# Anti-Money Laundering Policy

June 2023

**To our users,**
**At bunq, we believe in transparency and having an inside=outside approach to our policies and procedures. We want to be fully transparent with our users and inform them of anything you may want to know. For this reason, we aim to make our policies publicly available, where we (legally) can!**

bunq

BANK OF THE FREE

# Table of Contents

## Summary 📜

This policy contains bunq’s approach to financial crime, and particularly money laundering and terrorist financing. It outlines: who are the responsible parties, our risk appetite, how we classify risk, our onboarding process, the preventative measures against money laundering and terrorist financing implemented by bunq.

# 1 Introduction 📓

To ensure compliance with anti-money laundering (AML) and counter-terrorist financing (CTF) laws and regulations, bunq B.V. has developed and implemented extensive measures such as policies, procedures, internal controls and systems.

This policy outlines bunq's application of relevant laws and regulations relating to anti-money laundering and terrorism financing, specifically the 5th European AML directive (Directive (EU) 2018/843) and the Dutch Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). This policy has supporting procedural documents which describe the implementation of this policy.

This policy applies to all bunq departments and staff, including branches. Subsidiaries can have their own risk management arrangements and are outside the scope of this policy. However, risk oversight of the subsidiaries by (employees of) bunq is in the scope of this policy. This policy can be complemented by annexes for local branches or subsidiaries describing the local laws and regulations where they differ from that described in this policy.

# 2 Roles and Governance 🏢

Anti-money laundering (AML) safeguards are guided by a number of people, departments and processes within bunq. This section will list the roles and responsibilities of different parties in bunq in relation to AML. Furthermore, the governance structure behind AML efforts will be described by listing the available tools.

**Roles**

- **Managing Board**
    - The Managing Board is responsible for setting, approving, and overseeing bunq's overall AML policy and for ensuring sound business practices.
- **Chief Risk Officer**
    - Within the managing board, the Chief Risk Officer (CRO) is the board member responsible for the second line of defense.
- **Chief Information Officer**
    - Within the Managing Board, the Chief Information Officer (CIO) is responsible for the first line of defense; including Compliance Operations, Onboarding, and Support.
- **Head of Compliance**
    - The Head of Compliance plays an active role in identifying potential integrity risks, such as risks associated with money laundering and terrorism financing. The Chief Risk Officer may assign them the responsibility of maintaining the Systematic Integrity Risk Analysis.

- **Compliance Officers**
    - The Promise Keeper - Regulatory Compliance / Financial Crime is a Compliance Officer who is responsible for identifying regulatory obligations with regards to AML/CFT, translating these obligations into policies and monitoring execution by the first line of defense. They report to the Head of Compliance.
- **Onboarding team**
    - The onboarding team is responsible for onboarding new users in line with this policy and the related procedural documents.
- **Compliance Operations team**
    - The compliance Operations team is responsible for the ongoing monitoring and investigation of users in line with this policy and the related procedural documents.

**Governance**

- **Policies and procedures**
    - This Policy needs to be reviewed at least annually and requires the approval of the Management Board unless changes are non-material that can be approved by the CRO.
    - Procedures listed in Annex I need to be reviewed at least annually and require the approval of the CRO, they have the status of the key procedures as they are defined in the Policy of Policies**.**
    - bunq's Policy of Policies contains more details about approval authorities and periodic review requirements for policies and (key as well as non-key) procedures.
- **Risk scoring models and machine learning**
    - Material changes to the onboarding and dynamic risk scoring models and machine learning require the approval of the CRO.
    - Changes in country and industry/sector risk ratings require the approval of the CRO.
    - Non-material changes to the onboarding and dynamic risk scoring models and machine learning may be approved by the Head of Compliance Operations.
- **Peer Group and Source of Funds threshold models**
    - Changes to the peer group and source of funds threshold models require the approval of the CRO.
- **Transaction filtering and monitoring rules**
    - Implementation of new transaction monitoring rules and material changes to the existing rules require the approval of the Head of Compliance Operations or in his/her absence the approval of the Head of Operations.

