Last reviewed and approved on
27 November 2024

Anti-Money Laundering & Counter Financing of Terrorism Policy

1. OBJECTIVE

Prosus N.V. (the "company") is a global consumer internet group and one of the largest technology investors in the world. In this anti-money laundering and counter financing of terrorism policy (the "policy"), the group and its subsidiaries are together referred to as the "group", collectively referred to as "group companies", and individually referred to as a "group company".

We conduct business in compliance with applicable laws and regulations, and in accordance with our code of business ethics and conduct. We do not tolerate or facilitate, nor wish to be involved in, any form of financial crime and are committed to preventing unethical business practices to maintain the integrity of financial systems.

2. POLICY OBJECTIVE

The objective of this policy is to protect the group, its employees (both permanent and temporary) and directors from any form of involvement in money laundering or terrorism financing. We also want to ensure that group employees understand the importance of the principles that are set out in the code of business ethics and conduct and our commitment to combatting money laundering and terrorism financing.

The countries in which the group operates may have specific anti-money laundering ("AML") and counter terrorism financing ("CFT") laws and regulations, many of which apply not only within the borders of the country that enacted them but also to actions, individuals, or entities outside of that country.

This policy sets out the minimum AML and CFT requirements and standards that we expect group companies to implement with respect to anti-money laundering and counter terrorism financing. For further guidance on implementation, please refer to the Anti-Money Laundering & Counter Financing of Terrorism Programme Guidance.

3. OUR COMMITMENT / IMPORTANCE OF COMPLIANCE

The group considers money laundering and financing of terrorism, and violations of associated rules and obligations, to be a very serious matter. The group is committed to adhering to all applicable laws and regulations concerning AML/CTF. This commitment extends to preventing any involvement in or facilitation of money laundering and terrorism financing.

The consequences of money laundering and terrorism financing are severe, and can result in substantial fines, criminal proceedings, and imprisonment. Non-compliance with AML/CFT obligations may also trigger scrutiny from regulatory authorities. Money laundering and terrorism financing can cause serious damage to the reputation of the group, which could result in significant declining trust of business partners and customers, and ultimately business losses.

4. MONEY LAUNDERING AND TERRORISM FINANCING

MONEY LAUNDERING

Money laundering is the act or process whereby the proceeds of crimes are transformed into seemingly legitimate funds or other assets. This illegal practice is primarily aimed at concealing the origins of money obtained through various criminal activities (such as fraud, tax evasion, theft and drug trafficking) thereby integrating it – either directly or via layering - into the legal financial system.

TERRORISM FINANCING

Terrorism financing is the provision or collection of funds or assets, knowing that they will be used, in whole or in part, to support terrorist activities. Contrary to money laundering, the funds used for terrorism financing may originate from legitimate sources. The financing of terrorism involves the use of the financial system or international trade mechanisms to transfer funds or assets that will support terrorist acts or organisations.

5. COMPLIANCE REQUIREMENTS

The scope and requirements of laws and regulations related to AML and CFT, differ between the territories and jurisdictions in which the group operates, and depend on the product/business that the group operates. This means that group companies must at least annually (and, more frequently, if necessary, in response to any regulatory changes or updates, or changes in the group's product/business):

1. determine which specific AML/CFT legislation applies to them;
2. assess AML/CFT risk exposure, and legal obligations deriving from applicable law; and
3. have their management review their relevant AML/CFT programme.

Where this policy prescribes rules that are not explicitly prescribed by local law, the rules in this policy prevail. In jurisdictions where local laws or regulations are stricter than the rules in this policy, local and sector law prevails, but only insofar as it is stricter than this policy.

Where there is an apparent or perceived conflict between external legal requirements and this policy, management is required to consult the group chief ethics & compliance officer before taking any action.

5.1. WE UNDERSTAND OUR BUSINESS AND REGULATORY OBLIGATIONS

Depending on their business activities and the jurisdiction in which they operate, group companies may be subject to different legal and regulatory requirements. Group companies must understand whether any part of their business is regulated according to locally applicable laws and regulations. In case of doubt or uncertainty about the applicability of any regulation, management should consult their respective ethics & compliance officer.

The following business activities are important indicators that AML/CFT regulations may apply:

- Providing payments or services, that may also be provided by financial institutions (including banks, payment service providers, brokerage firms, savings associations);
- Providing professional (certain legal or notary) services, or consulting services (eg. financial or investment advice);
- Providing services in relation to virtual/crypto currencies, such as currency exchange or virtual wallets;
- Dealing with high value goods; and
- Receiving cash payments.

