



Identomat

COMPLIANCE GUIDE

Insurance & Insurtech Compliance in Poland

COUNTRY **Poland**

INDUSTRY **Insurance & Insurtech**

LAST UPDATED **20 October 2026**

KEY REGULATORS **Polish Financial Supervision Authority (KNF) · General Inspector of Financial Information (GIIF) · President of the Personal Data Protection Office (UODO)**

Key takeaways

- Poland's anti-money laundering (AML) law applies to life insurers and to intermediaries selling life policies; non-life insurers are not covered by it, although EU sanctions still bind every firm.
- Carrying on insurance business in Poland needs an authorisation from the Polish Financial Supervision Authority (KNF), and agents and brokers must be entered in the register of insurance intermediaries that KNF keeps.
- A life insurer must identify and verify the policyholder before the policy starts, and must identify the beneficiary no later than the moment it pays out.
- Online onboarding is allowed, but the AML Act treats customers who are not physically present as higher risk unless the risk is reduced, for example by using an electronic ID or a qualified trust service; KNF expects a documented assessment before any remote method goes live.
- The EU AML Regulation applies from 10 July 2027, and a Polish bill sent to Parliament in September 2026 would move reporting to GIIF onto a new system from 2027 (proposed, not yet law).

The Polish market is open to digital insurers and insurtechs, including through online sales, but only through an authorised insurer or a registered intermediary. KNF supervises insurers and intermediaries, including their AML compliance, and the General Inspector of Financial Information (GIIF) is the financial intelligence unit that receives reports.

The biggest obstacle for a new entrant selling life or investment-linked cover online is building a remote customer due diligence process that satisfies KNF's detailed expectations on remote identification while keeping biometric processing on a lawful footing under data protection rules.

CONTENTS

- | | |
|--|--|
| 1 Who regulates this sector | 7 Sector-specific obligations |
| 2 Licensing and authorisation | 8 Risk indicators and red flags |
| 3 AML, KYC and customer due diligence | 9 Enforcement and penalties |
| 4 Identity verification and onboarding | 10 Recent changes and what to watch |
| 5 Digital channels: what's different | 11 What this means for identity verification |
| 6 Data protection and biometrics | ▪ Sources |

1

Who regulates this sector

Insurance in Poland is regulated nationally; there is no regional licensing. EU regulations on AML and data protection apply directly alongside Polish statutes.

Regulator	Remit	Level	Official site
Polish Financial Supervision Authority (Komisja Nadzoru Finansowego, KNF)	Authorises and supervises insurers; keeps the register of insurance intermediaries; supervises AML compliance of supervised firms and imposes AML penalties on them	National	knf.gov.pl
General Inspector of Financial Information (Generalny Inspektor Informacji Finansowej, GIIF)	Financial intelligence unit; receives threshold and suspicious transaction reports; controls AML compliance; keeps the national list for special restrictive measures	National (Ministry of Finance)	gov.pl/web/finanse
Minister of Finance	Insurance legislation; competent authority for the Central Register of Beneficial Owners; final AML penalty decisions are published on its website	National	gov.pl/web/finanse
President of the Personal Data Protection Office (UODO)	Data protection, including biometric data used in identity verification	National	uodo.gov.pl
European Union (Regulation (EU) 2024/1624)	Directly applicable AML rulebook from 10 July 2027	Supranational	eur-lex.europa.eu

2

Licensing and authorisation

Under the Act of 11 September 2015 on Insurance and Reinsurance Activity, carrying on insurance or reinsurance business requires an authorisation from KNF (Article 7(1)), which KNF grants by decision on the founders' application (Article 162). Insurance may be carried

on only by a joint-stock company, a mutual insurance society or a European company. The Act splits cover into Division I (life insurance) and Division II (other personal and property insurance), and one insurer cannot carry on both (Article 9(1)). At the end of 2025, 46 domestic insurers held authorisations, 20 of them in life insurance.