- **Acceptance of users**
    - New users falling in the scope of our Acceptance Policy, which is bunq's guideline for what users we onboard and which we don't onboard, are approved by the Onboarding except for crypto companies, Politically Exposed Persons, and their Relatives and Close Associates, which all need to be approved by the Chief Risk Officer.
    - Deviations from the Acceptance Policy require the approval of the Chief Risk Officer (CRO) or any other senior employee authorized by the CRO.
    - Auto-deny rules need to be approved by the Head of Step 3 and CRO to ensure fair treatment of users.
- **Offboarding of users**
    - Offboarding decisions within the Offboarding Procedure are made by the Compliance Operations team.
    - Deviations from the Offboarding Procedure require the approval of the CRO or a senior officer assigned by the CRO.
- **FIU reporting and blocking user transactions/accounts**
    - Decisions to report users to the FIU (and respective reporting) and block their funds are made by the Compliance Operations, but respective requests can also come from the Promise Keeper - Regulatory Compliance / Financial Crime, Head of Compliance or the CRO. For more information on what these position mean please refer to the Risk Management policy.
- **Retool (Onboarding and Compliance Operations database)**
    - Changes need to be approved by the Head of Compliance Operations / Head of Onboarding (depending on the scope) and removal of information fields from Retool that are related to controls executed by agents and described in procedures from Annex I require CRO approval or a senior officer assigned by the CRO.

## 3 Risk appetite 🍽️

bunq's risk appetite is how much risk bunq is willing to accept. The risk appetite is reflected in our Risk Appetite Statement, which is a document explaining how much risk we are willing to take in different fields. With regard to risks related to money laundering and terrorism financing, these are the most relevant considerations for setting the appetite:

- No appetite for non-compliance with rules and regulations, including rules and regulations related to anti-money laundering and terrorism financing;
- No appetite to accept users (persons or company) if there are strong signs that they are inclined to violate bunq's terms and conditions and/or use bunq's services for illegal activities,
    - We will start an investigation as soon as there are signals on such activity;

- bunq reserves the right to review a relation of a user at any time; and
- bunq has no appetite to service users who are (suspected of) misusing our services longer than legally required.

## 4 Acceptance policy 🚪

bunq has no appetite to accept a person or company as a user if there are strong indications that the person or company may be inclined to violate its terms and conditions and/or use its services for illegal activities. This risk appetite statement has been translated into bunq's Acceptance Policy which lists the groups/types of users that we service.

## 5 Systematic Integrity Risk Analysis 🖊️

The Systematic Integrity Risk Analyses (SIRA) is an analysis of potential integrity risks and it is central to bunq's efforts to prevent money laundering and terrorist financing.

Integrity risks are defined by the regulation as a threat to the reputation, the capital or the results of a financial institution due to insufficient compliance with the rules that are in force under or pursuant to the law." In our internal SIRA, we map this definition to our risk taxonomy which we refer to as Eva's Wish List. You can take a look at this List in our Risk Management Policy.

The Systematic Integrity Risk Analysis (SIRA) answers the following questions:

- Which integrity risks does bunq face?
- Which (level of) risk are we willing to accept?
- How do we manage the integrity risks?

Based on the SIRA process, integrity risks are (i) identified, (ii) analyzed, (iii) managed (mitigated) and (iv) monitored.

The analysis is maintained and reviewed by multiple groups:

- Chief Risk Officer (CRO): has the ultimate responsibility to maintain the SIRA and delegates the development of it to the Head of Compliance..
- The First line of defense (this line of defense is in direct connection with the users and the company's business objectives): manages (and mitigates) the identified risks.
- Managing board: as mentioned above, the CRO holds the ultimate responsibility for integrity risk analysis within the Managing Board.
- Supervisory board: discusses SIRA at least once a year and approves it.

