



Identomat

COMPLIANCE GUIDE

Banking & Digital Banking Compliance in Poland

COUNTRY **Poland**

INDUSTRY **Banking & Digital Banking**

LAST UPDATED **20 October 2026**

KEY REGULATORS **Polish Financial Supervision Authority (KNF) · General Inspector of Financial Information (GIIF) · Bank Guarantee Fund (BFG)**

Key takeaways

- Taking deposits in Poland needs a permit from the Polish Financial Supervision Authority (KNF), or an EU bank's branch passport; doing it without one is a crime punishable by a fine of up to PLN 20 million and up to five years in prison.
 - Banks must identify and verify every customer, including the people who ultimately own or control business customers, before the account is used. A bank may sign the account agreement first, but no transactions can run until those checks are complete.
 - Fully online account opening is allowed. A customer who is not physically present counts as higher risk unless the bank uses an EU-recognised electronic ID or a trust service such as a qualified electronic signature; otherwise extra safeguards (for example liveness checks or a first transfer from the customer's own account at another bank) are expected.
 - Banks must report cash payments and transfers above EUR 15,000 to the financial intelligence unit (GIIF) within 7 days, and report suspicions within 2 working days.
 - A government bill sent to Parliament in September 2026 would move all reporting to a new GIIF system from 2027; it is not yet law. The EU Anti-Money Laundering Regulation will replace most national customer due diligence rules from 10 July 2027.
-

Poland is open to digital banking. Digital-only banks operate on the same licence as branch banks, and EU-authorised banks can enter through a passported branch or cross-border services. The rulebook is national law built on EU directives, supplemented by detailed supervisory positions from the KNF on remote onboarding.

The KNF licenses and supervises banks, including for anti-money laundering compliance. The General Inspector of Financial Information (GIIF), part of the Ministry of Finance, receives reports and also inspects. The Bank Guarantee Fund (BFG) runs deposit insurance.

The biggest obstacle for a new entrant is the licence itself: at least EUR 5 million in founders' capital, a three-year business plan, fit and proper management and, for a remote-first model, an onboarding process that meets the KNF's documented expectations for video, biometric and electronic-ID verification.

CONTENTS

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

1 Who regulates this sector

Authority	Remit	Level	Official site
Polish Financial Supervision Authority (KNF)	Bank licensing and prudential supervision; AML inspections and penalties for supervised banks	National	knf.gov.pl
General Inspector of Financial Information (GIIF), Ministry of Finance	Financial intelligence unit: threshold and suspicious activity reports, transaction holds, AML inspections, sanctions lists	National	gov.pl/web/finanse
Bank Guarantee Fund (BFG)	Deposit guarantee scheme and bank resolution	National	bfg.pl
Central Register of Beneficial Owners (CRBR)	Register that banks must consult when onboarding companies and other entities	National	crbr.podatki.gov.pl
President of the Personal Data Protection Office (UODO)	Data protection, including biometric data used in onboarding	National	uodo.gov.pl

2 Licensing and authorisation

Under the Banking Law (Prawo bankowe, Act of 29 August 1997, consolidated text Dz.U. 2026 poz. 38), a domestic bank needs two KNF decisions: a permit to establish the bank

(Art. 30 and 34) and a permit to start operating (Art. 36). App-only banks use the same permits.

Capital

Founders' capital of at least the złoty equivalent of EUR 5 million, or EUR 1 million for a cooperative bank joining an association, paid in cash in złoty before registration (Art. 32).

People and plan

Fit and proper founders and board members and a business plan covering at least three years (Art. 30(1)); certain board members must know Polish unless the KNF waives it.

EU passport

A branch of a credit institution authorised in another EU state may start business two months after the KNF receives the home supervisor's notification (Art. 48l).

Non-EU banks

A new KNF authorisation regime for branches of non-EU banks, with class 1 and class 2 branches, applies from 11 January 2027 **Adopted, effective 11 Jan 2027** (Act of 31 July 2026, Dz.U. 2026 poz. 1206).

Taking deposits without a permit, or using the words "bank" or "kasa" in a business name in breach of the Act, is a criminal offence punishable by a fine of up to PLN 20,000,000 and imprisonment of up to five years (Art. 171). Deposits at Polish banks are guaranteed by the BFG up to the złoty equivalent of EUR 100,000 per depositor per bank (Act of 10 June 2016 on the BFG, Art. 24, consolidated text Dz.U. 2026 poz. 620).