The authorisation covers the insurer and its classes of business; the Act sets no separate authorisation for online sales. An insurtech that does not become an insurer can distribute on behalf of one as an agent or broker. Under the Act of 15 December 2017 on Insurance Distribution, insurance agents, agents offering ancillary insurance and brokers must be entered in the register of insurance intermediaries, which KNF keeps online (Article 52). Each intermediary and each person carrying out agency activities receives a unique register number under the Regulation of the Minister of Finance of 21 August 2024.

3

AML, KYC and customer due diligence

Who is in scope

The Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing (the AML Act) lists as obliged institutions insurers carrying on Division I (life) business, including branches of foreign insurers (Article 2(1)(8)). Insurance intermediaries are obliged when they intermediate Division I products (Article 2(1)(9)), with one exception: a tied agent working for a single insurer within the same division who collects neither premiums from the customer nor amounts due to the customer. Non-life insurers do not appear on the list. For an insurance contract, the "customer" is the policyholder (Article 2(2)(10)).

Customer due diligence

Customer due diligence (CDD) covers identifying and verifying the customer, identifying the beneficial owner and taking reasonable steps to verify them, assessing the purpose of the relationship, and ongoing monitoring, including source-of-funds checks where justified (Article 34). It applies when a business relationship starts, for occasional transactions of EUR 15,000 or more, for occasional transfers of funds above EUR 1,000, on suspicion, and when earlier identification data are in doubt (Article 35). Verification must happen before the relationship begins, but may be completed during its establishment when this is needed for business continuity and the risk is low (Article 39).

Simplified measures may be used where the risk assessment confirms lower risk; a life contract with an annual premium of no more than EUR 1,500 or a single premium of no more than EUR 3,500 is listed as a lower-risk indicator, counted per insured person in group policies (Article 42). Enhanced measures are mandatory for politically exposed persons

(PEPs), high-risk third countries and unusual transactions, and are expected wherever risk is higher (Articles 43 to 46). For PEPs, enhanced treatment continues for at least 12 months after the person leaves office.

Beneficiaries and payouts

Life insurers must identify and verify the persons entitled under the policy as soon as they are determined and no later than the payout (Article 40(1)). When rights under a policy are transferred in whole or in part, beneficial ownership measures apply to the new holder (Article 40(2)). No later than the transfer or payout, the insurer must check whether beneficiaries or their beneficial owners are PEPs, and in higher-risk cases must analyse the relationship in more depth and inform senior management before paying (Article 46(3) and (4)).

Reporting and records

KNF's position of 19 March 2026 expects insurers' procedures to cover reports to GIIF of cash payments, withdrawals and transfers above EUR 15,000, due within 7 days under Article 72, suspicious activity notifications under Article 74 without delay and no later than 2 working days after the suspicion is confirmed, and notifications under Article 86 before a suspicious transaction is carried out. If CDD cannot be completed, the firm must not start or must end the relationship and must consider reporting (Article 41). CDD records and transaction evidence are kept for 5 years from the end of the relationship, extendable by up to 5 more years at GIIF's request (Article 49).

4 Identity verification and onboarding

For an individual, identification means recording full name, citizenship, PESEL number (or date and country of birth where there is none), the series and number of the identity document, and address where known (Article 36). Verification confirms those data against an identity document, an up-to-date register extract, or other documents, data or information from a reliable and independent source, including, where available, electronic identification means or trust services under the eIDAS Regulation (Article 37). Insurers may copy identity documents for CDD purposes and must tell the customer about the processing before the relationship starts (Article 34(4) and (5)). The beneficial owner of a corporate policyholder may not be verified solely from the Central Register of Beneficial Owners (Article 37(3)).

A life insurer may rely on another obliged institution's CDD, or one supervised to equivalent EU standards, but remains responsible and must be able to obtain the documents promptly

(Article 47). It may also entrust CDD to an agent acting in its name under a written agreement, again without shifting liability (Article 48). KNF expects the AML procedure to describe how an agency network is organised and controlled, and AML training to cover agents and other contractors who perform CDD.

