



Identomat

COMPLIANCE GUIDE

Banking & Digital Banking Compliance in Bulgaria

COUNTRY **Bulgaria**

INDUSTRY **Banking & Digital Banking**

LAST UPDATED **21 October 2026**

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

Key takeaways

- Taking deposits in Bulgaria requires a banking licence, and a new bank must be a joint-stock company with at least EUR 5 million of paid-in cash capital. Banks licensed elsewhere in the European Union (EU) can open a Bulgarian branch after their home supervisor notifies the Bulgarian National Bank.
- Every bank must identify and verify each customer before opening an account, find the real owners behind companies, check whether customers are politically exposed, and report suspicious transactions to the financial intelligence unit before carrying them out.
- Fully remote account opening is allowed. A bank that onboards without the customer present must verify identity with at least two independent methods, and the central bank expects video calls or automated selfie and document checks to meet detailed technical conditions.
- Biometric checks such as face matching need the customer's explicit consent, and photos, videos and check results must be kept for five years after the relationship ends.
- Since Bulgaria adopted the euro on 1 January 2026, due diligence and reporting thresholds are set in euro. The EU Anti-Money Laundering Regulation will replace much of the national rulebook from 10 July 2027.

Bulgaria is open to banks, including digital-only models, and the national rules expressly allow remote onboarding through video identification, electronic identification and automated document and biometric checks. Licensing is national, but prudential supervision is shared between the Bulgarian National Bank (BNB) and the European Central Bank (ECB) under the EU Single Supervisory Mechanism.

Anti-money laundering (AML) duties come from the Measures Against Money Laundering Act and its implementing Rules. The Financial Intelligence Directorate of the State Agency for National Security receives reports and inspects, while the BNB supervises banks' AML compliance and issues detailed guidelines.

For a new entrant the main obstacle is the remote onboarding standard: a product that relies on a single check, accepts uploaded photos taken before the session, or cannot document every verification step will not meet Bulgarian requirements.

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 banks	Level	Official site
Bulgarian National Bank (BNB)	Bank licensing and prudential supervision with the ECB; AML supervision of banks and their branches; AML guidelines	National	bnb.bg
European Central Bank (ECB)	Prudential supervision under the Single Supervisory Mechanism, shared with the BNB (Credit Institutions Act, Article 1(2))	Supranational	Credit Institutions Act
State Agency for National Security, Financial Intelligence Directorate (FID)	Financial intelligence unit; receives suspicious transaction and cash reports; controls application of the AML Act and imposes AML penalties	National	dans.bg
Financial Supervision Commission (FSC)	Opinion on banks' investment services and crypto-asset services; AML supervision of investment firms, insurers and other non-bank financial firms	National	fsc.bg
Registry Agency	Commercial Register, including beneficial ownership entries	National	registryagency.bg

Commission for Personal Data Protection	Supervision of the General Data Protection Regulation (GDPR), including biometric processing	National	cpdp.bg
European Banking Authority (EBA)	Guidelines the BNB has decided to apply, including on remote customer onboarding	Supranational	eba.europa.eu

Under Article 108 of the AML Act, the BNB supervises banks' AML compliance on a risk basis, and the FID inspects on site, alone or jointly with the BNB.

2 Licensing and authorisation

Article 13 of the Credit Institutions Act (Закон за кредитните институции) requires a licence to operate as a bank, meaning a legal entity that publicly takes deposits or other repayable funds and grants credit for its own account. The competent authorities under Article 1(2) are the BNB and the ECB, according to the division of tasks under the Single Supervisory Mechanism.

Capital and form

A bank is formed as a joint-stock company with minimum paid-in capital of EUR 5 million, contributed only in cash (Article 7, amended with effect from 1 January 2026). Shareholders subscribing 3% or more must show the funds are their own and of clear and lawful origin (Article 14(3)).

Decision and conditions

The authority decides within three months of a complete application (Article 14(4)). The applicant then has three months to show paid-in capital, suitable managers, premises and technical equipment, and risk management, compliance and internal audit functions (Article 15(1)).

