



Identomat

COMPLIANCE GUIDE

Fintech & Digital Payments Compliance in Bulgaria

COUNTRY **Bulgaria**

INDUSTRY **Fintech & Digital Payments**

LAST UPDATED **21 October 2026**

KEY REGULATORS **Bulgarian National Bank · State Agency for National Security, Financial Intelligence Directorate · National Revenue Agency**

Key takeaways

- To offer payments or issue e-money from Bulgaria you need a licence from the Bulgarian National Bank (BNB): a payment institution licence (initial capital from 20,000 to 125,000 euro, depending on the services) or an e-money company licence (at least 350,000 euro).
- Payment and e-money firms are covered by Bulgaria's anti-money laundering (AML) law. They must check customers' identity, screen for sanctions and politically exposed persons, monitor transactions and report suspicions to the Financial Intelligence Directorate before carrying out the suspicious payment.
- Fully online onboarding is allowed. In return, a firm must verify the customer's identity with at least two methods, run controls against forged documents and stolen identities, and follow fixed conditions if it uses live video calls.
- Since 1 June 2026, payment and e-money firms that keep IBAN accounts must send account data to the National Revenue Agency (NRA, Bulgaria's tax authority) at least weekly, in addition to reporting to the BNB's account register.
- More changes are on the way: the EU's single AML rulebook applies from 10 July 2027, payment and e-money firms must offer instant euro transfers by 9 April 2027, and the EU's proposed new payment services rules are not yet law.

Bulgaria is open to non-bank payment and e-money businesses, both those licensed locally and those passporting in from other EU countries. Since Bulgaria adopted the euro on 1 January 2026, the AML thresholds are set in euro.

The BNB licenses and supervises payment and e-money institutions. AML compliance is supervised both by the BNB and by the Financial Intelligence Directorate of the State Agency for National Security (DANS). The NRA receives account and card-acceptance data for tax purposes.

The biggest hurdle for a new entrant is a remote onboarding stack that meets the detailed controls in the AML Rules before the account goes live.

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 for fintech	Level	Official site
Bulgarian National Bank (BNB)	Licenses payment institutions and e-money companies, registers account information service providers and agents, runs payment supervision and AML supervision of the firms it licenses	National	bnb.bg
State Agency for National Security, Financial Intelligence Directorate (DANS FID)	Financial intelligence unit; receives suspicious transaction and cash reports; controls compliance with the AML Act through on-site inspections	National	dans.bg
National Revenue Agency (NRA)	Receives account and card-terminal data from banks and payment service providers	National	nra.bg
Commission for Personal Data Protection	Supervises processing of personal and biometric data under the GDPR	National	cpdp.bg
Consumer Protection Commission (Conciliation Commission for Payment Disputes)	Out-of-court resolution of disputes between payment service users and providers or e-money issuers	National	kzp.bg

The Financial Supervision Commission does not license payment or e-money institutions.

2

Licensing and authorisation

The Payment Services and Payment Systems Act (Закон за платежните услуги и платежните системи, last amended State Gazette No. 71 of 2026) prohibits anyone who is not a payment service provider from providing payment services (Art. 3(2)). It also bars unlicensed firms from using names or advertising that suggest they provide them.

Payment institutions

A firm planning to provide the services in Art. 4, items 1 to 7 must obtain a payment institution licence from the BNB before it starts (Art. 7). Initial capital under Art. 8 is:

- 20,000 euro for money remittance only;
- 50,000 euro for payment initiation services;
- 125,000 euro for any of the services in Art. 4, items 1 to 5 (account-based payments, card issuing and acquiring, and similar).

Account information service providers register instead of being licensed, and must hold professional indemnity insurance or a comparable guarantee (Art. 18). The BNB decides on a licence within three months of a complete application. If it asks for missing documents, the clock restarts when they arrive (Art. 11).

Under BNB Ordinance No. 16 the application must include the AML internal control mechanisms and draft internal AML rules (Art. 3(1), item 10).