KNF's position of 29 September 2023, which reflects the European Banking Authority's remote onboarding guidelines, sets out what a remote flow should contain; Figure 1 shows a typical one.

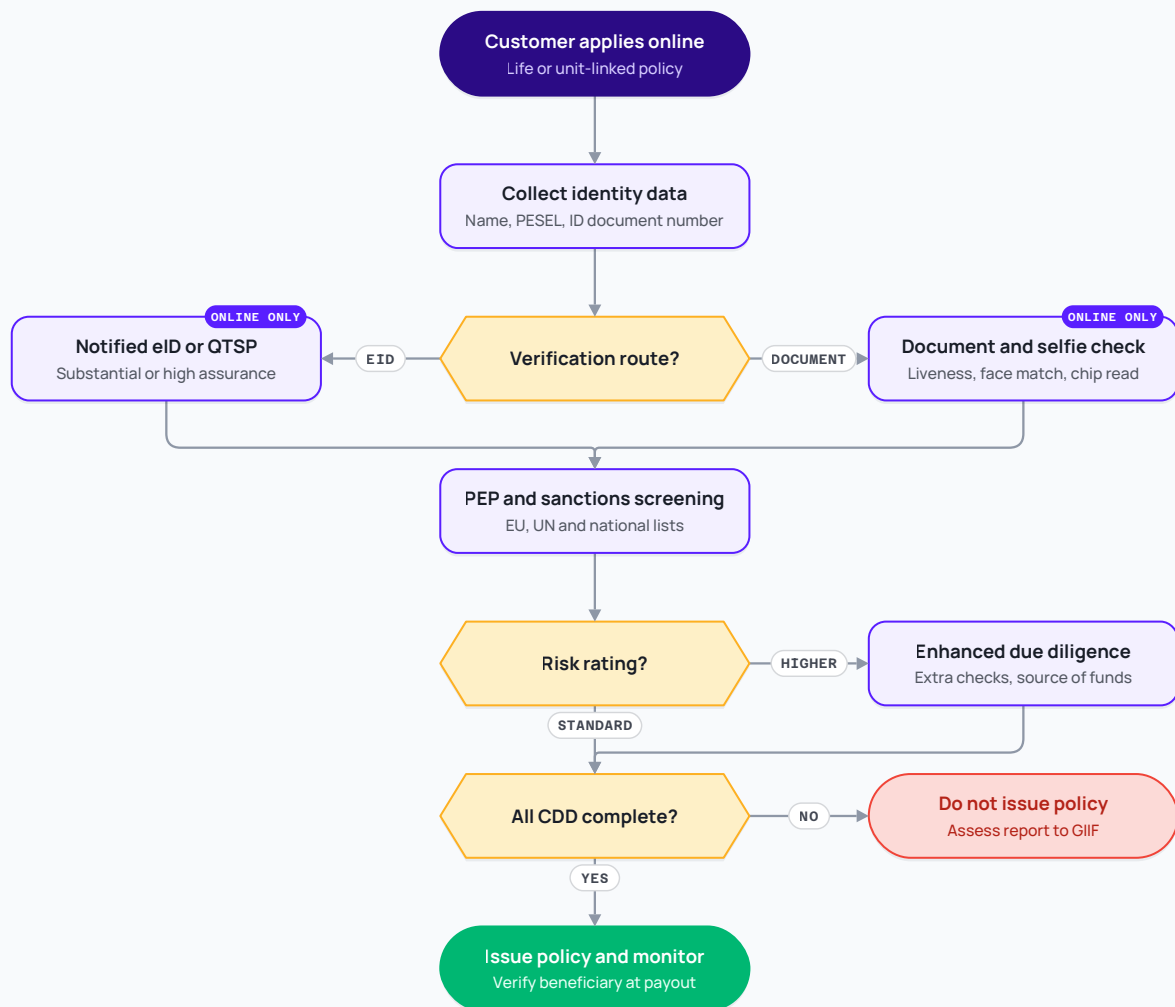


Figure 1. Remote onboarding for a life insurance policy in Poland.