This SIRA will be updated at least once a year and in case one of the following events occurs:

- when a new geographical market is entered into;
- when a new product or service is launched;

- when a material change to an existing product or service is implemented;
- when our acceptance policy and/or risk appetite changes; and
- when a new integrity risk is identified; and
- when significant control deficiencies are identified e.g. from risk incidents, KPI breaches, risk assessment, control testing activities or audits.

Relevant stakeholders have a monthly meeting to discuss whether one of the above mentioned events will occur in the foreseeable future or has occurred in the past period, and to update the SIRA accordingly.

Every quarter the CRO provides an updated integrity risk assessment in an aggregated manner (at the Risk Driver level of the Eva Wish List, i.e. Level 3 of bunq risk taxonomy) to the Risk and Audit Committee of the Supervisory Board. The report is provided in the form of a Risk Heat Map with highlights followed by detailed updates from Risk and Compliance departments.

## 6 Risk Classification ⚖️

In accordance with article 3 sub 8 of the Wwft, we adjust the customer's due diligence measures based on the risk level of the customer. We follow this legal requirement by using these risk models:

1. **Onboarding risk-scoring models**
    a. A scoring model for each new user based on the information gathered during the onboarding process (before account opening).
2. **Dynamic risk scoring models**
    a. These models keep the risk score of each user up to date during their relationship with bunq (after account opening).

Thus, there are 4 models in total, each with two versions (personal user and company user).

The models take into account (if relevant):

- Risk factors that are mentioned in annexes to EU 5th AML Directive 2018/843.
- Analysis of historical data
- User’s country and industry/sector risk ratings

Risk scores are classified into low, medium, high, and reject (rejected = no account will be opened). Risk classification is used for these procedures/processes:

- **Onboarding**
    - The risk score of a user is an important factor in the onboarding process and plays a role in whether or not we accept a user. Industry/sector risk rating also

influences whether a user company can be onboarded automatically or a manual check is required.

- **Monitoring**
    - We use the risk score as an input in our transaction monitoring system and we apply different, more stringent, monitoring thresholds to higher-risk users. As a consequence, users with a higher risk classification are more likely to create a hit and are thus more likely to be reviewed than users with a lower score.
- **User reviews/investigations**
    - Our analysts take a user’s risk score as a starting point when they review or investigate a user. The higher the score, the more careful the analysts are with assessing the user.
- **Periodic reviews**
    - The risk score of a user is a key factor in determining how often a user gets periodically reviewed.

## 7 Onboarding 🛳️

**Persons**

Onboarding is the process all users need to complete to open an account at bunq. The process allows us to identify a user and verify their identity based on documents, data, or information collected from a reliable and independent source.

**Companies**

Onboarding is the process that all user companies need to complete to open an account at bunq. This procedure allows us to:

- verify that any person claiming to act on behalf of a company is authorized to do so, and verify the identity of that person;
- identify the Ultimate Beneficial Owners (UBOs) (owners of those in charge of the company) and take reasonable measures to verify their identities;
- take reasonable measures to understand the governance and control structure of legal persons, trusts, companies, foundations, and similar legal arrangements; and
- assess and, as appropriate, collect information on the purpose and intended nature of the business relationship.

## 8 Measures to counter Money Laundering 🛡️

bunq has implemented a number of measures and processes in its anti-money laundering efforts. These include country, industry, and legal form risk rankings to classify different users

### Country, industry, and legal form risk ranking

Important indicator for our onboarding, risk scoring, and monitoring rules are

(i) the country of residence of the users;

(ii) the applicable company SBI code's risk rating; and

(iii) the legal form of the user company.

These factors influence the measures bunq implements for screening, monitoring and review of users.

### Transaction monitoring

To comply with legal obligations for ongoing monitoring of business relationships (article 3 sub 2d of the Wwft), we have developed a monitoring system. It consists of two parts: pre-transaction monitoring (transaction filtering) and post-transaction monitoring.

