



Identomat

COMPLIANCE GUIDE

Fintech & Digital Payments Compliance in Poland

COUNTRY **Poland**

INDUSTRY **Fintech & Digital Payments**

LAST UPDATED **20 October 2026**

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

Key takeaways

- To run payments, an e-wallet or e-money from Poland you need a licence from the Polish Financial Supervision Authority (KNF) or, for smaller domestic models, an entry in one of its registers. Running a payment business without one is a criminal offence.
 - Consumer lending apps that are not banks must be entered in the KNF register of lending institutions before their first loan, with at least PLN 1 million in share capital.
 - Every payment, e-money and lending firm must identify and verify each customer before opening an account, and must report transactions above EUR 15,000 and any suspicious activity to the General Inspector of Financial Information (GIIF), the national financial intelligence unit.
 - Fully online onboarding is allowed, but the law treats it as higher risk unless the risk is reduced, for example by an EU-recognised electronic ID. The KNF expects document authenticity checks, liveness detection and face matching when a customer onboards without a human agent.
 - Two changes are coming: the EU Anti-Money Laundering Regulation applies directly from 10 July 2027, and new EU consumer credit rules apply from 20 November 2026, although Poland had not yet passed its implementing act as of 20 October 2026.
-

Poland is open to digital payment, e-money and lending businesses, and the rules are the same whether a firm operates through an app or a branch network. Licensing is national and handled by one supervisor, the KNF. The Ministry of Finance's GIIF leads anti-money laundering supervision alongside the KNF.

The biggest practical hurdle for a new entrant is remote onboarding. The law permits it, but the KNF sets detailed expectations for how firms verify identity without the customer present, and the data protection authority treats biometric checks as an activity that needs explicit consent and an alternative route.

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

Regulator	Remit	Level	Official site
Polish Financial Supervision Authority (KNF)	Authorises and supervises payment and e-money institutions, keeps the registers of small payment institutions and lending institutions, inspects AML compliance of supervised firms	National	knf.gov.pl
General Inspector of Financial Information (GIIF), Ministry of Finance	Financial intelligence unit; receives threshold and suspicious activity reports, inspects all obliged institutions, imposes AML penalties	National	gov.pl/web/finanse
Office of Competition and Consumer Protection (UOKiK)	Collective consumer interests, including practices of consumer lenders and payment providers	National	uokik.gov.pl
President of the Personal Data Protection Office (UODO)	Data protection, including biometric identity checks	National	uodo.gov.pl
Financial Ombudsman (Rzecznik Finansowy)	Out-of-court handling of customer complaints against financial firms	National	rf.gov.pl

European Banking
Authority (EBA) and
EU Anti-Money
Laundering Authority
(AMLA)

EU guidelines on payments and
remote onboarding; EU-level AML
supervision from the new
framework

Supranational eba.europa.eu

Under the AML Act, the KNF inspects the AML compliance of the institutions it supervises, while the GIIF can inspect any obliged institution and coordinates inspections by other authorities ([AML Act, arts. 130 to 132](#)).

2 Licensing and authorisation

The Act of 19 August 2011 on Payment Services (Ustawa o usługach płatniczych, latest consolidated text Dz.U. 2026 poz. 623) sets out the licence routes. It lists eight payment services, from account-based transfers and card issuing to acquiring, money remittance, payment initiation and account information ([art. 3\(1\)](#)). The route depends on the services offered and the volume processed.

Status	Who it suits	Gate	Initial capital
National payment institution (art. 60)	Full payment service providers, wallets, acquirers, cross-border models	KNF authorisation; decision within 3 months of a complete application (art. 62)	EUR 125,000; EUR 50,000 for payment initiation; EUR 20,000 for money remittance only (art. 64)
Small payment institution (arts. 117f to 117h)	Domestic start-ups averaging no more than EUR 1.5 million a month in payment transactions	Entry in the KNF register; Poland only; may hold at most EUR 2,000 per user	No minimum set in the Act
Account information provider only (art. 117a)	Open banking aggregators	Entry in the KNF register; civil liability insurance or guarantee	No minimum set in the Act
National e-money institution (art. 132a)	Prepaid wallets and stored-value products	KNF authorisation	EUR 350,000 (art. 132b)

