KNOW YOUR BUSINESS POLICY

PayNox EOOD

ID number: 208071994

Legal address: Bulgaria, City of Burgas, 19 Marahydyk St., fl. 2, office 1

Table of contents

INTRODUCTION

The Know Your Business (KYB) Policy at PayNox is designed to ensure that all corporate clients undergo thorough verification before gaining access to our financial services. This policy aligns with Bulgarian regulations, EU directives, and FATF Recommendations to prevent financial crimes, including money laundering, fraud, and sanctions violations.

PayNox verifies companies' legal status, ownership structures, and business activities. Automated compliance tools such as LexisNexis, Refinitiv, and ComplyAdvantage are used for verifying corporate identities, checking Ultimate Beneficial Owners (UBOs), and conducting real-time risk assessments. High-risk entities undergo Enhanced Due Diligence (EDD).

By implementing continuous monitoring, sanctions screening, and adverse media checks, PayNox maintains a secure and compliant financial ecosystem. This approach not only mitigates risks but also enhances trust and security within the digital asset and payment processing industry.

DEFINITIONS

To ensure clarity and consistency in the Know Your Business (KYB) Policy, the following key terms are defined:

Know Your Business (KYB) is a compliance process used to verify the identity, legitimacy, and financial integrity of corporate clients. KYB helps prevent financial crimes such as money laundering, fraud, and terrorist financing by ensuring that businesses operate transparently and legally.

Ultimate Beneficial Owner (UBO) is A natural person who ultimately owns or controls a legal entity, either directly or indirectly, typically holding 25% or more of shares or voting rights. Identifying UBOs is a critical part of KYB to prevent hidden ownership structures that facilitate illicit activities.

Legal Entity is a company, partnership, or organization that has legal standing and can engage in business activities, enter contracts, and hold financial accounts. Examples include limited liability companies (LLCs), joint-stock companies (JSCs), and partnerships.

Enhanced Due Diligence (EDD) is a higher level of scrutiny applied to corporate clients identified as high-risk due to factors such as jurisdiction, industry, or ownership structure. EDD involves in-depth investigations, additional documentation, and ongoing monitoring to mitigate risks.

Sanctions Screening is a process of checking businesses, UBOs, and related parties against international sanctions lists such as the EU Sanctions List, UN Sanctions, U.S. OFAC List, and UK HM Treasury Sanctions. This ensures that PayNox does not engage with restricted or blacklisted entities.

Politically Exposed Person (PEP) is an individual who holds a prominent public position (e.g., government official, judge, military leader) and is at a higher risk of involvement in corruption or financial crimes. KYB includes PEP screening to assess potential risks related to corporate clients.

Risk-Based Approach (RBA) is a compliance strategy that categorizes businesses based on risk levels (low, medium, high) and applies appropriate due diligence measures. Higher-risk clients undergo more extensive verification and monitoring to ensure compliance.

Adverse Media Screening is a review of publicly available news sources and reports to detect negative media coverage related to financial crimes, fraud, or regulatory violations involving corporate clients or their stakeholders.

Continuous Monitoring is an ongoing assessment of corporate clients, transactions, and business activities to detect changes in risk profiles, ownership structures, or suspicious behaviors. This helps ensure long-term compliance with Bulgarian and EU regulations.

SCOPE

The Know Your Business (KYB) Policy of PayNox applies to all corporate clients and legal entities engaging with our financial services. The policy ensures compliance with Bulgarian laws, EU regulations, and international financial crime prevention standards by verifying businesses, their ownership structures, and their activities.

The KYB Policy applies to all corporate clients, legal entities, and business partners engaging with PayNox’s services. It ensures compliance with:

- Bulgarian AML laws (ZMIP)
- EU Anti-Money Laundering Directives (5AMLD & 6AMLD)
- Financial Action Task Force (FATF) Recommendations
- MiCA (Markets in Crypto-Assets) Regulation
- General Data Protection Regulation (GDPR)

This policy is directly linked to PayNox’s Know Your Transaction (KYT) and Risk Policy, ensuring a unified risk management strategy.

This policy covers the identification, verification, and risk assessment of companies, partnerships, trusts, and other legal entities to prevent financial crimes such as money laundering, fraud, terrorist financing, and sanctions violations. It applies to both new and existing clients, with continuous monitoring to detect changes in risk profiles or suspicious activities.

KYB procedures at PayNox extend to Ultimate Beneficial Owners (UBOs), directors, key stakeholders, and associated third parties to ensure transparency and compliance. The policy also includes screening against sanctions lists, adverse media checks, and a risk-based assessment to determine the appropriate level of due diligence required.

Additionally, the KYB policy applies to transactions, counterparties, and business activities conducted through PayNox. High-risk industries, cross-border transactions, and politically exposed persons (PEPs) are subject to Enhanced Due Diligence (EDD) for further scrutiny.

By implementing this policy, PayNox ensures a secure, transparent, and compliant business environment, protecting both the company and its stakeholders from regulatory risks and financial crime exposure.

CORE PRINCIPLES

The Know Your Business (KYB) Policy at PayNox is built upon key principles that ensure transparency, regulatory compliance, and risk mitigation in all business relationships. These principles guide our approach to verifying corporate clients and preventing financial crimes such as money laundering, fraud, terrorist financing, and sanctions violations.