E-money companies

A legal person must obtain a BNB licence as an e-money company before issuing e-money (Art. 36). Initial capital must be at least 350,000 euro (Art. 38, as amended with effect from 1 January 2026). For the issuing business, own funds must also be at least 2% of average outstanding e-money (Art. 39(3)).

Agents, outsourcing and passporting

Payment institutions may act through agents registered with the BNB before they start (Art. 28) and remain fully liable for agents, branches and subcontractors (Art. 30).

Passporting works in both directions through a branch, an agent or direct services (Arts. 32 and 33). The BNB also supervises AML compliance of Bulgarian branches and agents of firms licensed elsewhere in the EU (AML Act, Art. 108(6)).

3

AML, KYC and customer due diligence

The Measures Against Money Laundering Act (Закон за мерките срещу изпирането на пари, ZMIP; State Gazette No. 27 of 2018, last amended No. 51 of 2026) lists as obliged entities "other payment service providers" under the Payment Services Act and their agents (Art. 4, item 2). This covers payment institutions and e-money companies. The Rules on the Implementation of the Act (Правилник за прилагане, last amended State Gazette No. 61 of 2025) add the detail.

When due diligence applies

Customer due diligence applies when a firm (Art. 11):

- enters into a business relationship, including opening an account;
- carries out an occasional transaction of 15,000 euro or more, or 5,000 euro or more in cash;
- carries out an occasional transfer of funds of 1,000 euro or more;
- suspects money laundering or terrorist financing, whatever the amount;
- doubts identification data it already holds.

Low-value e-money exemption

E-money issuers and their agents may skip some measures where risk is low and the instrument is non-reloadable or capped at 150 euro a month for use in Bulgaria only, stores no more than 150 euro, is used only for purchases, cannot be funded with anonymous e-money and is monitored (Art. 24). The exemption does not cover cash redemption or remote payments above 50 euro.

Identification data

For individuals, firms collect name, date and place of birth, an identification number from an unexpired photo ID, all nationalities, and country of residence and address, which

cannot be a post office box (Art. 53(2)). For a business relationship they also record occupation and purpose (Art. 53(3)).

For legal persons, firms check the relevant register, establish the ownership and control structure and identify beneficial owners (Arts. 54 and 59). Bulgarian entities record their beneficial owners in the Commercial Register, the Register of Non-Profit Legal Entities or the BULSTAT register (Art. 63).

Enhanced due diligence

Enhanced measures are mandatory for politically exposed persons, high-risk third countries, products favouring anonymity, high-risk new products, channels or technologies, complex or unusually large transactions, and any other higher-risk case (Art. 35).

A relationship with a politically exposed person needs approval from senior management (Art. 38).

Reporting and retention

Suspicious transactions

Report to DANS FID immediately, before executing the operation, and delay it within the time allowed. If delay is impossible, report straight after execution and give the reason (Art. 72). The FID may suspend an operation for up to five working days (Art. 73).

Cash payments

Notify DANS FID of every cash payment above 15,000 euro made by or to a customer (Art. 76, amended for the euro changeover).

Retention

Keep all due diligence documents and data, including data obtained through electronic identification, for five years from the end of the relationship. The FID may extend this by up to two years (Art. 67).

Accepted documents. Customers identify themselves with an official identity document, and the firm takes a copy (Art. 53(1)). If the document lacks some of the required data, other unexpired official documents with a photo fill the gap (Art. 53(5)).

Verification methods. Art. 55(1) lists the permitted methods: additional documents, confirmation by another obliged entity, checks of official identity-document and register databases, technical checks that a document is genuine, a first payment from an account in the customer's name at an EU or equivalent credit institution, re-requesting documents, or another method that makes the identification reliable.

Remote onboarding. When the relationship is established electronically or otherwise without the customer present, the firm must use at least two of these methods (Art. 55(2)). It must also document the date, time and the person who performed each step (Art. 55(3)).

Electronic identification. Identification and verification may also be done with electronic identification means and qualified trust services under the eIDAS Regulation (EU) No 910/2014, or with another method recognised by statute (Art. 53(8); Rules, Art. 42).