5 Digital channels: what's different

Bottom line: the CDD obligations are the same online and face to face, but a remote customer counts as a higher-risk factor unless the insurer reduces that risk, and KNF expects a documented, tested remote process before launch.

Requirement	In person / agent-led	Online / remote	Difference
Remote onboarding permitted	Yes	Yes	Same
Risk treatment	Risk-based	Higher-risk factor unless mitigated (e.g. eID, trust service)	Differs
Verification methods	ID document seen in person	eID, qualified trust service, video or document plus biometric check	Differs
Assessment before launch	General business risk assessment	Documented analysis of the remote solution, approved by management	Differs
When CDD is completed	Before the relationship starts	Before the relationship; first transaction only after all CDD	Same
Beneficiary identification	No later than payout	No later than payout	Same
Location and device controls	Not applicable	Controls against IP spoofing and VPN masking	Differs
Evidence retained	Document copies, 5 years	Legible, time-stamped images, recordings and data, 5 years	Differs
Biometric data	Not usually processed	Explicit consent and a non-biometric alternative	Differs

Remote customers are a higher-risk factor

Article 43(2)(7) of the AML Act lists establishing or maintaining a relationship without the customer's physical presence as a higher-risk indicator where that risk has not been reduced in another way, including by electronic identification or trust services under eIDAS. KNF adds that, where eID or trust services cannot be used, the insurer should consider enhanced measures, and that offering products through new channels or technology is a separate risk indicator (Article 43(2)(9)).

What KNF expects from a remote flow

Notified eID schemes at substantial or high assurance, or qualified trust services, satisfy several of KNF's requirements on their own. For other solutions KNF expects the insurer to check document security features against official reference sources, validate the machine-readable zone, consider reading the identity card chip where the device allows, use strong face-matching algorithms and, in unassisted flows, a liveness check. Photos and video must be captured during the session, and the process must stop on technical faults. In video calls, staff need AML training and a scripted interview, ideally with randomised actions. A first payment from the customer's own account at a regulated institution may support verification but must not be the main or only method. Where doubts remain, the customer should be redirected to in-person verification.

Outsourcing to identity providers

Using a verification vendor does not move responsibility. KNF expects a written contract, monitoring by the AML reporting officer, minimal and access-logged storage of images, and no providers established in high-risk third countries.

Pending changes: the EU AML Regulation **Adopted, applies 10 Jul 2027** recognises that eIDAS electronic identification, with suitable risk mitigation, can bring remote onboarding risk down to standard or even low.

6 Data protection and biometrics

The GDPR applies directly, supervised by UODO. The AML Act itself authorises insurers to process the information in identity documents and to copy them for CDD, provided the customer is informed first (Article 34(4) and (5)). It does not mention biometric data.

In a position published on 30 April 2024 on biometric identity verification by financial institutions, UODO stated that biometric data are special-category data under Article 9 GDPR, that current Polish financial sector legislation does not provide a legal basis for

processing them, and that the only available basis is the customer's explicit and informed consent. UODO added that biometrics should not be the primary or only verification method, that a customer who refuses consent must be offered an alternative route, and that a data protection impact assessment should precede deployment.

Retention follows the AML Act's 5-year rule for CDD evidence; KNF expects remote onboarding data to be limited to what is necessary and access to be logged and restricted.

7 Sector-specific obligations

Intermediaries and embedded distribution

A bank, retailer or app that sells life cover as an agent is itself an obliged institution unless it falls within the tied-agent exception in Article 2(1)(9): one insurer, one division, and no handling of premiums or payouts. The EU AML Regulation follows a similar logic, explaining that intermediaries that do not handle funds should not be obliged entities because the insurer carries out the AML work.