Lending institution (Consumer Credit Act, arts. 59a to 59ac)

Non-bank consumer lenders, including online lenders

Entry in the KNF register of lending institutions before starting

PLN 1,000,000 share capital, paid in cash

An applicant for a payment institution licence must file a programme of operations and a three-year financial plan, proof of own funds, a description of its risk management and internal control system, its use of information and communication technology services under the EU Digital Operational Resilience Act, and fitness and propriety information on managers and qualifying shareholders (art. 61). The risk management system must cover AML obligations and the safeguarding of customer funds (art. 64(1)(3)).

Providing payment services or issuing e-money without authorisation carries a fine of up to PLN 5,000,000, imprisonment of up to 2 years, or both. The same applies to using terms such as "payment institution" in a company name or advertising without entitlement (Payment Services Act, art. 150). A non-bank lender operating without registration faces a fine of up to PLN 500,000 ([Consumer Credit Act, art. 59h](#)).

3

AML, KYC and customer due diligence

Payment institutions, e-money institutions, branches of EU payment and e-money institutions, small payment institutions, payment service offices and acquirers are obliged institutions under the Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing ([art. 2\(1\)\(3\)](#)). Lending institutions under the Consumer Credit Act are covered by art. 2(1)(25). There is no turnover threshold: the obligation follows the status.

When due diligence applies

On starting a business relationship; for an occasional transaction of EUR 15,000 or more, or a transfer of funds above EUR 1,000; on suspicion of money laundering or terrorist financing; and on doubts about identification data (art. 35).

What must be collected

For an individual: name, citizenship, PESEL number (or date and country of birth), series and number of the identity document, and address if held. Business details are added for sole traders (art. 36).

Beneficial owners

Firms must identify and verify beneficial owners and may not rely solely on the Central Register of Beneficial Owners (art. 37(3)).

If due diligence fails

The firm must not open the relationship or carry out the transaction, must end an existing relationship, and must consider reporting to the GIIF (art. 41).

Enhanced due diligence applies in higher-risk cases; the open list of risk factors includes products that favour anonymity, unknown third parties paying in for the customer, new products and distribution channels or technologies, links to high-risk third countries and non-face-to-face relationships (art. 43(2)). Simplified measures are allowed only where the firm's own risk assessment confirms lower risk (art. 42).

Reporting to the GIIF has three tiers:

- **Threshold reports:** cash deposits and withdrawals, and transfers of funds, above EUR 15,000, filed within 7 days. Some domestic transfers between obliged institutions and own-account transfers are excluded (art. 72).
- **Suspicious activity reports:** circumstances that may indicate money laundering or terrorist financing, filed no later than 2 working days after the suspicion is confirmed (art. 74).
- **Suspicious transaction notices:** filed before execution. The firm may not execute the transaction for up to 24 hours after the GIIF acknowledges the notice, and the GIIF can require a hold or account block of up to 96 hours (art. 86).

Due diligence records, including information obtained through electronic identification and trust services, and transaction records are kept for 5 years from the end of the relationship or the occasional transaction (art. 49).

4

Identity verification and onboarding

Verification means confirming the identification data against an identity document, a current register extract, or other documents, data or information from a reliable and independent source. That includes, where available, electronic identification means and trust services under the EU eIDAS Regulation ([AML Act, art. 37\(1\)](#)).

The mObywatel document in the government app has the same legal effect as an identity card wherever the law requires identity to be established from an identity document. It holds the user's name, PESEL number, date of birth, citizenship, photograph and document number ([Act on the mObywatel Application, art. 7](#)). Obligated institutions must apply the

Act's rules on using it for customer identification and verification since 1 September 2023 (art. 83). A recipient can check its authenticity through the minister's electronic seal, the user's electronic signature, data checks or its visual security features (art. 9).