PayNox strictly adheres to Bulgarian national laws, EU directives (AMLD5 & AMLD6), and international financial crime prevention standards. KYB procedures align with regulations such as the Bulgarian Anti-Money Laundering Act (ZMIP) and the Markets in Crypto-Assets (MiCA) Regulation to ensure compliance with evolving legal frameworks.

A risk-based methodology is applied to all corporate clients, assessing them based on factors such as industry type, transaction volumes, geographic exposure, and ownership structures. Higher-risk businesses undergo Enhanced Due Diligence (EDD), including deeper investigations and continuous monitoring.

All corporate clients must disclose their Ultimate Beneficial Owners (UBOs) to prevent hidden ownership structures that facilitate illicit activities. Identity verification, ownership structure analysis, and UBO screening ensure accountability and legitimacy.

PayNox screens all corporate clients, UBOs, and key stakeholders against sanctions lists (EU, UN, OFAC, UK Treasury), politically exposed persons (PEP) databases, and adverse media sources. Any entity linked to illicit activities, financial crimes, or regulatory breaches is flagged for further review.

KYB is not a one-time process; it involves continuous monitoring of corporate clients to detect changes in business activities, ownership structures, or potential compliance risks. Regular reviews and real-time transaction analysis help maintain a compliant business environment.

All KYB records, verification documents, and risk assessments are securely stored in compliance with data protection laws (GDPR and Bulgarian data regulations). Ensuring accuracy and maintaining up-to-date client records is essential for regulatory reporting and audit readiness.

By adhering to these core principles, PayNox strengthens financial security, enhances trust in business relationships, and ensures full compliance with regulatory obligations.

REGULATORY COMPLIANCE

PayNox is committed to maintaining full regulatory compliance with Bulgarian, EU, and international financial crime prevention laws. Our Know Your Business (KYB) Policy aligns with legal frameworks designed to prevent money laundering, terrorist financing, fraud, and sanctions violations.

PayNox operates under the Bulgarian Anti-Money Laundering Act (ZMIP) and complies with EU Anti-Money Laundering Directives (AMLD5 & AMLD6). These regulations establish strict due diligence requirements for verifying corporate clients, identifying Ultimate Beneficial Owners (UBOs), and monitoring financial transactions.

In addition, the company follows the Markets in Crypto-Assets (MiCA) Regulation, which introduces specific compliance standards for crypto-related businesses in the EU, ensuring transparency, consumer protection, and financial stability.

PayNox adheres to global Financial Action Task Force (FATF) recommendations, which set best practices for AML and counter-terrorist financing (CTF) compliance. The company also ensures compliance with Office of Foreign Assets Control (OFAC) sanctions, UN and EU restrictive measures, and other financial crime prevention standards.

KYB procedures at PayNox include verification through official business registries such as the Bulgarian Commercial Register and EU-wide corporate databases. Data privacy and security are also a priority, with full compliance with the General Data Protection Regulation (GDPR) to protect client information.

By enforcing strict regulatory compliance measures, PayNox ensures a secure, transparent, and legally compliant business environment while mitigating financial crime risks.

BUSINESS VERIFICATION PROCESS

The Know Your Business (KYB) Policy at PayNox establishes a thorough business verification process to ensure all corporate clients meet regulatory compliance standards and operate transparently. This process is designed to prevent money laundering, fraud, and financial crime by verifying the legitimacy of companies, their ownership structures, and their financial activities.

1. Collection of Business Information

To verify a corporate client, PayNox collects key information, including:

- Legal entity name and registration number
- Business structure (LLC, JSC, partnership, etc.)
- Registered address and operational locations
- Tax identification number (TIN) and VAT registration
- Nature of business activities and industry classification

2. Verification of Ultimate Beneficial Owners (UBOs)

A critical step in the KYB process is identifying the Ultimate Beneficial Owners (UBOs) who hold 25% or more of the company's shares or have significant control over business decisions. UBO verification includes:

- Collection of official identification documents (passports, national IDs)
- Screening against sanctions lists and politically exposed persons (PEP) databases
- Risk assessment based on ownership structure and financial background

3. Cross-checking with Official Business Registries

PayNox verifies company details through official registries such as:

- Bulgarian Commercial Register (Търговски регистър)
- EU-wide corporate databases
- International business verification platforms

This ensures that businesses are legally registered, active, and compliant with local and EU regulations.

4. Screening for Compliance and Financial Crime Risks

All businesses undergo screening against:

- EU, UN, and OFAC sanctions lists
- Adverse media sources for financial crime-related reports
- Regulatory enforcement actions and fraud alerts

If any red flags are detected, the client may be subject to Enhanced Due Diligence (EDD) for further investigation.

5. Ongoing Monitoring and Periodic Reviews

Verification is not a one-time process. PayNox conducts continuous monitoring to detect changes in ownership, risk profiles, and transaction behaviors. Companies are periodically re-assessed to ensure they remain compliant with evolving regulations.

By implementing this comprehensive business verification process, PayNox ensures a secure, transparent, and compliant business environment, reducing exposure to regulatory risks and financial crimes.