AML programme

The business plan, internal controls and the programme of AML measures must ensure stable and effective risk management before a licence is granted (Article 14(3), point 14).

EU and third-country banks

A bank licensed in another Member State may operate through one Bulgarian branch once its home supervisor notifies the BNB (Article 20). A third-country bank needs a branch licence (Article 17).

Digital-only banks follow the same route: there is no separate online banking licence. For investment or crypto-asset services the FSC gives a written opinion within one month (Article 14(2)).

Third-country branches face new limits **Adopted, effective 11 Jan 2027** : amendments in State Gazette No. 67 of 2026 confine a third-country branch's licensed activities to Bulgarian territory, subject to narrow intragroup and reverse-solicitation exceptions.

3 AML, KYC and customer due diligence

Banks are obliged entities under Article 4, point 1 of the Measures Against Money Laundering Act (Закон за мерките срещу изпирането на пари, promulgated State Gazette No. 27 of 2018, last amended State Gazette No. 51 of 2026). Detailed procedures are in the Rules on the Implementation of the Act (Правилник за прилагане на ЗМИП, last amended State Gazette No. 39 of 2024).

When due diligence applies

Trigger (Article 11(1))	Threshold
Establishing a business relationship, including opening an account	Always
Occasional transaction, single or linked	EUR 15,000 or more
Occasional transaction paid in cash	EUR 5,000 or more
Occasional transfer of funds under Regulation (EU) 2023/1113	EUR 1,000 or more
Occasional crypto-asset transaction	EUR 1,000 or more
Suspicion of money laundering or terrorist financing, or doubts about identification data	Any amount

Due diligence covers five elements (Article 10): identifying and verifying the customer from reliable and independent sources; identifying the beneficial owner and understanding the ownership and control structure; the purpose and nature of the relationship; the source of funds; and ongoing monitoring with up-to-date records.

Enhanced and simplified due diligence

Article 35 requires enhanced due diligence for politically exposed persons (PEPs) and their family members and close associates, customers established in high-risk third countries, products that could favour anonymity, new products or technologies assessed as high risk, complex or unusually large transactions, correspondent relationships with foreign respondents, and any other case assessed as higher risk. A PEP relationship needs senior management approval (Article 38), steps to establish source of wealth (Article 39(2)) and continued treatment as a PEP for at least one year after leaving office (Article 37). PEP status cannot be established solely from the customer's own declaration (Article 42(3)). Simplified measures need senior management approval and prior notice to the FID of the lower-risk categories concerned (Articles 25 and 26).

Beneficial ownership

Bulgarian companies record their beneficial owners in the Commercial Register, the register of non-profit legal entities or the BULSTAT register (Article 63). Banks verify beneficial owners using a register extract plus documents showing the nature of ownership or control (Article 59).

Reporting and records

- **Suspicious transactions:** report to the FID immediately and before executing the transaction, delaying it within the time legally allowed; if delay is impossible, report immediately afterwards with reasons (Article 72). The FID can suspend a transaction for up to five working days (Article 73). Reports can be filed electronically through the FID's goAML system.
- **Cash payments:** report every cash payment above EUR 15,000 made by or to a customer (Article 76).
- **FID requests:** answer within three working days; banking secrecy is not a ground to refuse (Article 74).
- **Retention:** keep all due diligence documents, data and information for five years, counted from the end of the relationship (Article 67).

4

Identity verification and onboarding

A natural person is identified by presenting an official identity document and taking a copy (Article 53(1)). The bank collects names, date and place of birth, the personal identification number or other unique identifier from a valid photo identity document, every citizenship

held, and country of permanent residence and address (a post office box is not enough). For a business relationship it also records the customer's occupation and the purpose of the relationship (Article 53(3)). Legal entities are identified from a register extract and constitutional documents (Article 54).