The KNF's position on remote onboarding of 29 September 2023 applies the EBA guidelines on remote customer onboarding (EBA/GL/2022/15) to Polish law. It sets the supervisor's expectations for every institution it supervises ([KNF position](#)):

- **Documents:** where a copy or scan is accepted, check security features against official databases such as the EU's PRADO register, the integrity of the machine-readable zone, signs of a replaced photograph, image quality, and whether the document was photographed off a screen. Where the device can read the identity document's chip, firms should consider using that data.
- **Unattended (automated) flows:** photographs or video must be captured during the session itself, with a liveness check and strong, reliable face-matching algorithms against the document photograph.
- **Agent-led video:** trained staff following a scripted interview, adequate image and sound quality, and where possible random assignment of agents and randomised customer actions.
- **Additional mitigants** proportionate to risk: a first payment from the customer's own account at a regulated European Economic Area institution (supporting evidence only, never the sole method), one-time passcodes, a phone call or direct correspondence.
- **Fallback:** if quality or reliability is insufficient, stop and restart the remote process or redirect the customer to in-person verification.

Notified eIDAS electronic identification schemes at the "substantial" or "high" assurance level, and qualified trust services, are treated as meeting several of these requirements on their own. Firms may use third parties for due diligence (art. 47) or outsource it (art. 48), but the obliged institution remains responsible in both cases.