ULTIMATE BENEFICIAL OWNERSHIP (UBO) TRANSPARENCY

In accordance with the Know Your Business (KYB) Policy, PayNox places significant emphasis on Ultimate Beneficial Ownership (UBO) transparency to ensure that all corporate clients operate with a clear and traceable ownership structure. Identifying and verifying UBOs is crucial to preventing financial crimes such as money laundering, tax evasion, and terrorism financing, which often involve complex ownership structures designed to obscure the true individuals in control of a business.

A UBO is the natural person who ultimately owns or controls a legal entity, either directly or indirectly. UBOs are typically those who hold 25% or more of the shares, voting rights, or control the entity through other means. Identifying UBOs allows PayNox to understand who is truly behind a company and assess the potential risks associated with that individual or entity.

Corporate clients must disclose the names of all individuals who hold a significant ownership stake or control the company (e.g., shareholders, members of the board, directors).

The ownership structure is reviewed to ensure that all beneficial owners are identified and no beneficial ownership is hidden behind complex layers of entities.

PayNox requires the submission of official documentation, such as identification cards, passports, and proof of address, for each UBO to confirm their identity.

Documentation must be official and verifiable, such as government-issued ID or valid business documents, and may include records from national company registries and ownership declarations.

UBOs are screened against global sanctions lists, including the OFAC List, EU Sanctions List, and UN Sanctions List, as well as PEP (Politically Exposed Persons) databases.

PayNox also conducts adverse media checks to ensure UBOs are not involved in financial crimes or regulatory violations.

UBO information is continuously monitored to detect any changes in ownership or control.

Periodic reviews are conducted to ensure that the UBO information remains up-to-date and accurate.

In cases where the ownership structure appears complex or high-risk (e.g., UBOs located in high-risk jurisdictions or involved in high-risk industries), PayNox applies Enhanced Due Diligence (EDD) measures.

This includes more in-depth checks, such as further investigation into the source of funds and the business background of the UBOs.

UBO transparency is mandated by both Bulgarian and EU legislation, including:

Bulgarian Anti-Money Laundering Act (ZMIP)

EU Anti-Money Laundering Directives (AMLD5 & AMLD6)

These regulations aim to enhance transparency in corporate ownership structures and facilitate the detection of illicit financial flows.

By enforcing UBO transparency, PayNox ensures it only conducts business with legitimate and fully accountable corporate clients. This practice minimizes the risk of exposure to financial crimes and protects the company's reputation, while ensuring compliance with local and international regulations.

SANCTIONS AND ADVERSE MEDIA SCREENING

At PayNox, Sanctions and Adverse Media Screening are critical components of the Know Your Business (KYB) Policy. These measures help ensure that the company does not engage in business relationships with entities or individuals involved in illegal, unethical, or high-risk activities. Screening against sanctions lists and adverse media sources is vital for preventing financial crimes, complying with international regulations, and maintaining a compliant, secure environment.

Sanctions screening refers to the process of checking corporate clients, their Ultimate Beneficial Owners (UBOs), directors, and key stakeholders against international sanctions lists to ensure that PayNox Bulgaria is not inadvertently conducting business with individuals or entities subject to restrictions or bans.

The main sanctions lists used include:

- OFAC (Office of Foreign Assets Control) – U.S. sanctions
- EU Sanctions List – Sanctions imposed by the European Union
- UN Sanctions List – United Nations sanctions
- UK Sanctions List – Sanctions imposed by the UK government

These lists contain entities and individuals who may be involved in activities such as terrorism, money laundering, or human rights violations. By screening against these lists, PayNox ensures that it does not engage with sanctioned individuals or entities, thus avoiding legal and reputational risks.

In addition to sanctions lists, PayNox conducts thorough adverse media screening to identify any news or reports linking a business or individual to illegal or unethical activities. Adverse media refers to negative information found in credible news sources, including:

- Reports on financial crimes (e.g., money laundering, fraud, tax evasion)
- Allegations of corruption, bribery, or fraud
- Environmental violations or unethical business practices
- Legal actions or sanctions imposed by authorities

PayNox utilizes advanced search tools to access global databases of news articles, social media, and other public sources to identify and assess potential reputational and legal risks associated with a client. The goal is to identify clients that could present elevated risks due to their association with negative press, criminal activities, or other problematic behaviors.

PayNox regularly screens clients, UBOs, and related individuals against sanctions lists. If a match is found, the transaction or business relationship is halted and subjected to a further investigation.

PayNox adheres to strict blocking and reporting obligations in case of a confirmed match with a sanctioned individual or entity.

PayNox uses specialized software to search for adverse media mentions, such as news articles, legal actions, and public reports.

This information is cross-referenced with the client’s identity and business activities to determine whether there are any potential risks or violations.

If adverse media or sanctions screening reveals concerning results, PayNox escalates the matter for Enhanced Due Diligence (EDD). This involves a deeper investigation into the client's background, ownership structure, and any related issues.

The client may be asked to provide additional documentation or clarification, and transactions involving such clients are closely monitored.