Verification methods

Article 55(1) lists the permitted verification methods: additional documents; confirmation by another obliged entity; checks in official databases provided to verify identity documents; checks in official public registers; technical means to verify document authenticity; requiring the first payment to come from an account in the customer's name at a bank in Bulgaria, another Member State or an equivalent third country; re-requesting documents during the relationship; or another method giving reasonable assurance. Each check is documented with date, time and the employee's name (Article 55(3)).

Remote identification

Without the customer present, identification may rely on a copy of the identity document, but the data must be verified with **two or more** of the Article 55(1) methods (Articles 53(7) and 55(2)). Identification and verification may also use electronic identification means and qualified trust services under the eIDAS Regulation (EU) No 910/2014, including a notified electronic identification scheme (Article 53(8); Rules, Article 42). Article 41 of the Rules requires internal controls against false data, use of another person's documents and identification under duress; checks for tampering with security features against reference specimens; establishing the customer's location; and limiting accepted documents through at least two of: documents with security features, documents with biometric data, a qualified electronic signature, or another risk-based condition.

The BNB's Guidelines on remote establishment of business relationships with bank customers, which apply the EBA remote onboarding guidelines (EBA/GL/2022/15) to banks from 2 October 2023, accept original identity documents listed in the EU PRADO register that carry a photo and signature, a machine-readable zone and two advanced visual security features. A Bulgarian identity card without a machine-readable zone may be accepted after a risk assessment if the video session includes a check in the Ministry of Interior's online document validity service.

Reliance

A bank may rely on identification already performed by a credit institution in Bulgaria, another Member State or an equivalent third country, if the documents are available and certified copies can be provided within three days; the relying bank stays liable (Article 56). Reliance on a bank from a high-risk third country is not allowed.

