3% of previous-year revenue
Cybersecurity duties of key / important entities	Competent cybersecurity authority	Higher of EUR 10m or 2% of revenue / EUR 7m or 1.4%

UKE fines are calculated on revenue from the previous calendar year (art. 446(1)). Where that revenue was nil or did not exceed PLN 500,000, UKE uses the average of the three preceding years, and if that average is also at or below PLN 500,000 the fine is capped at PLN 15,000 (art. 446(2) and (3)). UKE takes into account the nature and scope of the breach, prior conduct and financial capacity, may fine even after the breach has ended, and may estimate the revenue base, at no less than PLN 500,000, if the provider does not supply its figures within 30 days (art. 446(7) and (8)). Decisions imposing fines are not given immediate enforceability. Beyond fines, UKE's suspension of a provider's remote biometric route under art. 296(6) is immediately enforceable and can halt online sales at once.

10 Recent changes and what to watch

- **6 November 2026** **Adopted, effective 6 Nov 2026** Dz.U. 2026 poz. 1296 adds the role of Digital Services Coordinator to UKE's tasks; no change to subscriber identification, but UKE's remit widens.
- **6 October 2026** **Bill, not enacted** Sejm print 3176, sent to first reading in committee, would require operators to tell the payment sector about released phone numbers where a payment identifier is linked to a number; watch it if your numbers are recycled.
- **3 April 2026** **In force** the NIS2 implementation (Dz.U. 2026 poz. 252) brings electronic communications providers into the national cybersecurity system as key or important entities.
- **10 November 2024** **In force** the Electronic Communications Law replaces the Telecommunications Law, keeping prepaid registration and adding the eSIM-inclusive PESEL check and the mObywatel route.
- **25 September 2023** **In force** the Act on Combating Abuse in Electronic Communications introduces mandatory smishing blocking and CLI spoofing controls.

What this means for identity verification

Design onboarding around the activation gate: capture name and PESEL or document details, confirm them, and only then provision the line or eSIM profile. A partially onboarded customer should have no working service.

Offer more than one statutory route. mObywatel, bank login and Trusted Profile cover most Polish residents with little friction; a document-plus-face comparison covers foreign nationals and customers without eID, but it is the route UKE can suspend, so keep evidence that each check was done with due care: the comparison result, the document data captured and the session record.

Do not ask for more than art. 296 lists. A scan of the identity document is not part of the statutory data set, and biometric images used for the comparison need a documented GDPR basis and a short retention period.

Treat SIM replacement and eSIM transfer as re-verification events: run the PESEL reservation check on every request, record its result and refuse when the number is reserved. Because porting without consent triggers daily compensation, authenticate the subscriber before accepting a port-out request as well.

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 onboarding with ID document capture and verification, face match and biometric liveness before the line is activated.
- Video KYC for agent-assisted remote identification of customers without Polish electronic ID.
- Re-verification of the subscriber with face match before a SIM replacement or eSIM transfer.
- No-code workflows that route customers to the right verification method and keep an audit trail of each check.
- Cloud, on-premises or hybrid deployment to fit data residency needs.

[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

- **Ustawa z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej** [Electronic Communications Law], Dz.U. 2024 poz. 1221, arts. 5–17, 23–25, 47, 296–297, 325–326, 444–446, Journal of Laws, dziennikustaw.gov.pl/DU/2024/1221
- **Ustawa z dnia 4 września 2026 r. o zmianie ustawy o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw** [Act amending the Act on Providing Services by Electronic Means and certain other acts], Dz.U. 2026 poz. 1296, art. 7, dziennikustaw.gov.pl/DU/2026/1296
- **Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej** [Act on Combating Abuse in Electronic Communications], consolidated text Dz.U. 2024 poz. 1803, arts. 3–9, 16, 26–28, dziennikustaw.gov.pl/DU/2024/1803

- **Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw** [Act amending the Act on the National Cybersecurity System], Dz.U. 2026 poz. 252, dziennikustaw.gov.pl/DU/2026/252
- **Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu** [Act on Counteracting Money Laundering and Terrorist Financing], consolidated text Dz.U. 2025 poz. 644, art. 2(1), dziennikustaw.gov.pl/DU/2025/644
- **Regulation (EU) 2016/679** (General Data Protection Regulation), arts. 4 and 9, EUR-Lex, eur-lex.europa.eu
- **Poselski projekt ustawy o zmianie ustawy – Prawo komunikacji elektronicznej** [Members' bill amending the Electronic Communications Law], Sejm print no. 3176, sejm.gov.pl