PayNox Bulgaria's sanctions and adverse media screening processes are compliant with national and international regulations, including:

- Bulgarian Anti-Money Laundering Act (ZMIP)
- EU Anti-Money Laundering Directives (AMLD5 & AMLD6)

By implementing these measures, PayNox ensures it adheres to compliance obligations while maintaining a clean and transparent business network.

Sanctions and adverse media screening is an ongoing process. PayNox continuously monitors the status of its clients and updates its screening systems to ensure that new sanctions or adverse media reports are identified promptly. Clients may be re-screened periodically or whenever significant changes in the business relationship occur.

No Match: If no match is found, the client proceeds as normal through the KYB process.

Potential Match: If there is a potential match, PayNox initiates an investigation to confirm the identity and nature of the match.

Confirmed Match: If a confirmed match with a sanctioned entity or individual is found, the business relationship is terminated, and a report is filed with the appropriate authorities.

By enforcing sanctions and adverse media screening, PayNox Bulgaria protects its operations, reputation, and regulatory standing, while contributing to global efforts in combating financial crimes and maintaining a compliant, ethical business environment.

RISK-BASED ASSESSMENT

The Risk-Based Assessment (RBA) approach is a fundamental part of PayNox's Know Your Business (KYB) policy. This methodology ensures that compliance efforts are proportionate to the risks associated with each corporate client. By applying a risk-based approach, PayNox can efficiently allocate resources to high-risk clients while ensuring a smooth and compliant onboarding process for low-risk businesses.

The RBA is guided by international compliance standards, including the Financial Action Task Force (FATF) Recommendations, EU Anti-Money Laundering Directives

(AMLD5 & AMLD6), and Bulgarian AML legislation (ZMIP). This approach enables PayNox to:

- Identify high-risk clients and apply Enhanced Due Diligence (EDD) where necessary.
- Streamline onboarding for low-risk businesses with simplified due diligence.
- Continuously monitor clients to detect changes in risk levels over time.

PayNox follows a Risk-Based Approach (RBA), classifying clients into low, medium, and high-risk categories based on:

- Industry type (e.g., fintech, gambling, crypto exchanges = high risk)
- Geographic risk (FATF Grey and Black Lists jurisdictions)
- Ownership transparency (complex structures = high risk)
- Transaction behavior (unusual volumes = EDD required)

All corporate clients undergo automated LexisNexis, Refinitiv, and ComplyAdvantage screenings for sanctions, PEP exposure, and negative media.Businesses in sectors prone to money laundering, fraud, or regulatory scrutiny (e.g., cryptocurrency exchanges, gambling, remittance services) are classified as high-risk.

Low-risk industries typically include regulated financial institutions and traditional commerce businesses.

Clients operating in or linked to high-risk jurisdictions, including those identified by the FATF Grey List or Blacklist, receive increased scrutiny.

Countries with strong AML/CFT regulations and transparent financial systems pose a lower risk.

Companies with complex ownership structures, offshore entities, or anonymous shareholders may pose higher risks.

Businesses with clear, well-documented ownership are considered lower risk.

Unusual transaction patterns, high-value cross-border transfers, and frequent large deposits may indicate potential financial crime risks.

Stable, predictable transaction flows aligned with the nature of the business reduce risk.

Businesses with a history of non-compliance, sanctions, or legal violations are classified as high-risk.

Companies with a clean compliance record and positive regulatory standing are lower risk.

Based on these risk factors, PayNox classifies corporate clients into three primary categories:

Low-Risk Clients: Standard Customer Due Diligence (CDD) applies, with basic verification of business details and ownership.

Medium-Risk Clients: Additional scrutiny, including deeper ownership verification and periodic reviews, is required.

High-Risk Clients: Enhanced Due Diligence (EDD) is applied, involving detailed background checks, source of funds verification, and ongoing transaction monitoring.

Risk assessments are not static. PayNox implements continuous monitoring to detect risk changes based on transaction behaviors, regulatory updates, or changes in ownership structure. Clients may be reclassified if new risks emerge, ensuring compliance remains adaptive and effective.

By adopting a Risk-Based Assessment approach, PayNox Bulgaria enhances its ability to detect, prevent, and mitigate financial crime risks while maintaining a seamless and compliant business operation.

ENHANCED DUE DILIGENCE (EDD)

Enhanced Due Diligence (EDD) is a critical process under PayNox's Know Your Business (KYB) Policy, designed to assess and mitigate higher risks associated with certain corporate clients. EDD is employed for clients or business relationships that are considered higher risk based on a risk-based assessment (RBA). The purpose of EDD is to gather a more comprehensive understanding of a business's structure, operations, financial activities, and background to identify potential risks such as money laundering, terrorism financing, and fraud.

EDD is applied in situations where a client is deemed to have a higher risk profile due to one or more of the following factors:

Jurisdictional Risks: If the business or its key stakeholders are located in or linked to countries with weak regulatory frameworks, high corruption, or those under sanctions (FATF High-Risk or Non-Cooperative jurisdictions).

Industry Risks: If the business is operating in high-risk sectors like cryptocurrency exchanges, online gaming, or gambling, which are more susceptible to financial crimes.