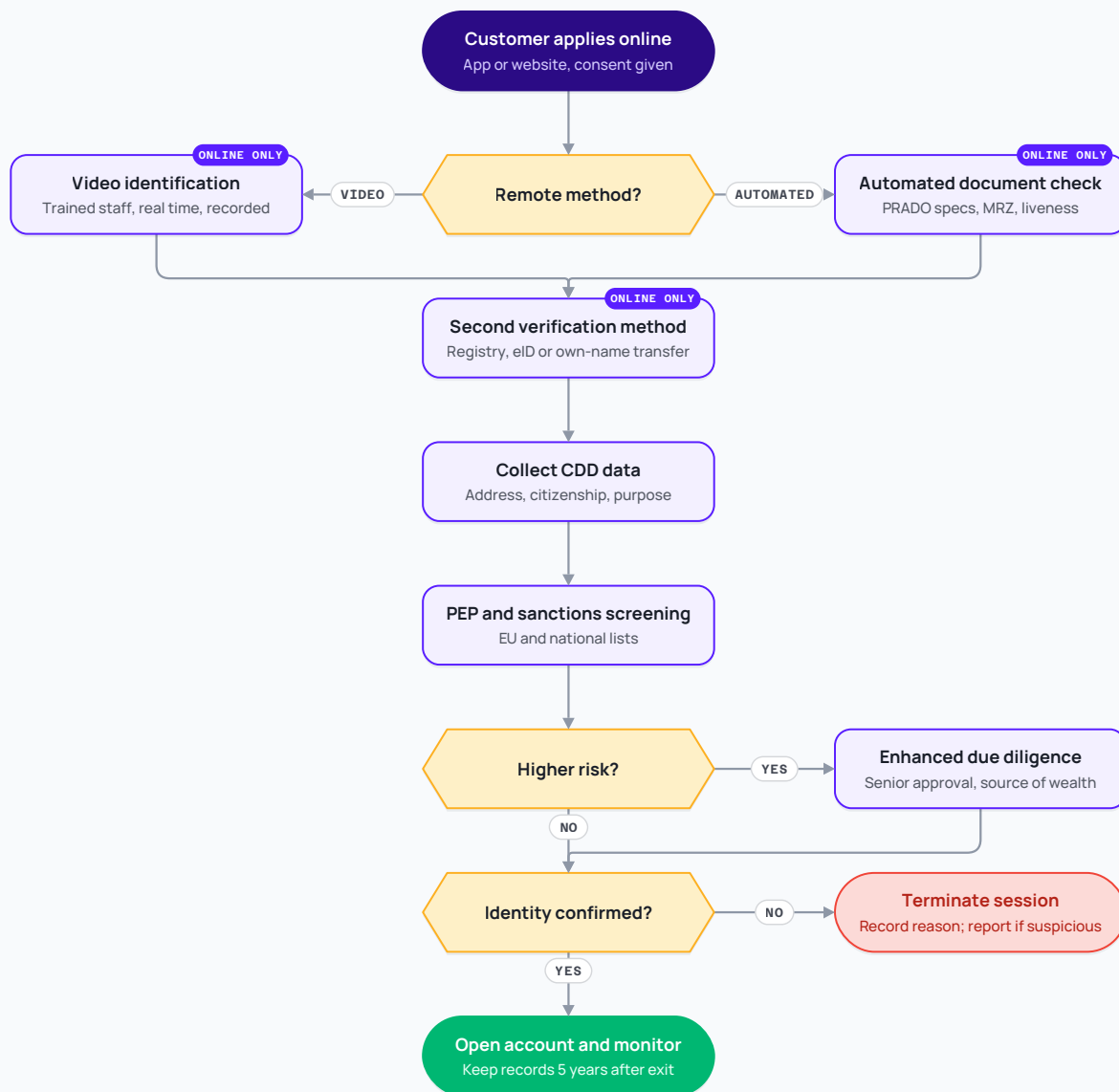


Figure 1. Remote account opening for a personal customer at a Bulgarian bank.

5

Digital channels: what's different

Bottom line: the duty to identify customers is the same in a branch and online, but remote onboarding requires at least two verification methods, prescribed technical controls and recorded evidence of each session.

Requirement	In person / branch	Online / remote	Difference
-------------	--------------------	-----------------	------------

Duty to apply due diligence at account opening	Required	Required	Same
Verification of identification data	One or more Article 55(1) methods	Two or more Article 55(1) methods	Differs
Identity document	Official document presented, copy taken	Copy accepted; BNB expects PRADO-listed documents with MRZ and security features	Differs
Risk treatment	Standard risk-based approach	Not an automatic enhanced due diligence trigger, but a separate risk assessment of the remote channel is required	Differs
Customer location	Not specified	Controls to establish the customer's location	Differs
Evidence kept	Documents and check records, 5 years	Also photos, video recordings and check results, 5 years	Differs
Biometric processing	Not required	Explicit, specific consent to biometric and remote identification	Differs
PEP and sanctions screening	Required	Required	Same

Video identification

Article 41(5) of the Rules sets minimum conditions for video conference identification: a trained employee of the bank or of an external provider, a separate room, the customer's explicit prior consent, adequate lighting, a real-time conversation, and recording of the customer's face and both sides of the identity document. The BNB adds that staff must work in a restricted-access area and that applications should be allocated to staff at random.

Automated selfie and document checks

The BNB accepts automated onboarding without staff involvement, but expects real-time capture with no files created before the session, one device throughout, movement-based liveness techniques, reliable biometric matching to the document photo and a one-time code sent by email or SMS. Because no employee is involved, banks must add risk-mitigating measures, such as requiring the first transfer to come from an account in the customer's name at an EU or FATF-member institution, code confirmation for access to remote channels, a phone call before higher-risk transactions, and device data such as IP address or location.

Stopping and outsourcing

The session must end without completion if visual verification fails, data conflict with an independent source, or money laundering risk appears unacceptable, and the reason must be recorded. A bank may outsource remote identification, but keeps ultimate responsibility, must approve every change to the provider's process, and may not use a provider in a country whose laws restrict information exchange with the bank or the BNB.

Pending

Under the eIDAS Regulation as amended by Regulation (EU) 2024/1183, banks required to use strong user authentication must accept European Digital Identity Wallets at the user's request no later than 36 months after the relevant implementing acts entered into force (Article 5f(2)) **Adopted, phased application**.