3

AML, KYC and customer due diligence

Domestic banks, branches of EU credit institutions and branches of foreign banks are obliged institutions under Art. 2(1)(1) of the Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing (the AML Act, consolidated text Dz.U. 2025 poz. 644). Every bank must document a business-wide risk assessment and apply customer due diligence (CDD) in proportion to the risk it identifies (Art. 27 and 33).

When CDD applies

CDD is required when a business relationship is established; for an occasional transaction of EUR 15,000 or more (single or linked); for a transfer of funds above EUR 1,000; whenever money laundering or terrorist financing is suspected; and whenever the bank doubts previously obtained identification data (Art. 35(1)). It must be reapplied when a customer's circumstances or beneficial owners change (Art. 35(2)).

What CDD consists of

CDD covers verifying the customer and any representative; identifying beneficial owners and the ownership structure; understanding the purpose of the relationship; and ongoing monitoring, including source of funds where justified (Art. 34). If CDD cannot be completed, the bank must not open the relationship, must not execute transactions through the account and must terminate an existing relationship, then consider whether to report (Art. 41).

Enhanced due diligence

Enhanced measures apply in higher-risk cases, including private banking, products that favour anonymity, links to high-risk third countries and onboarding without the customer being physically present unless that risk is mitigated through electronic identification or trust services under the eIDAS Regulation (Art. 43(2)). Politically exposed persons (Art. 46) and cross-border correspondent relationships with respondents from outside the EU (Art. 45) always require enhanced measures.

Beneficial ownership

When onboarding an entity required to register beneficial owners, the bank must obtain confirmation of registration or an extract from the CRBR or the equivalent register of another EU state (Art. 39(1a)), but must not rely solely on the register (Art. 37(3)).

Reporting and retention

Obligation	Trigger	Deadline	Provision
Threshold report to GIIF	Cash deposit or withdrawal, or transfer, above EUR 15,000; purchase or sale of foreign currency above EUR 15,000	7 days	Art. 72
Suspicious activity report	Circumstances that may indicate money laundering or terrorist financing	Promptly, no later than 2 working days after the suspicion is confirmed	Art. 74
Transaction hold notice	Reasonable suspicion about a specific pending transaction or assets	Immediately; transaction held up to 24 hours; GIIF may order a hold or account block of up to 96 hours	Art. 86

Record retention	CDD copies and information, including data obtained through electronic identification, and transaction records	5 years from the end of the relationship; GILF may require up to 5 more years	Art. 49
------------------	--	---	---------

Banks must freeze assets of persons on GILF's terrorism-related lists (Art. 117 and 118); EU sanctions apply directly.

4 Identity verification and onboarding

For an individual, the bank must record the full name, citizenship, PESEL national identification number (or date and country of birth where no PESEL exists), the series and number of the identity document, the residential address where known, and business name, tax number (NIP) and address for sole traders (AML Act, Art. 36(1)). Verification means confirming those data against an identity document, an up-to-date register extract, or other reliable and independent documents, data or information, including electronic identification means and trust services under the eIDAS Regulation where available (Art. 37(1)). Verification precedes the relationship, but may finish during onboarding where risk is low (Art. 39).

The KNF has set out how it expects this to work remotely in two positions. Its **video verification position** of 5 June 2019 treats eIDAS electronic identification and qualified electronic signatures as the most reliable remote tools. Where a bank uses video calls instead, it expects:

- at least partial involvement of a bank employee;
- the identity card shown to the camera from several angles;
- checks against the registers of lost and stolen documents, the PESEL register and sanctions lists;
- a one-time SMS code read back during the call;
- archiving of the full recording;
- as an additional measure, a first transfer from the customer's account at another obliged institution, used only as supporting evidence.

The KNF's **remote onboarding position** of 29 September 2023 applies to all supervised institutions and incorporates the European Banking Authority's remote onboarding guidelines (EBA/GL/2022/15). For unassisted flows it expects:

- photos and video captured during the live session;

- a liveness check, either active (the customer performs an action) or passive;
- strong and reliable algorithms matching the face to the document photo;
- use of identity card chip data where the device and access allow it;
- checks of document security features;
- controls against spoofed IP addresses and VPNs.