1. Pre-transaction monitoring (pre-transaction filtering)

This process involves monitoring before a transaction is fully executed. In other words, before a transaction reaches the account of the intended payee. This calls for several monitoring rules, each with several criteria. When each criterion applies to a transaction or transaction pattern, the rule applies, and an 'alert' is created. When an alert is triggered, the transaction gets automatically redirected to a suspense account. The redirection occurs to prevent the transaction from reaching the payee.

All alerts show up as notifications in our customer relationship management system and are investigated by our analysts. An alert investigated by our analysts awho may reverse or freeze the transaction if the investigation proves that the transaction is likely related to any illegal activities.

2. Post-transaction monitoring

The post-transaction monitoring system refers to monitoring that takes place *after* a transaction is fully executed. This system creates alerts in a similar fashion to the pre-transaction monitoring system mentioned above, but it does not divert transactions, because the monitoring takes place after the transactions have already been fully executed. Most monitoring takes place post-execution in order not to disrupt payment traffic too much (this is a common industry practice).

The post-transaction monitoring system consists of both monitoring rules and machine learning models. The machine learning models have been 'trained' on historical transaction data we suspect to be related to money laundering and which we have detected in various ways over a period of several years.

The models are designed to detect whether a transaction or pattern is similar to a transaction or a pattern the model was trained on. The output of the models is a similarity score between zero and one. This score indicates how ‘similar’ the model believes a transaction is based on what it has ‘learned’ from the historical data (0 - not similar at all, 1 - exactly the same). In case the score is above a set threshold, an alert is created. The threshold is the best possible balance between false positives and false negatives.

In some cases, the system will not only trigger an alert but also an automatic and immediate account freeze or account restrictions. The account freeze or restrictions allow an analyst to investigate a user without the risk that the user conducts (materially) more illegal activities with his/her account in the course of the investigation.

### Source of funds

Furthermore, besides transaction monitoring, we are required to, where necessary, ask for a user’s source of funds. Our approach to company users is different from the approach to user persons because the behavior of user companies is much more diverse and complex than that of user persons. Our agents are tasked with manually assessing the behavior of user companies and if needed manually inquiring about their source of funds.

### Screening

We screen users or parties related to the users based on lists that concerns:

- Politically Exposed Persons (PEP), including Relatives and Close Associates (RCA);
- Special Interest Persons (SIP);
- Entities and individuals that received adverse media attention; and
- Sanctioned entities and individuals.

### Enhanced Due Diligence

bunq applies due diligence measures to all business relationships it creates with users. We take a further step and apply enhanced due diligence measures to business relationships or transactions. These measures allow bunq to be more thorough in assessing users and transactions.

### Periodic reviews and keeping our files up to date

bunq has a legal obligation to keep the files of our users up to date. For this purpose we conduct checks on our user’s personal details, transaction profiles, and risk profiles.

## 9 Off-boarding ❌

We have no appetite to service users who are (suspected of) misusing our services longer than legally required. Legally, even if a user is (suspected of) misusing their bunq account, we have to follow our duty of care toward users for a period of time, as users have a right to a bank account.

Taking into account our risk appetite and the law on the right to a bank account, we have defined several non-exhaustive situations in which we believe to have a proper reason to terminate a relationship with a user.

If we have indications that a user might be misusing our services, but the case is not strong enough to warrant the termination of the relationship, the user will be: (i) investigated further, (ii) reported to the FIU and/or (iii) be subject to further (enhanced) monitoring.

## 10 Policy deviations 🛣️

In exceptional cases, an analyst from the First line of defense can request a deviation of this policy if they believe that it is in the best interest of bunq. Such a request can be submitted to the CRO and should always include:

- A clear description of why the analyst wants to deviate; and
- A clear description of why the analyst believes it is in the best interests of bunq to deviate in the particular case.

Only the CRO can approve deviation requests but they can also delegate this responsibility to other senior employees.

The CRO, or an authorized employee, can approve a request in case: (i) there are no legal objections, (ii) the situation presented by the analyst justifies a deviation, and (iii) the deviation is an acceptable risk.