These activities are often subject to increased legal requirements, and additional regulatory scrutiny applies in most jurisdictions and territories. To meet these local and sector specific requirements, this policy may need to be supplemented with additional measures.

In markets where regulatory guidelines exist for AML and CFT, these regulations should be reviewed regularly, and will require strong oversight and management through the AML/CFT programme.

AML/CFT requirements may also apply to businesses where activities do not include payment services or other financial products and services. Every group company is therefore required annually to assess AML/CFT exposure of its business activities, and which AML/CFT specific laws and regulations apply (or may be applicable in the future).

5.2. WE ASSESS & MANAGE THE MONEY LAUNDERING AND TERRORISM FINANCING RISKS FACING OUR BUSINESS

Appropriate steps must be taken to identify and assess the exposure and the risk of money laundering and terrorism financing. In doing so, each group company must consider risk factors relating to their:

- customers[1];

[1] Procedures for mitigating AML/CFT customer risks, such as know your customer procedures, may need to be

- geographical areas of operations;
- products and services;
- distribution channels;
- transactions; and
- third parties[2].

At a minimum, applicable legislation must be assessed annually, and, in addition, group companies must ensure that their AML/CFT risks are adequately assessed when a change in business or regulation occurs.

The AML/CFT risk assessment will determine a risk-based design and appropriate level of implementation of the AML/CFT programme on a local level (fit for purpose).

AML/CFT is a specialised compliance area, requiring specific knowledge and expertise, and it is imperative that individuals with relevant experience provide guidance on the development, implementation and monitoring (including assurance) of local AML/CFT programmes. Given the substantial exposure associated with AML/CFT, it is crucial that this subject is comprehensively integrated into the ethics & compliance programmes of group companies.

6. MINIMUM STANDARDS OF THE AML AND CFT PROGRAMME

The AML/CFT programme implemented by each group company should respond to the risks identified through the completed risk and exposure assessment. The following minimum standards should be implemented, to form the framework of an AML/CFT programme:

6.1. AML/CFT POLICIES AND PROCEDURES

AML/CFT policies and procedures form the base of an AML/CFT programme. Certain global regulations require minimum standards to be included in policies and procedures.

Depending on the nature of the business activities and risk exposure, a group company should consider developing internal policies, controls and procedures that include: (i) AML/CFT objectives, (ii) risk management, (iii) customer due diligence, (iv) customer and/or transaction screening, (v) transaction monitoring, (vi) reporting, (vii) record-keeping, (viii) internal controls, (ix) compliance management, (x) employee screening, and (xi) employee training and awareness.

6.2. PERIODIC AML/CFT RISK ASSESSMENT

As the risk profile of any group company may change over time (for example, due to the expansion of business activities, or a changed customer/product portfolio), AML/CFT risk assessments should be updated annually (and on ad hoc basis, depending on significant changes in operations and the regulatory environment). After the AML/CFT risks of the business have been reassessed, the AML/CFT programme should be adapted to mitigate any new potential risks.

6.3. KNOW YOUR CUSTOMER (KYC)[3]

Customer risk is often the largest factor exposing an organisation to risks of money laundering and terrorism financing which means that one of the most important aspects of an effective AML/CFT programme is knowing our customers and understanding the business relationships that we have with each of them. Appropriate KYC processes and procedures include identification and verification of the ultimate beneficial owner(s), and updated procedures to include the enhanced due diligence for high-risk third parties.

applied in addition to other third party contracting or vendor selection procedures e.g. due diligence procedures.

[2] Various other policies and procedures aimed at mitigating the AML/CFT risks may apply to the group companies, such as the group's anti-bribery and anti-corruption policy (including third party due diligence), the group's sanctions & export controls policy and local procurement policies.

[3] Terminology varies across industries and regions. Know your customer may also be referred to as customer due-Diligence. Please also refer to Third Party Risk Management Policy for guidance.

The results of customer due diligence activities and procedures, including third-party risk classification, mitigating measures and approvals, must be recorded and available to the relevant functions and personnel. Appropriate AML monitoring needs to be set up, including periodic review.