An eIDAS-notified electronic ID at substantial or high assurance, or qualified trust services, is treated as meeting these expectations. Where data quality is insufficient, the bank should restart or move the customer to in-person verification.

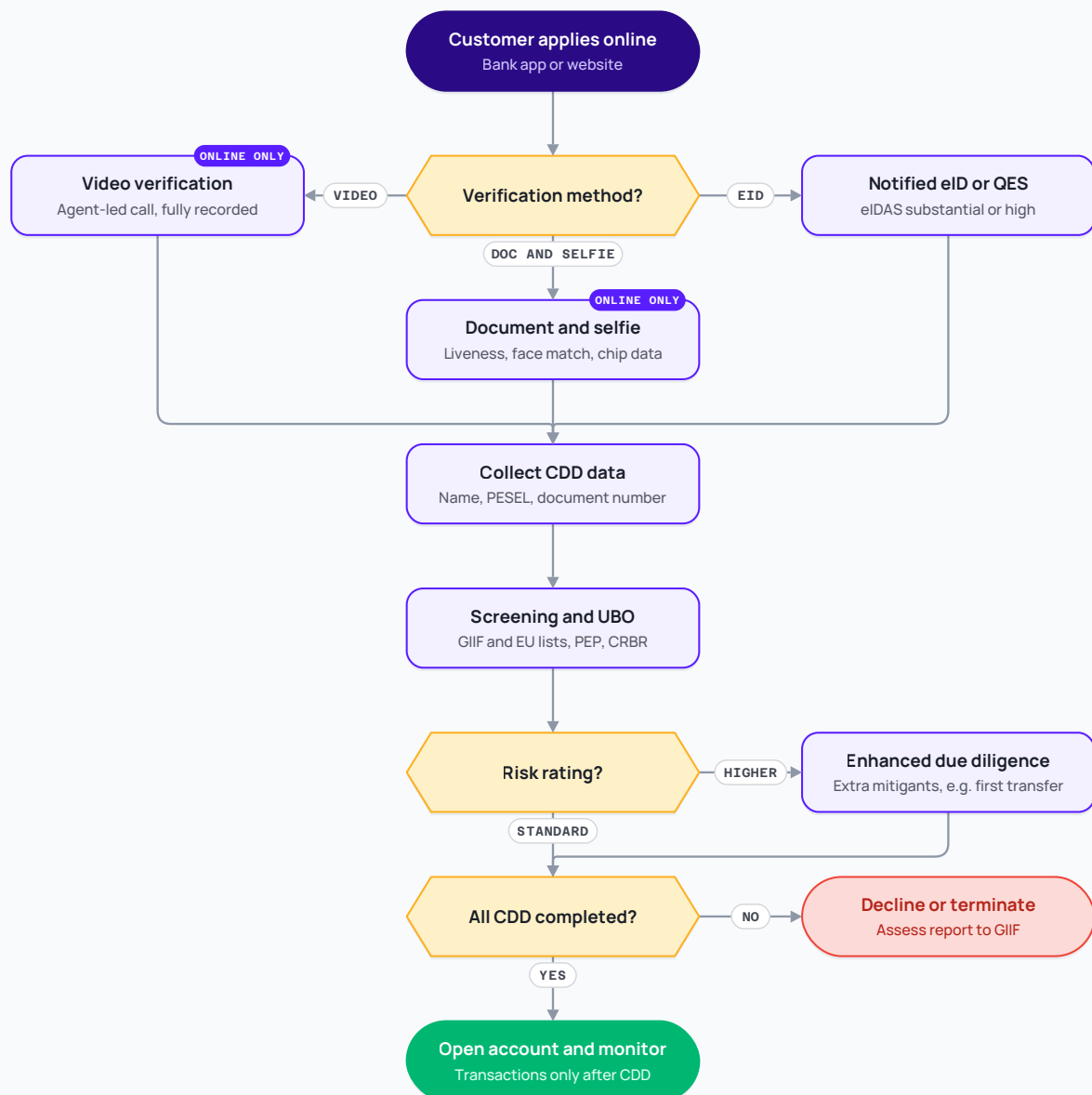


Figure 1. Remote account opening for an individual customer at a Polish bank.