6 Data protection and biometrics

The GDPR (Regulation (EU) 2016/679) applies directly and is supervised in Bulgaria by the Commission for Personal Data Protection. Facial images processed to uniquely identify a person are biometric data (Article 4(14)), a special category whose processing is prohibited unless an exception applies, such as explicit consent (Article 9(1) and (2)(a)).

For banks, the BNB's remote onboarding guidelines require explicit and specific consent for biometric and remote electronic identification, and require customers to be informed about the processing. The Rules require explicit prior consent to video identification (Article 41(5)). All records from the remote process must be kept intact and unaltered, protected against tampering, for the five-year AML retention period. Where an onboarding provider is outside Bulgaria, banks must assess the legal, operational and data protection risks, and the BNB expects providers to be certified to information security standards.

Correspondent banking

Correspondent relationships with a respondent institution or person from another country require enhanced due diligence (Article 35, point 7, as amended in 2025).

Targeted financial sanctions

EU restrictive measures apply directly. The Measures Against the Financing of Terrorism and Proliferation of Weapons of Mass Destruction Act adds a national list adopted by the Council of Ministers, most recently amended by Decision No. 606 of 16 August 2024, and the BNB publishes the consolidated list.

Euro changeover

Amendments in State Gazette No. 70 of 2024 converted the AML Act's due diligence and cash-reporting thresholds to euro with effect from Bulgaria's euro adoption on 1 January 2026, and the Credit Institutions Act's capital requirement now stands at EUR 5 million. The AML Act's penalty provisions are still stated in leva in the consolidated text published in June 2026.

RED FLAGS FROM THE BNB'S GUIDELINES FOR BANKS (FEBRUARY 2024)

- **Shared identifiers:** the same addresses, phone numbers or employment details used across apparently unrelated accounts.
- **False contact data:** random or sequential phone numbers, or numbers that are disconnected or do not exist.
- **Unstable profile:** unexpected or frequent changes to phone, email or other contact details.
- **Remote-only behaviour:** operations ordered exclusively through remote channels while avoiding any direct contact with staff.
- **Location mismatch:** IP addresses far from the address established at due diligence, or logins from conflict zones.
- **Pass-through accounts:** frequent incoming transfers promptly forwarded to other persons.
- **Screening evasion:** attempts to avoid name checks against sanctions lists or use of aliases instead of full names.
- **Unexplained credit use:** drawing a credit line to its limit with no repayments.

Article 116 of the AML Act sets penalties per violation, unless the act is a crime. Banks and other financial obliged entities face a property sanction of BGN 5,000 to 50,000; BGN 10,000 to 200,000 for a repeated violation; and for serious or systematic violations BGN 20,000 to 10,000,000 or up to 10% of annual turnover. Natural persons face fines of BGN 1,000 to 10,000, rising to BGN 5,000 to 2,000,000 for serious or systematic violations.

The FID publishes a register of the property sanctions it has imposed (version dated 20 February 2026). It records a penalty decree of 12 February 2025 against TBI Bank EAD for breaches relating to information requested by the FID (Article 74(2), (5) and (11)), with a BGN 3,500 sanction settled by agreement.

Recent changes and what to watch

- **8 July 2026:** bill 52-654-01-82 to amend the AML Act **Bill, not enacted**. It would require banks to screen new relationships for links to sanctioned persons over five years and monitor such relationships monthly with reports to the FID.
- **5 June 2026:** State Gazette No. 51 amended the AML Act to add the Anti-Corruption Commission as a recipient of FID disclosures **In force**. No change to banks' due diligence duties.
- **1 January 2026:** euro adoption converted AML thresholds and bank capital to euro **In force**. Systems and policies must use the euro thresholds.
- **4 July 2025:** State Gazette No. 54 amended the AML Act, including the transfer-of-funds trigger under Regulation (EU) 2023/1113 and correspondent relationships **In force**. It also amended the penalty provision for financial obliged entities.
- **11 January 2027:** third-country branch limits under the Credit Institutions Act **Adopted, effective 11 Jan 2027**. Non-EU banks must plan Bulgarian branch activities accordingly.
- **10 July 2027:** the EU Anti-Money Laundering Regulation (EU) 2024/1624 applies **Adopted, effective 10 Jul 2027**. It allows verification by eIDAS electronic identification at assurance level "substantial" or "high" and qualified trust services (Article 22(6)).