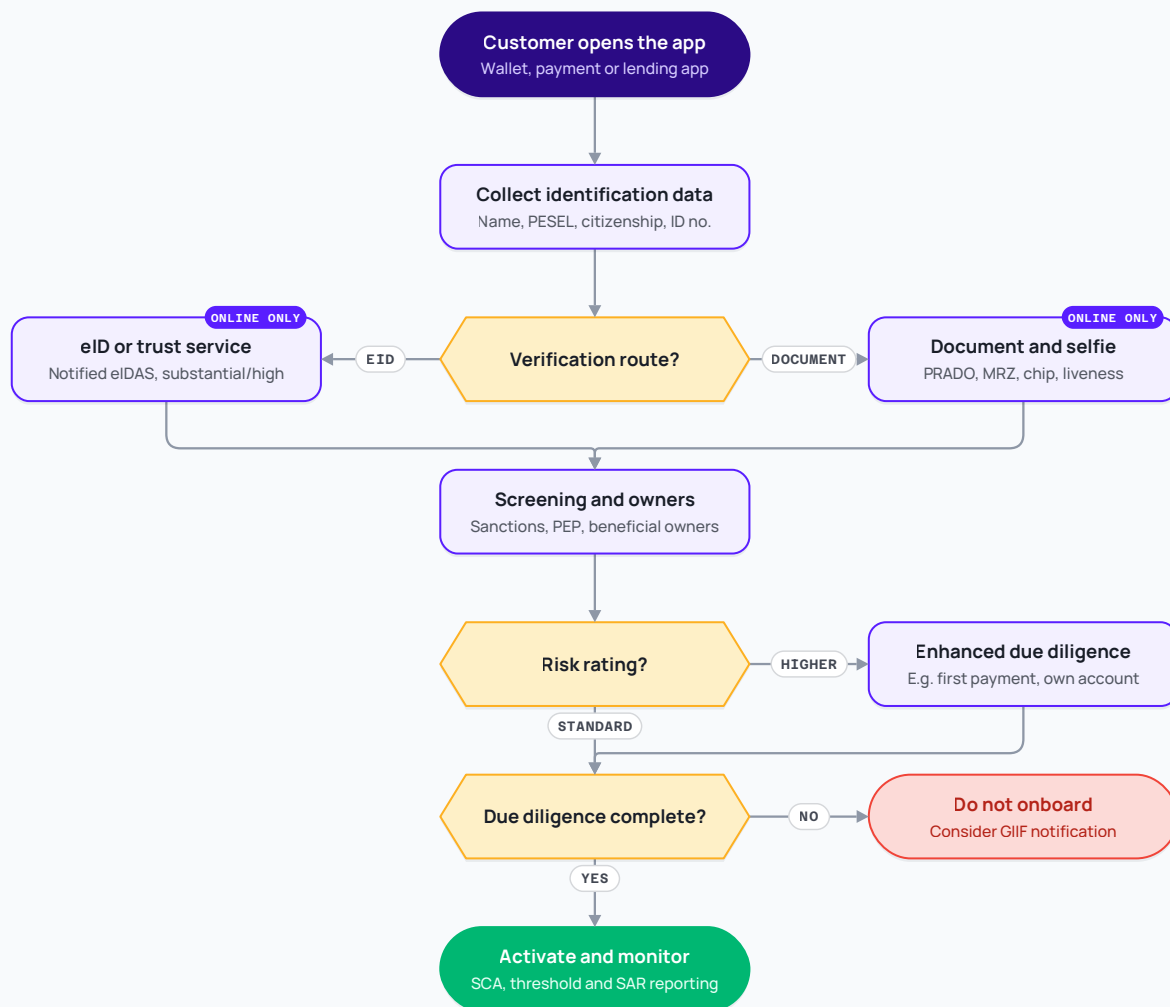


Figure 1. Remote onboarding for a payment, e-money or lending app in Poland.

5 Digital channels: what's different

Bottom line: the licences and reporting duties are channel-neutral, but remote onboarding is a statutory higher-risk factor unless mitigated, and the KNF expects specific technical controls when the customer is not present.

Requirement	In person / branch	Online / remote	Difference
Licence or registration	Payment Services Act routes	Same routes; no separate online licence	Same

Identification data	AML Act art. 36 elements	Same elements	Same
Risk treatment	Risk-based	Higher-risk factor unless mitigated, e.g. by eIDAS eID (art. 43(2) (7))	Differs
Accepted evidence	Original identity document or mObywatel	eID, trust services, mObywatel, or document copy with authenticity checks	Differs
Liveness and face match	Not required	Expected by the KNF for unattended flows	Differs
Low-value e-money exemption	Up to EUR 150, conditions apply	Lost for any remote payment above EUR 50	Differs
Strong customer authentication	For electronic payments	Also for online account access and risky remote actions	Differs
GLIF reporting thresholds	EUR 15,000; suspicion within 2 working days	Same	Same
Record retention	5 years	5 years, including images, video and eID data, time-stamped	Same

Remote onboarding is a risk factor, not a prohibition

The AML Act lists starting or maintaining a relationship without the customer's physical presence as a higher-risk factor only where that risk has not been limited in another way, including by electronic identification means and trust services under eIDAS ([art. 43\(2\) \(7\)](#)). The KNF expects firms that cannot use eID or trust services to consider enhanced measures and to assess any new channel or technology before using it, with documented testing, monitoring and controls against IP address spoofing and virtual private networks ([KNF position, 2023](#)).

E-money exemption shrinks online

An e-money issuer may skip identification for a non-reloadable instrument, or one with a monthly limit of EUR 150 usable only in Poland, holding no more than EUR 150 and used only for purchases. The exemption does not apply to redemption or cash withdrawal above EUR 50, or to a payment initiated over the internet or another remote channel above EUR 50 (AML Act, art. 38).

Strong customer authentication

Providers must apply strong customer authentication when a payer accesses an account online, initiates an electronic payment or performs a remote action that carries a fraud risk. Internet payments require dynamic linking to the amount and payee ([Payment Services Act, art. 32i](#)). If the payer's provider does not require it, the payer bears no liability for unauthorised transactions unless acting intentionally (art. 46(4a)).

Pending

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

Adopted, applies 10 Jul 2027 will replace the national due diligence rules with directly applicable EU rules, including for remote onboarding ([EUR-Lex](#)).

6

Data protection and biometrics

The EU General Data Protection Regulation (GDPR) applies directly, supervised by the President of UODO. For fintech onboarding, the critical point is biometrics. UODO's position of 30 April 2024 on biometric verification of payment service users states that facial images and behavioural profiles (for example, typing rhythm or mouse movement) used to identify or authenticate a person are biometric data, a special category under GDPR art. 9 ([UODO bulletin, 30 April 2024](#)).