Sanctions screening

The AML Act requires obliged institutions to apply special restrictive measures (freezing and not making assets available) to persons on UN Security Council lists and on the list kept by GIIF (Article 117). KNF also expects firms to screen against EU sanctions lists and the national list under the Act of 13 April 2022 on special solutions for counteracting support for aggression against Ukraine, to carry out a sanctions risk assessment, and to set rules for freezing and reporting. Non-life insurers outside the AML Act remain bound by directly applicable EU asset freezes, which the EU AML Regulation confirms bind all natural and legal persons in the Union.

Periodic review

KNF accepts market practice of reviewing high-risk customers every year, normal-risk customers every 3 years and low-risk customers every 5 years, and asks firms to bear in mind that Article 26 of the EU AML Regulation caps the interval at 1 year for higher-risk customers and 5 years for all others. Identity document expiry dates should be monitored.

Risk indicators and red flags

The AML Act's higher-risk factors and unusual-transaction criteria (Article 43(2) and (4)) translate into these life insurance warning signs.

LIFE INSURANCE WARNING SIGNS

- **Unrelated payer:** premiums paid by third parties unknown to or unconnected with the policyholder.
- **Large single premium:** high amounts not explained by the customer's profile or circumstances.
- **Policy assignment:** full or partial transfer of rights to a new holder, triggering beneficial ownership checks.
- **PEP beneficiary:** payout or assignment to a PEP, family member or close associate.
- **High-risk geography:** links to an EU-listed high-risk third country or a sanctioned state.
- **Opaque structure:** corporate policyholder with unusual or overly complex ownership.
- **Remote anomalies:** masked location, VPN use or doubtful document images during onboarding.

Enforcement and penalties

KNF controls AML compliance of the institutions it supervises (Article 130(2)) and imposes the full catalogue of administrative penalties on them (Article 151): publication of the breach, an order to cease specified activities, withdrawal of authorisation or deletion from a register, a ban of up to one year on the responsible manager, and a fine (Article 150). For life insurers and insurance intermediaries, the fine may reach twice the benefit gained or loss avoided or, where that cannot be established, EUR 1 million; for legal persons the ceiling is EUR 5 million or 10% of turnover in the last approved financial statements, and for individuals PLN 20,868,500. Gravity, duration, cooperation and previous breaches are weighed (Article 150(4)). Final decisions are published on the Ministry of Finance website under Article 152, naming the institution, the breach, the penalty and any court challenge. Failing to adopt an AML procedure is itself sanctionable (Article 147).

In a decision published on 7 November 2025, KNF fined Sopockie Towarzystwo Ubezpieczeń na Życie ERGO Hestia S.A., a life insurer, PLN 300,000 for failing to ensure that staff performing AML duties took part in training programmes (Article 52(1)). The insurer appealed; the Voivodeship Administrative Court dismissed the complaint, and the judgment is not yet final.

10 Recent changes and what to watch

- **28 September 2026:** Government bill amending the AML Act (Sejm print 3163) **Bill, not enacted**. It would require every obliged institution to register for a new GIIF reporting system (SIGIIF), with a 15 to 31 January 2027 window for life insurers and intermediaries already registered with GIIF, shorten the suspicious activity deadline from 2 working days to 2 days, and limit beneficial ownership register access to those with a legitimate interest.
- **19 March 2026:** KNF position on processes that AML procedures must cover **In force**. Insurers should map their procedures against it; KNF may check implementation in inspections.
- **7 November 2025:** Publication of KNF's PLN 300,000 AML penalty on a life insurer for training failures **In force**. Training must cover everyone performing AML tasks, including agents.
- **30 April 2024:** UODO position on biometric identity verification **In force**. Biometric steps need explicit consent and an alternative route.
- **10 July 2027:** EU AML Regulation applies **Adopted, applies 10 Jul 2027**. Polish AML Act provisions will need to be read alongside a directly applicable EU rulebook, including for life insurers and intermediaries.