Complex Ownership or Structure: If a business has a complex ownership structure, with multiple layers of entities or offshore connections that obscure the identity of Ultimate Beneficial Owners (UBOs).

Negative Media Reports or Sanctions: If adverse media or sanctions lists indicate any historical association with criminal activities, fraud, or regulatory violations.

Unusual Transaction Patterns: If the company exhibits irregular transaction behavior or large, unexplained financial transfers, especially across borders.

The core objective of EDD is to ensure that PayNox Bulgaria gains a deep, nuanced understanding of the client's business, its ownership structure, and the sources of its funds. EDD involves the following comprehensive steps:

PayNox ensures that the business's identity, ownership, and structure are fully documented. This often includes:

In-depth verification of UBOs (Ultimate Beneficial Owners): Identifying the individuals who ultimately own or control the business, especially in cases where ownership structures are complex or involve multiple layers of entities.

Obtaining valid and up-to-date documentation, such as:

- Articles of Incorporation, business licenses, and proof of operations.
- Shareholder registers and organizational charts.
- Corporate tax returns or financial statements.

Source of Funds (SoF) and Source of Wealth (SoW) Investigation

A key part of EDD is ensuring that PayNox has a clear understanding of the business's source of funds and the overall source of wealth:

Source of Funds: How funds are being used in the business transactions (e.g., operational revenue, investments, loans).

Source of Wealth: The overall origin of the business's wealth and capital, whether from entrepreneurial activities, investments, or previous savings.

PayNox conducts additional screening to search for any negative media coverage, involvement in legal disputes, or associations with sanctioned entities or individuals. This step helps to flag any potential reputational risks or legal exposure the business may carry.

Using both traditional media outlets and online platforms, PayNox checks for any news articles, press releases, or reports linking the business to criminal or unethical behavior.

During EDD, PayNox verifies that the business's operations align with the documentation provided and that the nature of the activities is consistent with the client's stated objectives and expected financial transactions. This step may include:

Confirming the legitimacy of business activities: Verifying the existence of the business and its operations, including checking with local regulators or industry associations.

Understanding the transaction flow: Assessing whether the volume, frequency, and type of transactions are in line with the company's operations.

EDD does not end at the onboarding stage. PayNox establishes a process for ongoing monitoring to detect any changes in the client's risk profile or suspicious activity. This includes periodic re-assessment of:

Transaction patterns: Continued monitoring of the business's transactions for any signs of irregular activity, such as sudden increases in volume or large international transfers.

Changes in ownership or control: If a business changes its UBOs or ownership structure, PayNox ensures that updated information is obtained and assessed for any associated risks.

Once the EDD process is completed, PayNox determines the risk level of the client and decides on the appropriate actions:

Low to Medium Risk: If no further risks are identified after EDD, the business may be approved for continued engagement under standard monitoring procedures.

High Risk: If the investigation raises red flags, PayNox may terminate the relationship, refuse to proceed with certain transactions, or subject the client to heightened scrutiny and ongoing monitoring.

Suspicious Activity: If evidence of money laundering, terrorism financing, or other illicit activities is found, the appropriate authorities are notified, and the relationship is immediately terminated.

EDD is crucial for PayNox's AML (Anti-Money Laundering) and CTF (Counter-Terrorism Financing) efforts. It helps to:

Mitigate financial crime risks and prevent illegal activity by thoroughly assessing high-risk clients.

Maintain regulatory compliance, especially in jurisdictions with stringent AML and KYC requirements.

Protect PayNox's reputation and ensure that it is not inadvertently facilitating criminal or unethical activity.

By performing comprehensive Enhanced Due Diligence, PayNox ensures that it is working with businesses that meet all legal, regulatory, and ethical standards, while also protecting itself from risks associated with criminal enterprises or reputational damage.

ONGOING MONITORING & COMPLIANCE

Ongoing Monitoring is a cornerstone of PayNox's Know Your Business (KYB) policy. This process ensures that PayNox remains vigilant in detecting potential risks throughout the lifecycle of its business relationships. Continuous monitoring not only helps to ensure compliance with Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) regulations but also mitigates emerging risks from evolving business activities, new jurisdictions, or changes in ownership.

In the context of KYB, ongoing monitoring refers to the systematic, continuous process of assessing the behavior and status of corporate clients and their transactions. It is designed to:

- Detect suspicious activity in real-time or near-real-time to prevent illicit activities such as money laundering, fraud, and financing of terrorism.
- Adapt to changing risk profiles by ensuring that PayNox remains aware of any significant alterations to a client's operations, ownership, or financial behaviors.
- Ensure continued regulatory compliance by aligning with international standards and ensuring adherence to local laws.

Ongoing monitoring is an essential compliance obligation for businesses like PayNox to comply with regulations such as AML Directives in the EU, local AML laws in Bulgaria, and international standards from the FATF (Financial Action Task Force).

PayNox actively monitors the transactions made by its corporate clients to identify any irregular or suspicious activity. This includes:

- Real-time analysis of transaction patterns to detect anomalies (e.g., unusually large transactions, rapid fund transfers, or inconsistent activity compared to expected behavior).
- Monitoring for cross-border transactions, especially if linked to high-risk countries or jurisdictions under sanctions or with weak AML frameworks.
- Assessing transaction volumes and comparing them to historical patterns to detect sudden spikes that may signal illicit activity.