A bank may rely on CDD performed by another obliged institution or an equivalent supervised entity elsewhere, provided it can obtain the documents on request, but it remains responsible (Art. 47). It may also outsource CDD under a written agreement to an agent treated as part of the bank, again without shifting liability (Art. 48). Under the Banking Law, a bank's liability to customers for an outsourced provider's failures cannot be excluded or limited (Art. 6b(2)).

5 Digital channels: what's different

Bottom line: the legal CDD duties are the same online and in a branch, but remote onboarding is a statutory higher-risk factor unless the bank uses EU-recognised electronic ID or trust services, and the KNF expects specific liveness, recording and anti-spoofing controls when it does not.

Requirement	In person / branch	Online / remote	Difference
Data to collect	Art. 36 identification data	Art. 36 identification data	Same
Verification source	Identity document checked by staff	eIDAS eID or trust service, video verification, or document and selfie with liveness	Differs
Risk treatment	Risk-based; no channel factor	Higher-risk factor unless mitigated by eID or trust services	Differs
When verification is completed	Before the relationship; no transactions until CDD is done	Same rule, with controls so the first transaction follows full CDD	Same
Evidence kept	Copies of documents and CDD information	Also images, audio and video, time-stamped and readable for later review	Differs
Device and location checks	Not applicable	Controls against spoofed IP addresses and VPNs	Differs

Account access	Branch identification	Strong customer authentication for online access and remote payments	Differs
Reliance and outsourcing	Bank remains liable	Bank remains liable, including for onboarding vendors	Same
Retention period	5 years after the relationship ends	5 years, including data from electronic identification	Same

Electronic ID lowers the risk classification

Art. 43(2)(7) of the AML Act lists non-face-to-face onboarding as a higher-risk indicator only where the risk is not otherwise mitigated, naming eIDAS electronic identification and trust services as the mitigants. Both KNF positions say that where these are not used, the bank should consider enhanced measures and treat the remote channel as a distribution-channel risk factor in its business-wide assessment.

Assisted video sessions

For staff-assisted video, the 2023 KNF position expects trained staff following a call script, a random sequence of customer actions and random assignment of the employee to prevent collusion; the 2019 position adds checks for coercion, intoxication or a third person in the room.

Strong customer authentication after onboarding

Once the account is open, the Payment Services Act (Dz.U. 2026 poz. 623, Art. 32i) requires strong customer authentication when the customer accesses the account online, initiates an electronic payment, or performs any remote action that may carry a fraud risk. Remote payments must use authentication dynamically linked to the amount and payee.

What is changing

The EU Anti-Money Laundering Regulation (EU) 2024/1624

Adopted, applies from 10 Jul 2027 states in its recitals that eIDAS electronic identification should be accepted and can lower risk to standard or low.

The GDPR applies directly, supplemented by the Polish Act of 10 May 2018 on the Protection of Personal Data. For onboarding, the AML Act provides the legal basis for processing information from identity documents and making copies of them (Art. 34(4)), and requires the bank to inform the customer about this processing before the relationship begins (Art. 34(5)).

Biometric data is treated differently. In a statement published on 30 April 2024, the President of UODO took the view that existing sector law does not provide a legal basis for financial institutions to process biometric data, so explicit consent under Art. 9(2)(a) GDPR is the only available basis. UODO also said that:

- biometric verification should not be the primary or only method of verifying identity;
- an alternative method must be offered to customers who refuse consent;
- the purpose must be stated at the point of consent;
- a data protection impact assessment should precede deployment.

UODO reached this view on behavioural biometrics but stated it for biometric verification by financial institutions generally, so a face-match flow needs explicit consent plus a non-biometric route.

The KNF expects vendors storing onboarding images and videos to keep only necessary data, for no longer than the AML retention period, with logged access.

Banking secrecy

Everything a bank learns about a banking transaction during negotiation, conclusion and performance of the contract is covered by banking secrecy (Banking Law, Art. 104). Unauthorised disclosure is punishable by a fine of up to PLN 1,000,000 and imprisonment (Art. 171(5)).

Outsourcing and third parties

Banks may entrust intermediaries with activities such as concluding account agreements under a written contract (Art. 6a). They must notify the KNF before outsourcing to providers outside the EU (Art. 6d). For onboarding vendors, the KNF also expects a

documented risk assessment, a clear contractual split of duties and monitoring by the AML compliance officer.