In UODO's view, biometric processing by financial institutions to verify identity should not be the basic or only method used. The sole legal basis should be the customer's explicit, informed consent, and the decision to use biometrics should follow a careful analysis, including a data protection impact assessment. In practice, a remote flow that uses face matching should offer a non-biometric route, such as an eID login, agent-led video or a branch or partner visit, for customers who decline.

The KNF expects vendors to collect only necessary data, log access to stored images and video, and keep them only for the AML retention period ([KNF position, 2023](#)).

7

Sector-specific obligations

Creditworthiness checks for online lenders

A lending institution may lend only after a positive creditworthiness assessment based on data from trusted providers, in particular the banks' credit information institution or licensed business information bureaus. If those data are insufficient, and in every case

where the loan exceeds twice the national minimum wage, it must also take the consumer's statement of income and fixed household expenses with supporting documents. The statement is annexed to the agreement ([Consumer Credit Act, art. 9a](#)).

Limits on small payment institutions

A small payment institution operates only in Poland, must keep its 12-month average below EUR 1.5 million a month (including agents) and may hold no more than EUR 2,000 per user at any time. Transfers to payees go only through a dedicated payment account at a bank or other authorised provider, which is protected from enforcement by the institution's creditors ([Payment Services Act, arts. 117f to 117ha](#)).

Agents and outsourcing

Small payment institutions may use agents and outsource operational tasks under the payment institution rules (art. 117i). A vendor performing due diligence for the firm must be treated as part of it under a written agreement, and liability stays with the firm (AML Act, art. 48).

8 Risk indicators and red flags

FINTECH AND PAYMENTS RED FLAGS (AML ACT ART. 43 AND KNF GUIDANCE)

- **Virtual account numbers:** services creating extra account numbers that let third parties identify payments or payers.
- **Unknown funders:** transfers to the customer ordered by unknown or unrelated third parties.
- **Location masking:** spoofed IP addresses or virtual private networks during remote onboarding.
- **Document tampering:** replaced photographs, altered data, broken MRZ checks or documents shown on a screen.
- **High-risk geography:** links to high-risk third countries or jurisdictions associated with corruption or terrorism.
- **Opaque ownership:** unusual or overly complex ownership for the business's size and activity.
- **Cash-intensive merchants:** business models with many or large cash transactions.
- **Fraud spikes:** a significant rise in attempted fraud, which the KNF treats as a trigger for an ad hoc review of the onboarding solution.

9 Enforcement and penalties

AML penalties are administrative and imposed by the GIIF or, for supervised firms, the KNF ([AML Act, arts. 150 and 151](#)). They include publication of the breach, an order to cease specific activity, withdrawal of the licence or deletion from the register, a ban of up to one year on the responsible manager, and a fine:

Tier	Maximum fine
General cap	Twice the benefit gained or loss avoided, or EUR 1,000,000 where that cannot be established
Financial institutions, including payment, e-money and lending institutions (legal persons)	EUR 5,000,000 or 10% of turnover in the last approved financial statements

Separately, the KNF can fine a payment institution up to PLN 1,000,000 and a responsible manager up to PLN 500,000, restrict its activity or withdraw its authorisation ([Payment Services Act, art. 105](#)).

Recent KNF decisions in the sector include a PLN 200,000 fine on Payment Technology sp. z o.o. in 2025. The breaches covered its institutional risk assessment, customer identification and verification, ongoing monitoring of higher-risk relationships, documentation of due diligence and staff training. In July 2026 the KNF fined lending institution Reliance Capital SA PLN 178,000 for breaches of its Consumer Credit Act reporting duties ([KNF list of penalties](#)).

10 Recent changes and what to watch

- **9 October 2026:** government bill amending the AML Act (Sejm print 3163) had its first reading **Bill, not enacted**. It would extend asset freezing to proliferation financing, widen GIIF inspection powers and change access to the beneficial ownership register ([Sejm legislative record](#)).
- **20 November 2026:** the new EU Consumer Credit Directive (2023/2225) applies, bringing buy now, pay later and loans under EUR 200 into scope ([EUR-Lex](#)) **Polish implementing act not adopted**. As of 20 October 2026 no implementing bill had reached the Sejm, so the 2011 Consumer Credit Act still governs Polish lenders.
- **1 January to 11 February 2027:** three amending acts change the Payment Services Act and the AML Act, covering administrative procedure simplification, third-country branches and KNF fees **Adopted, effective 1 Jan to 11 Feb 2027**.
- **10 July 2027:** the EU Anti-Money Laundering Regulation applies directly **Adopted, applies 10 Jul 2027**. Due diligence rules, thresholds and remote onboarding standards will come from EU law rather than the 2018 Act ([EUR-Lex](#)).
- **In force:** KNF position on remote onboarding (29 September 2023) and use of mObywatel for customer verification (since 1 September 2023) **In force**.