Clients are re-assessed periodically, and risk factors such as industry, jurisdiction, ownership structure, and transaction behavior are reviewed:

- If there are significant changes in the business, such as a change in the Ultimate Beneficial Ownership (UBO), new market operations, or new sources of funds, these are evaluated.
- A risk score is updated regularly based on the business's activities and any external factors (e.g., changes in international law, media reports, or sanctions updates).

PayNox performs regular screening for negative media reports and sanctions updates. This involves:

- Automated screening tools to search for mentions of the client in news outlets, regulatory announcements, or social media platforms.
- Cross-checking clients against sanctions lists, including those maintained by the EU, UN, and OFAC, to ensure they are not engaged in activities prohibited by law.

Reviewing any adverse news related to corruption, fraud, or criminal investigations.

Even after the onboarding process, PayNox conducts periodic reviews of existing clients to ensure:

Updated information on clients, including UBO details, financial status, and business activities.

Periodic documentation checks, such as reviewing tax filings, corporate structure, and proof of operations.

Monitoring to verify that the nature of business activities remains consistent with the original assessment and that there are no signs of deviations indicating higher risks.

Suspicious Activity Detection and Escalation

The system is designed to detect suspicious activity that might indicate illegal activities, such as money laundering or terrorist financing. If suspicious activity is flagged:

The activity is escalated for further investigation by the compliance team or internal monitoring staff.

If the suspicion is confirmed, PayNox will report the activity to the relevant authorities, including the Financial Intelligence Unit (FIU) in Bulgaria, in line with AML obligations.

If the client's activities raise significant concerns, the business relationship may be terminated, or further EDD (Enhanced Due Diligence) may be applied.

Compliance staff and relevant personnel undergo regular training on monitoring processes, regulatory updates, and how to detect suspicious activities. This ensures that all team members are well-equipped to identify potential issues and escalate them appropriately.

PayNox uses automated tools to assist in real-time monitoring and analysis. These systems are integrated with internal databases and external sources, such as sanctions lists and media monitoring tools. The use of technology ensures greater accuracy and efficiency in detecting anomalies and potential risks.

Timely detection of illicit activity that could undermine the integrity of its services or lead to financial or reputational damage.

Adaptation to changing risks in real time by adjusting to fluctuations in the client's behavior, operations, or external factors (e.g., a new regulatory landscape or sanctions imposition).

Regulatory compliance, which helps avoid penalties or legal consequences that could arise from non-compliance with AML and CTF laws.

PayNox's ongoing monitoring procedures are aligned with international and national laws, including:

- EU Anti-Money Laundering Directives (AMLD), which require ongoing due diligence and monitoring for all regulated entities.
- FATF Recommendations on the need for ongoing monitoring to ensure that businesses effectively prevent financial crime and maintain compliance.
- Bulgarian ZMIP (Anti-Money Laundering Act), mandates businesses to implement ongoing surveillance systems and periodically reassess client risk profiles.

Ongoing monitoring is a proactive and continuous process that ensures PayNox stays ahead of potential risks and maintains a compliant, transparent relationship with its corporate clients. It allows PayNox to effectively identify suspicious activity, ensure up-to-date client information, and respond to regulatory changes. By maintaining robust and dynamic monitoring systems, PayNox can ensure the integrity of its operations, protect itself from financial crime, and uphold its reputation as a trusted partner in the financial services industry.

RECORDKEEPING & REPORTING

Recordkeeping and Reporting are critical components of PayNox's Know Your Business (KYB) policy, ensuring that the company remains compliant with regulatory requirements and is prepared to respond to any scrutiny from authorities or audits. These processes help maintain transparency, traceability, and accountability for all client-related activities, mitigating the risks of non-compliance and fraud.

PayNox maintains comprehensive and accurate records for each corporate client to facilitate effective monitoring and regulatory compliance. The key documents and information that must be kept include:

- Business Identification Documents: Including corporate registration details, proof of operations, and ownership structure.

- Know Your Business (KYB) Documentation: The full scope of the client's due diligence file, including information about the Ultimate Beneficial Owner (UBO), shareholders, and directors.
- Transaction Records: Detailed information about inbound and outbound transactions, including amounts, sources, counterparties, dates, and purposes. This is crucial for the detection and investigation of suspicious transactions.
- Communication Logs: Copies of correspondence and other relevant interactions with the client, ensuring transparency throughout the client relationship.
- Screening and Monitoring Reports: Detailed records of ongoing monitoring efforts, including regular risk assessments, adverse media findings, and sanctions screening results.

All client records and transaction data must be kept for a minimum of five years after the end of the business relationship or after the date of the last transaction, in accordance with local and international regulatory requirements, including the EU Anti-Money Laundering Directives (AMLD) and Bulgarian Anti-Money Laundering Act (ZMIP). This allows PayNox to:

- Respond to inquiries or audits from regulatory authorities.
- Retain the necessary documentation for investigating suspicious activities or transactions.
- Ensure compliance with statutory retention periods under local laws and international standards.