Internal AML procedures

The KNF's position of 19 March 2026 sets out what internal AML procedures must cover and requires senior management approval of each version; procedure deficiencies made up 19.39% of AML irregularities the KNF found in 2024.

8

Risk indicators and red flags

BANKING AND REMOTE ONBOARDING RED FLAGS (AML ACT, KNF, GIIF)

- **Straw-person accounts:** account opened remotely for someone unaware of its purpose, or under a third party's direction (KNF 2019).
- **Coached applicant:** another person present or prompting during video verification, or the session paused so the customer leaves the camera.
- **Location masking:** device location hidden behind a VPN or spoofed IP address during onboarding (KNF 2023).
- **Unexplained third-party funding:** transactions for the customer's benefit ordered by unknown or unconnected third parties (AML Act, Art. 43(2)(8)).
- **Shell company chains:** companies with nominee owners from other countries, accounts abroad, and generic consulting or marketing payment descriptions (GIIF 2025 report).
- **Fictitious loans and invoices:** repeated transfers between related companies labelled as loans or invoice payments with no economic rationale (GIIF 2025 report).
- **Fraud proceeds:** fraud, including investment fraud, phishing and impersonation, was the most common predicate offence in foreign requests to GIIF in 2025 (GIIF 2025 report).

9

Enforcement and penalties

The KNF imposes AML penalties on the banks it supervises; GIIF inspects and can also impose penalties (AML Act, Art. 151). Available sanctions include publication of the breach,

an order to cease specific activities, withdrawal of the licence, a ban of up to one year on the responsible manager, and fines (Art. 150(1)).

Basis	Maximum fine
General rule	Up to twice the benefit gained or loss avoided, or up to EUR 1,000,000 where that cannot be established (Art. 150(2))
Banks and other financial institutions (legal persons)	Up to EUR 5,000,000 or 10% of turnover in the last approved annual (or consolidated) financial statements (Art. 150(3))
Natural persons in those institutions	Up to PLN 20,868,500 (Art. 150(3))

Fines reflect the gravity and duration of the breach, financial capacity, gains, third-party losses, cooperation and previous breaches (Art. 150(4)); GIIF publishes final decisions.

In a decision published on 13 June 2025, the KNF fined Credit Agricole Bank Polska S.A. PLN 1,000,000 in total for:

- an inadequate business-wide risk assessment;
- failing to establish the ownership and control structure of corporate customers;
- failing to monitor transactions against the customer's profile;
- failing to keep CDD information up to date.

In a decision published in October 2025, the KNF fined mBank S.A. (brokerage unit) PLN 1,390,000 for, among other breaches, not recording customers' PESEL numbers and countries of birth, failing to identify beneficial owners, and not documenting CDD.

10 Recent changes and what to watch

- **10 July 2027:** EU Anti-Money Laundering Regulation (EU) 2024/1624 **Adopted, applies from 10 Jul 2027**. It replaces most of the national CDD rulebook with directly applicable EU rules; onboarding flows built on the AML Act will need to be mapped to it.
- **29 September 2026:** Act of 31 July 2026 amending the Banking Law (Dz.U. 2026 poz. 1206), implementing the EU's Capital Requirements Directive VI **Partly in force**. It raises fines for unauthorised acquisitions of bank shares (now up to 10% of annual net turnover for companies) and introduces the non-EU branch regime from 11 January 2027.

- **28 September 2026:** government bill amending the AML Act (Sejm print no. 3163)

Bill, not enacted . It would:

- require banks to register on GLIF's new reporting system by 14 January 2027, with reports moving to it from April 2027;
- require new products and channels to be risk-assessed before launch;
- require banks to document their attempts to apply CDD and any failure to complete it;
- limit public access to the beneficial ownership register to people with a legitimate interest.

Its proposed main start date is 1 January 2027.

- **19 March 2026:** KNF position on internal AML procedures **In force** . Banks should review their procedures against it now; the KNF says it may check implementation in inspections.
- **29 November 2025:** Act of 25 July 2025 amending the Banking Law (Dz.U. 2025 poz. 1191) **In force** . Banks must check the PESEL register to confirm whether the holder is alive 5 years after the last instruction on an account.