Reliance. A payment or e-money firm may rely on identification already performed by a credit institution in Bulgaria, the EU or an equivalent third country, provided that copies of the documents can be supplied within three days. It may not rely on a bank in a high-risk third country, and it stays liable for its own due diligence (Art. 56).

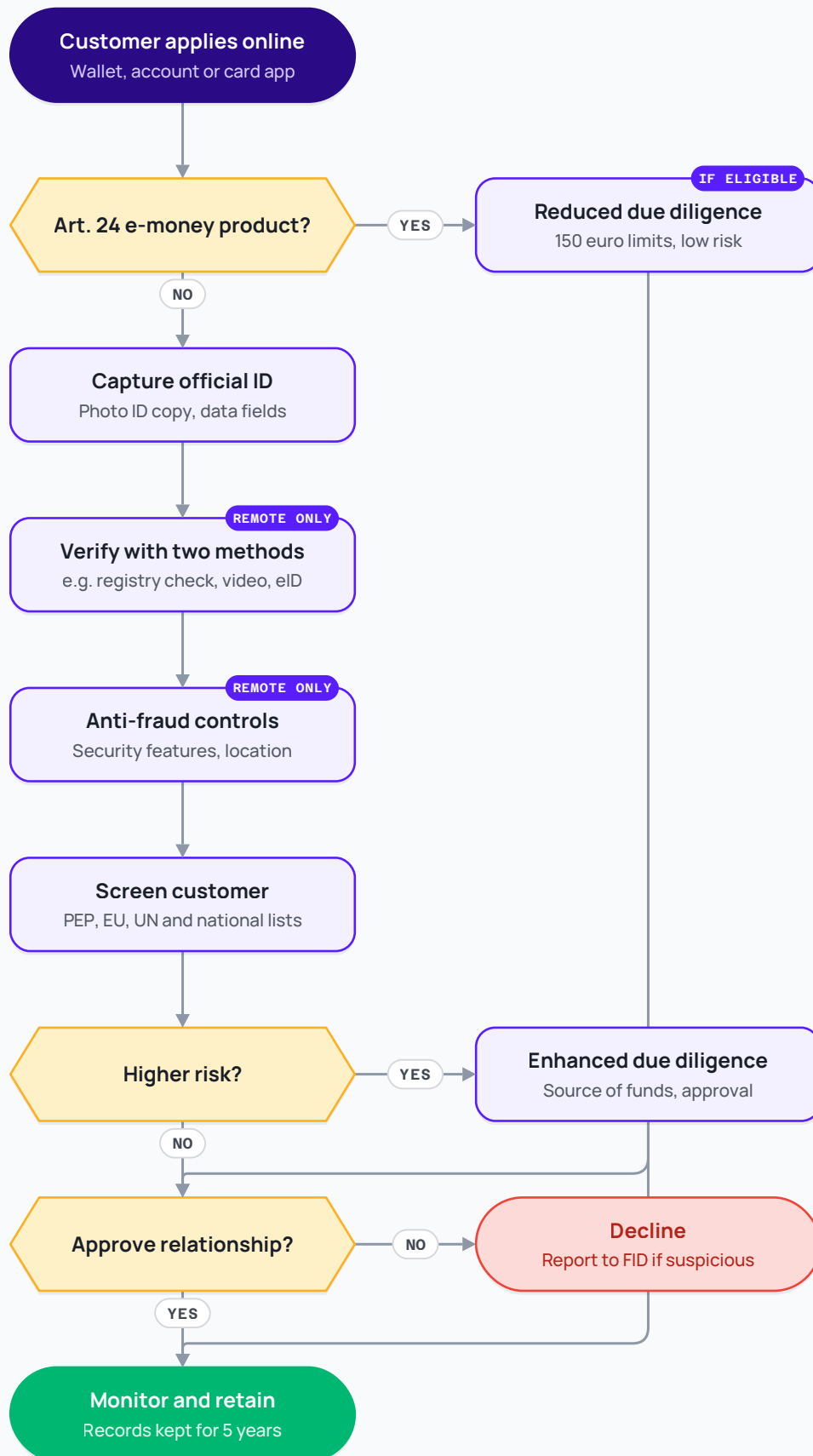


Figure 1. Remote onboarding of a retail customer by a Bulgarian payment or e-money institution.