PayNox uses secure systems to store all records, including digital and paper files. These systems ensure that records are:

- Protected from unauthorized access, alteration, or destruction.
- Easily retrievable in case of audits or regulatory inspections.
- Backed up and archived to prevent data loss, with strong encryption protocols and secure access control.

All client records are handled with the utmost confidentiality, in line with data protection laws such as the General Data Protection Regulation (GDPR) in the EU and relevant Bulgarian data privacy regulations. PayNox ensures that personal and business-sensitive information is:

- Processed in compliance with GDPR principles, including data minimization, purpose limitation, and ensuring that data is used only for legitimate purposes.
- Disclosed only to authorized personnel within PayNox or to regulatory authorities, where required by law.

If PayNox detects any suspicious activity during the course of its client monitoring, including unusual transactions or discrepancies in transaction patterns, it is required to file a Suspicious Transaction Report (STR) with the relevant regulatory body or Financial Intelligence Unit (FIU).

Triggers for STR: This may include large, complex, or unusual transactions, or activities involving high-risk jurisdictions, politically exposed persons (PEPs), or transactions inconsistent with the client's business profile.

The STR must include a detailed account of the suspicious activity, the client's identity, and the potential reasons why the transaction is deemed suspicious. This helps authorities assess whether the activity is connected to money laundering, terrorism financing, or other illicit activities.

In cases where a client or a transaction is found to be linked to sanctioned entities or individuals, PayNox must ensure that the appropriate regulatory authorities are notified and that the relevant actions are taken, including:

- Freezing the assets or suspending the transactions of sanctioned individuals or entities.
- Reporting these actions to the relevant regulatory authority, such as the Bulgarian National Bank (BNB) or EU sanctions bodies.

PayNox also ensures that it provides regular compliance reports to its internal governance bodies, senior management, and regulatory authorities. These reports typically include:

- A summary of the risk assessment and monitoring activities.
- Records of any reported suspicious activity or incidents.
- Documentation of client due diligence (CDD) and enhanced due diligence (EDD) efforts.
- Updates on any regulatory changes and how the company is ensuring compliance with them.

As part of its ongoing obligations under AML regulations and KYC (Know Your Customer) and KYB laws, PayNox is required to submit regular reports to regulatory authorities, including:

Annual reports on compliance with AML and KYC regulations, including details of the company’s internal controls, monitoring procedures, and training activities.

Ad hoc reports in response to specific requests from regulators, such as updates on particular clients or transactions, especially in cases of high scrutiny or investigation.

In addition to external reporting requirements, PayNox has an internal compliance reporting mechanism that allows employees to report:

- Any issues or concerns regarding the effectiveness of the KYB or compliance processes.
- Potential breaches of regulatory requirements or internal policies.
- Red flags or suspicious activities that may not yet have been flagged by automated monitoring tools.

Internal and external audits are conducted regularly to ensure that PayNox's KYB and compliance measures remain effective. The findings of these audits are reported to the Board of Directors, senior management, and relevant stakeholders, with recommendations for improvements or corrective actions where needed.

PayNox's recordkeeping and reporting practices are in line with local and international regulations, such as:

- EU Anti-Money Laundering Directives (AMLD), which require businesses to maintain accurate records and report suspicious transactions.
- Bulgarian Anti-Money Laundering Act (ZMIP), which mandates the retention of records for at least five years.
- FATF (Financial Action Task Force) Recommendations, which set global standards for record retention and suspicious transaction reporting.

Recordkeeping and reporting are vital components of PayNox's KYB policy to ensure compliance with legal and regulatory requirements and to maintain a secure and transparent environment for corporate clients. These activities not only help mitigate the risks associated with financial crime but also ensure that PayNox can respond effectively to regulatory inquiries, audits, and suspicious activity investigations. By maintaining accurate, comprehensive records and fulfilling its reporting obligations, PayNox upholds its reputation as a trusted financial partner and ensures the integrity of its operations.

POLICY UPDATES AND COMPLIANCE REVIEW

To maintain regulatory alignment, this policy is reviewed and updated regularly:

- Quarterly Internal Compliance Reviews
- Annual External Audits for EU AMLD, FATF, and GDPR compliance
- Immediate updates when new AML laws or FATF sanctions are introduced

Any updates are communicated to employees and compliance teams via structured training sessions.

INTEGRATION WITH KYT & RISK POLICY

PayNox ensures a cohesive compliance framework by integrating KYB with:

- Know Your Transaction (KYT) Policy: Monitoring business transactions for suspicious activities
- Risk Policy: Aligning KYB risk categorization with transaction monitoring and due diligence procedures

This integration ensures a holistic approach to risk assessment, regulatory adherence, and financial crime prevention.

COMPLIANCE & CONTINUOUS IMPROVEMENT

Compliance and continuous improvement are fundamental to ensuring that PayNox Bulgaria maintains the highest regulatory standards in its Know Your Business (KYB) procedures. By continuously enhancing compliance measures and adapting to evolving legal requirements, industry best practices, and emerging risks, PayNox fosters a secure and transparent business environment.