What this means for identity verification

- Design remote onboarding around two independent verification methods, for example document authentication plus a registry check, eID or a first transfer from an own-name account.
- Accept identity documents that meet PRADO specifications with a machine-readable zone; plan a separate path, including the Ministry of Interior validity check, for Bulgarian identity cards without one.
- Capture images in real time on one device with liveness detection and biometric matching; reject pre-recorded files.
- Collect explicit consent for biometric processing and video recording before the session starts.
- Log date, time, operator and every check result, and retain recordings and results for five years after the relationship ends.
- Build PEP checks on databases, not self-declaration alone, and screen against EU and national sanctions lists.

- Re-verify when identification data are doubted or change, and plan for the EU Anti-Money Laundering Regulation from July 2027.

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 KYC onboarding with ID document capture and verification, including NFC chip reading and checks of security features and the machine-readable zone.
- Video KYC with recorded sessions conducted by trained agents, supporting real-time video identification.
- Biometric liveness and face match against the document photo, with explicit consent capture in a no-code workflow.
- AML screening against sanctions, PEP and adverse-media lists at onboarding, plus ongoing monitoring.
- KYB and beneficial owner verification for corporate customers, with an audit trail of every 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], ДВ бр. 27/2018, consolidated as amended to ДВ бр. 51/2026, Articles 4, 10, 11, 25 to 26, 35 to 42, 53 to 59, 63, 67, 72 to 76, 108, 116, Financial Supervision Commission, fsc.bg

- **Правилник за прилагане на Закона за мерките срещу изпирането на пари [Rules on the Implementation of the AML Act]**, ДВ бр. 3/2019, as amended to ДВ бр. 39/2024, Articles 30, 41 and 42, State Agency for National Security, dans.bg
- **Закон за кредитните институции [Credit Institutions Act]**, ДВ бр. 59/2006, as amended to ДВ бр. 71/2026, Articles 1, 2, 7, 13 to 17, 20, Bulgarian National Bank, bnb.bg
- **Насоки за дистанционно установяване на делови взаимоотношения с клиенти на банки [BNB Guidelines on remote establishment of business relationships with bank customers]**, January 2024, Bulgarian National Bank, bnb.bg
- **Насоки за червени флагове за мониторинг на сделки, операции и клиенти [BNB Guidelines on red flags for monitoring transactions, operations and customers]**, February 2024, section 3, Bulgarian National Bank, bnb.bg
- **BNB AML guidelines index**, Bulgarian National Bank, bnb.bg
- **List of persons under the Measures Against the Financing of Terrorism and Proliferation Act**, Bulgarian National Bank, bnb.bg
- **Measures against money laundering and terrorist financing**, Financial Intelligence Directorate, State Agency for National Security, dans.bg
- **Указания за уведомяване по чл. 72 от ЗМИП и чл. 9 от ЗМФТ [Instructions on reporting under Article 72 AML Act]**, 18 March 2024, Financial Intelligence Directorate, dans.bg
- **Наложени имуществени санкции [Register of property sanctions imposed]**, version of 20 February 2026, Financial Intelligence Directorate, dans.bg
- **Bill 52-654-01-82 amending the Measures Against Money Laundering Act**, submitted 8 July 2026, National Assembly, parliament.bg
- **Regulation (EU) 2024/1624 on the prevention of the use of the financial system for money laundering or terrorist financing**, Articles 22 and 90, EUR-Lex, eur-lex.europa.eu
- **Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 (European Digital Identity Framework)**, Article 5f, EUR-Lex, eur-lex.europa.eu
- **Regulation (EU) 2016/679 (General Data Protection Regulation)**, Articles 4(14) and 9, EUR-Lex, eur-lex.europa.eu