Bottom line: remote onboarding is permitted and is not automatically high risk. However, the AML Rules impose a specific set of remote-only controls (two verification methods, document security checks, location checks and video-call conditions) that do not apply at a counter.

Requirement	In person / agent location	Online / remote	Difference
Identity document	Original official ID presented, copy taken	A copy of an official ID is acceptable	Differs
Verification of data	One or more Art. 55(1) methods	At least two Art. 55(1) methods	Differs
Risk treatment	Standard risk assessment	Remote delivery is a risk factor to assess, not an automatic trigger for enhanced checks	Differs
Anti-impersonation controls	No specific list	Internal control system required by Rules Art. 41	Differs
eID and qualified trust services	Not needed	eIDAS means and qualified trust services accepted	Differs
Due diligence triggers and thresholds	Art. 11 thresholds	Art. 11 thresholds	Same
Strong customer authentication	Not required for counter transactions	Required for online account access and electronic payments	Differs
Record retention	5 years	5 years, including video-call recordings	Same

Remote-only internal controls

Art. 41 of the AML Rules requires internal controls against false data, use of another person's documents and identification under coercion. They must detect altered

document security features, compare them with reference samples, establish the person's location and explain why a foreign customer uses a Bulgarian provider. Firms must also apply at least two document restrictions: only IDs with security features, only IDs with biometric data, a qualified electronic signature, or another risk-based condition (Art. 41(4)).

Video identification

Video calls must be run by trained staff (in-house or an external provider) in a separate room, in real time and good light, with the customer's explicit prior consent, and must record the customer's face and both sides of the ID (Art. 41(5)).

Recordings fall under the five-year retention rule (Art. 41(8)).

EBA remote onboarding guidelines

On 18 May 2023 the BNB decided to apply the EBA Guidelines on the use of remote customer onboarding solutions (EBA/GL/2022/15) from 2 October 2023, to credit and financial institutions under the AML Directive. AML Act Art. 9d makes EBA guidelines binding on obliged entities once their supervisor has decided to apply them.

Strong customer authentication

Strong customer authentication applies to online account access, electronic payments and other remote actions carrying fraud risk, with dynamic linking to amount and payee for remote payments (Payment Services Act, Art. 100).

Pending: from 10 July 2027, the EU AML Regulation will allow identity to be verified with electronic identification means at assurance level "substantial" or "high" and relevant qualified trust services, as an alternative to an identity document

Adopted, applies 10 Jul 2027 .

6

Data protection and biometrics

The GDPR applies directly, and the Commission for Personal Data Protection supervises it. Facial images processed to uniquely identify a person are biometric data (Art. 4(14)). Their processing is prohibited unless an exception in Art. 9(2) applies, such as explicit consent or substantial public interest on the basis of Union or Member State law.

The AML Rules require explicit prior consent from the customer for video identification (Art. 41(5), item 3). Firms using automated face matching should document their own Art. 9 legal basis and assess the processing in a data protection impact assessment.

Retention follows the AML Act's five-year rule (Art. 67), including eID data and video recordings.

7 Sector-specific obligations

Account register and NRA reporting

Banks, payment institutions and e-money companies report to the BNB's electronic register the following data on IBAN payment accounts (Credit Institutions Act, Art. 56a):

- account holders and authorised users;
- beneficial owners;
- any attachments (court-ordered freezes) on the accounts.

Since State Gazette No. 30 of 27 March 2026 amended Art. 25 of the National Revenue Agency Act, they must also send this data to the NRA at least weekly, and must notify the NRA within seven days of each POS or virtual POS terminal provided to traders.

The NRA applies a new data format from 1 June 2026 under Order No. 3-LIY-30-849 of 18 May 2026. Late or missing data is punishable by a sanction of 2,500 to 8,000 euro for legal persons, and 5,000 to 15,000 euro for a repeat offence (new Art. 27).