- **Data capture:** collect PESEL (or date and country of birth for foreigners), citizenship and identity document series and number at registration; they are mandatory identification elements.
- **Preferred remote methods:** notified eIDAS eID at substantial or high level and qualified trust services carry the most regulatory weight; mObywatel is legally equivalent to the identity card.
- **Document and selfie flows:** document authenticity checks (PRADO, MRZ, chip where readable), in-session capture, liveness and face matching are KNF expectations, not options.
- **Biometrics:** explicit consent, a data protection impact assessment and a non-biometric alternative route.
- **Timing:** due diligence must be complete before the first transaction, and purpose and intended nature of the relationship captured before onboarding ends.
- **Re-verification triggers:** changes in customer or beneficial owner data, doubts about earlier data, and changes in the nature of the relationship (art. 35).

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 onboarding with ID document capture and verification, including NFC chip reading, face match and biometric liveness, in line with KNF expectations for unattended flows.
- Video KYC with agent-led sessions for customers who decline biometric checks or need enhanced due diligence.
- AML screening against sanctions, PEP and adverse-media lists, with ongoing monitoring of existing customers.
- KYB and beneficial owner verification for merchant and business customers.
- No-code workflow builder and a time-stamped audit trail to support the five-year AML record-keeping duty.

[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 19 sierpnia 2011 r. o usługach płatniczych** [Act of 19 August 2011 on Payment Services], Dz.U. 2011 poz. 1175, consolidated text Dz.U. 2026 poz. 623 as amended, arts. 3, 32i, 46, 60 to 64, 105, 117a, 117f to 117i, 132a, 132b, 150, ISAP, isap.sejm.gov.pl
- **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, arts. 2, 35 to 38, 41 to 43, 47 to 49, 72, 74, 86, 130, 150, 151, ISAP, isap.sejm.gov.pl

- **Ustawa z dnia 12 maja 2011 r. o kredycie konsumenckim** [Act of 12 May 2011 on Consumer Credit], Dz.U. 2011 poz. 715, consolidated text Dz.U. 2025 poz. 1362 as amended, arts. 9a, 59a to 59ac, 59h, ISAP, isap.sejm.gov.pl
- **Ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel** [Act of 26 May 2023 on the mObywatel Application], Dz.U. 2023 poz. 1234, consolidated text Dz.U. 2026 poz. 1232, arts. 7, 9, 83, ISAP, isap.sejm.gov.pl
- **Stanowisko UKNF dotyczące prawidłowego wykorzystania w sektorze finansowym rozwiązań w zakresie nawiązywania stosunków gospodarczych bez fizycznej obecności klienta** [KNF Office position on remote onboarding], 29 September 2023, knf.gov.pl
- **Wykaz kar nałożonych przez KNF w 2025 i 2026 roku** [KNF lists of penalties imposed in 2025 and 2026], updated October 2026, knf.gov.pl
- **Biometryczna weryfikacja tożsamości klientów usług płatniczych** [Biometric verification of payment service users], UODO bulletin, 30 April 2024, uodo.gov.pl
- **Rządowy projekt ustawy o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu** [Government bill amending the AML Act], Sejm print 3163, legislative record as of 9 October 2026, sejm.gov.pl
- **Directive (EU) 2023/2225 on credit agreements for consumers**, EUR-Lex, eur-lex.europa.eu
- **Regulation (EU) 2024/1624 on the prevention of the use of the financial system for money laundering or terrorist financing**, EUR-Lex, eur-lex.europa.eu