Group companies shall implement a risk-based approach to the KYC process. KYC procedures will be mandatory for customers that exhibit higher risk exposure. The criteria for determining high-risk customers will include, but are not limited to, the nature of the business, geographical location, and transaction patterns. Customers with lower risk exposure may undergo simplified due diligence measures. This approach ensures that resources are focused on higher-risk areas, enhancing the effectiveness of the policy.

6.4. CUSTOMER AND TRANSACTION SCREENING

To detect potential money laundering or terrorism financing risk factors and indicators, all group companies should implement processes in their AML/CFT programme, aimed at identifying customers and transactions involving politically exposed persons, sanctioned persons, entities, or countries. As risks related to politically exposed persons and sanctions are integral elements to be addressed by AML/CFT regulations globally, this policy should be read in conjunction with the group's anti-bribery and anti-corruption and sanctions & export controls policies.

6.5. TRANSACTION MONITORING

Transaction monitoring procedures should aim to scrutinise transactions throughout the course of a business relationship. This is to ensure that the transactions conducted are consistent with the organisation's understanding of the customer's expected business activity (as obtained through the onboarding and KYC processes).

Group companies must be aware of any obligations to report unusual or suspicious activities to financial intelligence units/ and other authorities (as well as monitoring and reporting, derived from contractual obligations with partners). This requires handling of all generated alerts without delay, and prompt reporting of alerts that cannot be reasonably discarded as not suspicious or as a false positive.

6.6. AML/CFT REPORTING (EXTERNAL AND INTERNAL)

Group companies should establish processes and procedures that allow them to respond appropriately and timely to external information sharing requests regarding AML/CFT topics (for example from financial intelligence units or other authorities).

Group companies should also ensure that there are processes and procedures in place to facilitate regular and ad-hoc reporting to management on AML/CFT related subjects and issues.

6.7. TRAINING AND CAPABILITIES

Ongoing training is an essential element of a strong AML/CFT programme and it must be regularly updated to reflect legal and regulatory developments, emerging risks, changes in the AML/CFT requirements, trends, internal policies/procedures and best practices. Training objectives, plan, and completion rates, as well as identification of functions are risk should be recorded and monitored.

6.8. ACCURATE BOOKS AND RECORD KEEPING

All AML/CFT relevant information and documentation must be accurately, completely and timely recorded in the books and records of the relevant group company. Appropriate documentation to support all AML/CFT activities and its monitoring, including e.g. transactions that were scrutinised in the transaction monitoring process, must also be maintained insofar as permitted, for at least as long as required by local laws and regulations.

7. GOVERNANCE

Management is responsible for the implementation of this policy and a fit for purpose AML/CFT compliance programme in the group company for which they are responsible. The design (depth and breadth) of the programme, must be based on the outcome of an AML/CFT risk assessment. The programme must be designed to ensure that all employees comply with applicable laws and regulations and conduct business in accordance with the requirements set in this policy.

The ethics & compliance officer supports management in the implementation of this Policy and reports to group ethics & compliance on the design and implementation of the programme.

Group ethics & compliance serves as the point of contact for this policy and will - along with group risk & audit - monitor the design, implementation, adequacy and effectiveness of the programme, as necessary.

The prior written approval of the group chief ethics & compliance officer, who is the ultimate owner and has overall responsibility for the implementation of this policy, is required for any deviation from this policy.

This policy will be reviewed on an annual basis by group ethics & compliance.

8. APPLICABILITY

This policy applies to all group companies and to (temporary and permanent) employees, directors, officers, trainees, and secondees. Where applicable, contract workers, consultants, agents and any other third parties acting on our behalf are required to comply with relevant principles of this policy.

9. NON-COMPLIANCE

Group expects every employee to strictly adhere to this policy and the requirements therein. Non-compliance with AML/CFT obligations and/or any involvement in money laundering and/or terrorism financing, may lead to disciplinary action, including, where appropriate, dismissal or termination of contract. Violations of AML and CFT regulations can have additional legal consequences for individuals involved, including civil or criminal liability, monetary fines and imprisonment.

10. QUESTIONS

If you have any questions about this policy, please contact your ethics & compliance officer. If you are unsure whether an activity is contrary to this policy, seek guidance from your ethics & compliance officer before any action is taken.

11. REPORTING CONCERNS

If you believe that there has been a breach of this policy (or that one is about to happen), we encourage you to speak up. For further details please see the group speak up policy. If you do not feel comfortable making a speak up report internally, you may use the external speak up service operated by an independent third party at: https://speakup.prosus.com