Sanctions screening

BNB guidelines on targeted financial sanctions for banks, payment institutions and e-money companies require screening of customers, beneficial owners, representatives and transaction parties against three sets of lists:

- the UN lists;
- the EU consolidated list;
- the national list under the Measures Against the Financing of Terrorism Act.

List changes should be run against the customer base within one day; a match means freezing assets and notifying the authorities.

Instant euro payments

Under Regulation (EU) 2024/886, payment institutions and e-money institutions located in a euro-area member state must offer sending and receiving of instant credit transfers in euro by 9 April 2027, including the payee-verification service the regulation introduces

Adopted, applies 9 Apr 2027. The Payment Services Act was amended with effect from 1 January 2026 to apply the regulation.

Risk indicators and red flags

RED FLAGS FROM BNB GUIDANCE FOR BANKS, PAYMENT AND E-MONEY INSTITUTIONS

- **Channel avoidance:** operations ordered only through remote channels, with the customer avoiding any direct contact with staff.
- **IP mismatch:** customer uses IP addresses far from the address established during due diligence.
- **Conflict-zone logins:** e-wallet or online access from devices or IP addresses in or near conflict zones or regions with a heightened terrorist threat.
- **Shared identifiers:** the same address, phone number or other data used across apparently unrelated accounts held by different people.
- **Third-party control:** customer accompanied or watched by third parties, suggesting someone else owns the funds or the customer is under pressure.
- **Immediate offshore transfers:** loan or other funds transferred straight to offshore accounts or unrelated third parties abroad.

Enforcement and penalties

AML Act. Penalties are per violation (Art. 116) and stated in leva in the consolidated text; the Euro Introduction Act keeps leva-denominated fines applicable under its conversion rules. Payment service providers face a property sanction of BGN 5,000 to 50,000, BGN 10,000 to 200,000 for a repeat breach, and BGN 20,000 to 10,000,000 or up to 10% of annual turnover for serious or systematic breaches.

Managers and compliance officers face personal fines, of up to BGN 15,000,000 for serious or systematic breaches (Art. 117). DANS FID publishes lists of the sanctions and fines it has imposed.

Payment Services Act. Supervised payment service providers face a property sanction of BGN 20,000 to 40,000 per breach, and BGN 40,000 to 60,000 for a repeat breach (Art. 185(3)). Two recent BNB settlements with e-money companies each ended with a BGN 14,000 sanction for breaches of Ordinance No. 16 provisions linked to registration of representatives:

- Izi Payment Services, disclosed July 2025;
- Econt Financial Services, agreed 19 December 2025 and disclosed February 2026.

Recent changes and what to watch

- **2 October 2026:** DANS opened consultation on a draft amendment to the AML Act aligning it with Directive (EU) 2024/1640 and Regulation (EU) 2024/1624, mainly on access to beneficial ownership registers **Proposed, comments close 2 Nov 2026**.
- **1 June 2026:** new NRA format for weekly account data and POS terminal notifications from banks and payment service providers **In force**.
- **27 March 2026:** National Revenue Agency Act Art. 25 rewritten and euro-denominated penalties added (State Gazette No. 30 of 2026) **In force**.
- **1 January 2026:** euro adoption; AML thresholds now in euro, e-money company capital set at 350,000 euro, and Payment Services Act measures for instant euro payments **In force**.
- **Pending:** the Commission's 2023 proposals for a Payment Services Regulation and a Third Payment Services Directive have not been adopted as of October 2026 **Proposed, not adopted**. Licensing and fraud-prevention rules will change once they are adopted and apply.
- **9 April 2027:** instant euro credit transfers and payee verification mandatory for euro-area payment and e-money institutions **Adopted, applies 9 Apr 2027**.
- **10 July 2027:** the EU AML Regulation (EU) 2024/1624 replaces most national due diligence rules **Adopted, applies 10 Jul 2027**.