PayNox adheres to both local and international regulations, ensuring that its KYB processes align with Anti-Money Laundering (AML) laws, Counter-Terrorism Financing (CTF) regulations, data protection rules, and financial crime prevention standards. The company remains committed to full compliance with:

- European Union Anti-Money Laundering Directives (AMLDs)
- Bulgarian Anti-Money Laundering Act (ZMIP)
- Financial Action Task Force (FATF) Recommendations
- General Data Protection Regulation (GDPR)
- Sanctions compliance requirements, including EU, UN, and OFAC sanction lists

By integrating these regulatory requirements into its KYB framework, PayNox ensures that all corporate clients are properly vetted, reducing risks related to money laundering, fraud, and other illicit financial activities.

To ensure that compliance measures remain effective, PayNox employs continuous monitoring of its KYB processes. This includes:

Ongoing Risk Assessments: Regularly evaluating clients' business activities, ownership structures, and financial behavior to detect any changes that may pose heightened risks.

Periodic Review of Client Information: Ensuring that corporate clients’ data, including Ultimate Beneficial Owner (UBO) details, business activities, and risk classifications, are updated as required by regulations.

Monitoring for Adverse Media and Sanctions: Conducting frequent screenings of corporate clients against sanctions lists, watchlists, and adverse media reports to detect potential risks.

Transaction Behavior Analysis: Identifying unusual transaction patterns that may indicate suspicious activity, fraud, or non-compliance.

These monitoring efforts help PayNox proactively identify, mitigate, and respond to compliance risks before they escalate into regulatory violations or reputational damage.

A strong compliance culture is upheld through regular training and awareness programs for PayNox employees. This ensures that all team members understand the importance of KYB, AML, and CTF obligations, as well as how to apply compliance policies effectively in their daily work.

Employees receive mandatory compliance training upon onboarding and periodic refresher courses.

Specialized training sessions focus on detecting financial crime risks, handling suspicious transactions, and implementing Enhanced Due Diligence (EDD) measures.

Senior management and compliance officers engage in ongoing professional development to stay informed about regulatory updates and industry trends.

By continuously educating employees, PayNox enhances its ability to prevent regulatory breaches and effectively manage compliance risks.

To remain compliant with regulatory changes and best practices, PayNox regularly reviews and updates its KYB policies, procedures, and controls. This includes:

Annual Compliance Audits: Internal and external audits assess whether KYB processes are operating effectively and in accordance with applicable laws.

Policy Adjustments Based on Regulatory Changes: Updates to KYB procedures occur when new AML or financial crime laws are introduced at the EU or Bulgarian national level.

Leveraging Technology for Compliance Improvement: Implementing new compliance tools, automation, and AI-driven solutions to enhance screening, risk assessments, and fraud detection.

By adapting KYB policies and procedures to align with evolving regulatory landscapes, PayNox ensures that its compliance framework remains robust, effective, and future-proof.

PayNox actively collaborates with regulators, financial authorities, and industry stakeholders to ensure that its compliance framework aligns with global best practices. This includes:

Participating in AML and compliance forums to stay informed about emerging risks.

Engaging with regulatory bodies to ensure adherence to Bulgarian and EU financial crime prevention requirements.

Cooperating with law enforcement agencies and financial institutions to strengthen financial transparency and crime prevention.

By maintaining open communication with regulatory bodies and industry experts, PayNox strengthens its compliance standards and enhances its ability to detect and prevent financial crimes.

Continuous improvement in KYB compliance is essential for maintaining regulatory integrity, protecting PayNox from financial crime risks, and ensuring long-term business sustainability. Through rigorous monitoring, ongoing training, policy enhancements, and industry collaboration, PayNox remains at the forefront of corporate compliance and risk management.

CONCLUSIONS

The Know Your Business (KYB) policy of PayNox is designed to ensure regulatory compliance, risk management, and business transparency while fostering trust and security in financial transactions. By implementing a robust KYB framework, PayNox can effectively verify corporate clients, assess financial risks, and prevent illicit activities such as money laundering, fraud, and sanctions violations.

A risk-based approach remains at the core of PayNox's KYB policy, allowing the company to apply Enhanced Due Diligence (EDD) where necessary, ensuring that high-risk entities undergo thorough scrutiny. Through ongoing monitoring, compliance audits, and regulatory adherence, PayNox continuously improves its processes to align with Bulgarian, EU, and global financial crime prevention standards.

By integrating technology-driven compliance solutions, PayNox enhances the efficiency of business verification, UBO transparency, transaction monitoring, and sanctions screening. In addition, regular training and awareness programs for employees reinforce a strong compliance culture, ensuring that staff members remain informed about evolving risks and regulatory obligations.

As regulations and financial crime risks evolve, PayNox remains committed to adapting and strengthening its KYB framework, ensuring proactive risk management and legal compliance. By maintaining transparency, accountability, and a commitment to continuous improvement, PayNox safeguards its operations and fosters a secure financial ecosystem for its corporate clients.

PayNox maintains a robust KYB framework that integrates AML, CTF, and blockchain analytics. Through continuous monitoring, enhanced verification processes, and a dynamic compliance strategy, PayNox ensures regulatory compliance, financial security, and operational resilience.

This policy is reviewed quarterly and updated as necessary to reflect regulatory changes and emerging risks in business verification and financial crime prevention.