11 What this means for identity verification

A life or investment-linked product sold online needs, at onboarding, the Article 36 data set (including PESEL or date and country of birth and the identity document number) verified against a reliable source before the policy starts. Notified eID at substantial or high assurance or a qualified trust service is the route KNF treats most favourably; document capture with face match and liveness is acceptable when backed by the controls KNF describes, a pre-launch risk assessment and explicit biometric consent with a non-biometric fallback.

Identity work does not end at issuance. Beneficiaries must be identified and verified by the time of payout, assignments trigger beneficial ownership checks, PEP status must be checked at payout, and customer files need periodic refresh by risk level. Evidence, including session recordings, is kept for 5 years. Non-life products still need sanctions screening.

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 policyholder verification with ID document capture and checks (including NFC chip reading), face match and biometric liveness.
- AML screening of policyholders, beneficial owners and beneficiaries against sanctions and PEP lists, at onboarding, at payout and on an ongoing basis.
- KYB and beneficial owner verification for corporate policyholders.
- Video KYC with recorded sessions and an audit trail of every check for 5-year retention.
- A no-code workflow builder to route customers between eID, document and video checks and to request explicit biometric consent.

[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 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu [Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing], Dz.U. 2018 poz.

723, consolidated text Dz.U. 2025 poz. 644 as amended (unified text dated 8 October 2026), Articles 2, 34 to 49, 72, 74, 117, 130, 147, 150 to 152, isap.sejm.gov.pl

- **Government bill amending the AML Act**, Sejm print no. 3163, 28 September 2026, sejm.gov.pl
- **Ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej** [Act on Insurance and Reinsurance Activity], consolidated text Dz.U. 2025 poz. 1526 as amended, Articles 7, 9 and 162, isap.sejm.gov.pl
- **Ustawa z dnia 15 grudnia 2017 r. o dystrybucji ubezpieczeń** [Act on Insurance Distribution], Dz.U. 2017 poz. 2486, consolidated text Dz.U. 2026 poz. 12 as amended, Article 52, isap.sejm.gov.pl
- **Rozporządzenie Ministra Finansów z dnia 21 sierpnia 2024 r. w sprawie prowadzenia rejestru pośredników ubezpieczeniowych** [Regulation on keeping the register of insurance intermediaries], Dz.U. 2024 poz. 1293, isap.sejm.gov.pl
- **Działalność ubezpieczeniowa i reasekuracyjna** [Insurance and reinsurance activity], Ministry of Finance, gov.pl/web/finanse
- **Stanowisko UKNF dotyczące prawidłowego wykorzystania rozwiązań w zakresie nawiązywania stosunków gospodarczych bez fizycznej obecności klienta** [KNF position on remote onboarding], 29 September 2023, knf.gov.pl
- **Stanowisko UKNF dotyczące procesów realizowanych przez instytucje obowiązane w zakresie AML/CFT** [KNF position on AML/CFT procedures], 19 March 2026, knf.gov.pl
- **Stanowiska UKNF: rynek ubezpieczeń** [KNF positions for the insurance market], updated 24 July 2026, knf.gov.pl
- **Kara administracyjna nałożona przez KNF na Sopotckie Towarzystwo Ubezpieczeń na Życie ERGO Hestia S.A.** [AML penalty publication], Ministry of Finance, first published 7 November 2025, gov.pl/web/finanse
- **Biometryczna weryfikacja tożsamości klientów usług płatniczych** [Biometric identity verification of financial customers], UODO, 30 April 2024, uodo.gov.pl
- **Regulation (EU) 2024/1624** on the prevention of the use of the financial system for money laundering or terrorist financing, recitals 9, 33, 34 and 66, Article 26, eur-lex.europa.eu