What this means for identity verification

- **Two methods, by design.** Pair document authenticity checks with a second method such as a registry check, a video call, an eID or a first payment from a bank account in the customer's name.
- **Document policy.** Accepting only chip-based IDs with biometric data and security features satisfies two of the Art. 41(4) restrictions.
- **Location and context.** Capture device location or IP data and the reason a foreign resident is using a Bulgarian provider.
- **Evidence.** Keep images, results, recordings and the date, time and operator of each check for five years after the relationship ends.
- **Agents and reliance.** Agents are obliged entities, but the licensed institution remains liable for them and for its own due diligence when relying on a bank.

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 biometric documents.
- Biometric liveness and face match to support controls against use of another person's identity documents.
- Video KYC sessions run by trained agents, recorded with the customer's face and both sides of the ID.
- AML screening against sanctions, PEP and watchlists at onboarding and through ongoing monitoring.
- No-code workflow builder to combine two or more verification methods and keep an audit trail of each check.

[Request a meeting](#)

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- Закон за мерките срещу изпирането на пари [Measures Against Money Laundering Act], State Gazette No. 27 of 2018, consolidated to No. 51 of 5 June 2026, Arts. 4, 11, 24, 35, 38, 53 to 56, 59, 63, 67, 72 to 76, 108, 116, 117, Financial Supervision Commission, fsc.bg
- Правилник за прилагане на Закона за мерките срещу изпирането на пари [Rules on the Implementation of the Measures Against Money Laundering Act], State Gazette No. 3 of 2019, consolidated to No. 61 of 29 July 2025, Arts. 20, 41, 42, Financial Supervision Commission, fsc.bg

- **Закон за платежните услуги и платежните системи [Payment Services and Payment Systems Act]**, consolidated to State Gazette No. 71 of 2026, Arts. 3, 7, 8, 11, 18, 28 to 33, 36 to 39, 100, 154, 175, 185, Bulgarian National Bank, bnb.bg
- **Наредба № 16 на БНБ [BNB Ordinance No. 16 of 29 March 2018 on licences, approvals and registration]**, amended to State Gazette No. 88 of 2025, Art. 3, Bulgarian National Bank, bnb.bg
- **Закон за кредитните институции [Credit Institutions Act]**, Art. 56a, Bulgarian National Bank, bnb.bg
- **Закон за въвеждане на еврото в Република България [Euro Introduction Act]**, State Gazette No. 70 of 2024, para. 5, Bulgarian National Bank, bnb.bg
- **Act amending the Act on Revenue Collection and Expenditure in 2026** (amending Arts. 25 and 27 of the National Revenue Agency Act), State Gazette No. 30 of 27 March 2026, dv.parliament.bg
- **NRA, Data submission specification for commercial banks and payment service providers** (Order No. 3-ЦУ-30-849 of 18 May 2026), nra.bg
- **BNB press release, application of EBA Guidelines on remote customer onboarding (EBA/GL/2022/15)**, 18 May 2023, bnb.bg
- **BNB, Red flag guidelines for monitoring transactions, operations and customers (banks, payment institutions, e-money companies)**, bnb.bg
- **BNB, Guidelines on targeted financial sanctions related to terrorist financing (banks, payment institutions, e-money companies)**, bnb.bg
- **BNB supervisory disclosure, settlement with Izi Payment Services**, July 2025, bnb.bg
- **BNB supervisory disclosure, settlement with Econt Financial Services**, February 2026, bnb.bg
- **DANS, Measures against money laundering and terrorist financing** (Financial Intelligence Directorate), dans.bg
- **Public consultation No. 12770, draft Act amending the Measures Against Money Laundering Act**, 2 October to 2 November 2026, strategy.bg
- **Regulation (EU) 2024/1624 (AML Regulation)**, Arts. 22(6) and 90, EUR-Lex, eur-lex.europa.eu
- **Regulation (EU) 2024/886 (Instant Payments Regulation)**, amending Regulation (EU) No 260/2012, Art. 5a(8), EUR-Lex, eur-lex.europa.eu
- **Regulation (EU) 2016/679 (GDPR)**, Arts. 4(14) and 9, EUR-Lex, eur-lex.europa.eu
- **Proposal for a Regulation on payment services in the internal market, COM(2023) 367**, EUR-Lex, eur-lex.europa.eu