11

What this means for identity verification

- **Documents and data:** capture the full Art. 36 data set, including PESEL (or date and country of birth) and the document series and number; missing PESEL data has already led to a KNF fine.
- **Remote methods:** offer eIDAS-notified electronic ID or qualified trust services where available, because these remove the statutory higher-risk factor.
- **Document-and-selfie flows:** build in liveness, strong face-matching, chip reading where possible and anti-spoofing controls.
- **Biometrics:** treat biometric verification as consent-based and optional, with a non-biometric route such as staff-assisted video or electronic ID.
- **Evidence:** keep images, video and audio, time-stamped and readable for later review, for 5 years after the relationship ends.
- **Re-verification:** repeat CDD on changes in customer or ownership data, doubts or suspicion.
- **Business customers:** verify beneficial owners independently of the CRBR extract, and record any discrepancies.

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 KYC onboarding with ID document capture and verification, including NFC chip reading of identity cards and passports.
- Biometric liveness detection and face match for unassisted remote onboarding, with configurable consent and fallback routes.
- Video KYC with recorded, agent-led sessions for customers who choose a non-biometric route.
- KYB and beneficial owner verification, plus AML screening against sanctions, PEP and watchlists at onboarding and on an ongoing basis.
- No-code workflow builder and an audit trail of every check, with cloud, on-premises or hybrid deployment.

[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 on Counteracting Money Laundering and Terrorist Financing], consolidated text Dz.U. 2025 poz. 644, Art. 2, 27, 33 to 49, 72, 74, 86, 117, 118, 150, 151. dziennikustaw.gov.pl; status: isap.sejm.gov.pl
- **Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe** [Banking Law], consolidated text Dz.U. 2026 poz. 38, Art. 6a, 6b, 6d, 7, 30, 32, 34, 36, 48l, 104, 171. dziennikustaw.gov.pl; status: isap.sejm.gov.pl
- **Ustawa z dnia 31 lipca 2026 r. o zmianie ustawy – Prawo bankowe oraz niektórych innych ustaw** [Act amending the Banking Law], Dz.U. 2026 poz. 1206, published 14 September 2026, Art. 1, 33 and 57. dziennikustaw.gov.pl

- **Ustawa z dnia 25 lipca 2025 r. o zmianie ustawy – Prawo bankowe oraz niektórych innych ustaw** [Act amending the Banking Law], Dz.U. 2025 poz. 1191, Art. 1. dziennikustaw.gov.pl
- **Ustawa z dnia 10 czerwca 2016 r. o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji** [Act on the Bank Guarantee Fund], consolidated text Dz.U. 2026 poz. 620, Art. 24. dziennikustaw.gov.pl
- **Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych** [Payment Services Act], consolidated text Dz.U. 2026 poz. 623, Art. 32i. dziennikustaw.gov.pl
- **Rządowy projekt ustawy o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu** [Government bill amending the AML Act], Sejm print no. 3163, 28 September 2026. sejm.gov.pl
- **Stanowisko UKNF dotyczące identyfikacji klienta i weryfikacji jego tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideoweryfikacji** [KNF position on video verification in banks], 5 June 2019. knf.gov.pl
- **Stanowisko UKNF dot. prawidłowego wykorzystania w sektorze finansowym 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 przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu** [KNF position on internal AML procedures], 19 March 2026. knf.gov.pl; list of positions: knf.gov.pl
- **Biometryczna weryfikacja tożsamości klientów usług płatniczych** [Biometric identity verification of payment service customers], President of the Personal Data Protection Office, 30 April 2024. uodo.gov.pl
- **Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji ustawy w 2025 roku** [GIIF annual report for 2025], March 2026, sections 4.1.2 and 5. gov.pl
- **Kara administracyjna nałożona przez KNF na Credit Agricole Bank Polska S.A.** [Administrative penalty imposed by the KNF], Ministry of Finance, published 13 June 2025. gov.pl
- **Kara administracyjna nałożona przez KNF na mBank S.A.** [Administrative penalty imposed by the KNF], Ministry of Finance, published 9 October 2025. gov.pl
- **Regulation (EU) 2024/1624** on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, OJ L 2024/1624, 19 June 2024, recital 66. eur-lex.europa.eu