

Last reviewed and approved on
27 November 2024

Third Party Risk Management Policy



prosus

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 third party risk management 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 take our legal and ethical responsibilities seriously. It is our policy to operate in accordance with applicable laws and regulations and our code of business ethics and conduct.

This policy outlines the group’s approach to managing third-party risks, emphasizing a risk-based approach to due diligence. The principles and minimum standards set forth in this policy are designed to protect the group’s reputation and mitigate risks associated with third-party engagements.

2. POLICY OBJECTIVE

The objective of this policy is to:

- set out the principles to which the group is committed and which it expects all employees, officers and directors (as well as anyone working for or on behalf of the group) to observe and to adhere to; and
- set out the minimum standards that we expect group companies to implement with respect to third party relationships.

3. THIRD PARTIES

Illegal conduct by third parties with whom we do business can seriously affect the group’s reputation. We can also be held liable for the illegal conduct of third parties that act on behalf of any group company.

A third party is any company, organisation or individual with which the group or any group company has an existing, past or prospective business relationship. This includes (but is not limited to), for example: vendors; suppliers; strategic partners; intermediaries; consultants; charitable organisations; and sponsorship recipients. (Acquisition targets are also third parties, how to engage with them is covered in the Investment / M&A Compliance Guidelines). Specific sets of third parties, which pose negligible risk, may be excluded from this Policy, in agreement with the group Ethics & Compliance function (e.g. independent delivery riders).

4. RISK FRAMEWORK

Depending on the nature of the third party, the nature of the services provided, geographical location, and/or the business case for engaging, third parties could expose the group to different risks, including, without limitation, in relation to: bribery and corruption; sanctions and export controls; competition law; cyber security; and fraud.

Group companies must establish a risk framework to determine the level of risk posed by each third party and adopt a compliance approach that is based on the following risk determination.

4.1. Nature of the third party

Group companies should consider:

- whether the third party is reputable (i.e. they have a history of providing the services requested, the due diligence process did not reveal significant red flags);
- whether the third party has significant relationships with public officials (as defined in the group Anti-Bribery and Anti-Corruption Policy), and the nature of those relationships (including relating to beneficial ownership);
- the third party’s location of operation, business or incorporation and whether the location is at higher risk of corruption or sanctions; and
- any history of non-compliance or previous misconduct of any nature.

4.2. Nature of the services provided

Group companies should also consider whether the third party would:

- represent the group company (e.g. as an intermediary or agent), particularly to public officials;
- help gain or retain business;
- be in a position to influence decisions or the conduct of other third parties for the benefit of the group company;
- be involved in obtaining a regulatory approval or any kind of license or permit (even where routine in nature).

4.3. Business Case

Based on the considerations from 4.1 and 4.2, group companies should carefully consider the business case for engaging (or retaining) the proposed third party. Considerations should include:

- whether the service is needed;
- the compensation structure (including the incentives of the structure); and
- whether the transaction is one-off and of significant value (for example where it is difficult to determine an appropriate market rate).

4.4. High Risk Third Parties

Those acting on behalf of the group or recommended by public officials are classified as high-risk and require enhanced due diligence, regular re-evaluation, and robust contractual agreements to mitigate risks.

5. DUE DILIGENCE PROCESS

The group expects its group companies to perform risk-based due diligence on third parties with whom they do business. The risk level is determined within the group company's risk framework, as set out in Section 4 above.

Third party relationships must undergo appropriate due diligence, proportionate and commensurate to the potential risk, as per the minimum standards set out throughout this policy.

While the due diligence process should be tailored to the group company's unique risks, the due diligence process for third parties with a medium or high risk profile should typically include:

- a review of corporate information (including beneficial owners and controllers);
- a background investigation (into the third party and its beneficial owners and controllers);
- a search of relevant sanctions- and watch-lists and, to the extent available, relevant court judgements or regulatory enforcement.
- for software as a service (SaaS), enquiries to ensure usage of AI (if any) meet group standards; and
- for significant IT services providers, enquiries to ensure the vendor has appropriate security controls in place.

Group companies must also consider potential conflicts of interest and, where they arise, ensure a management plan is in place.

Group companies are responsible for determining the appropriate level of due diligence for third parties, in a risk-based manner and allocating resources appropriately to manage the third party risks effectively.

6. RED FLAGS

The purpose of conducting due diligence is to obtain information about the third party's business situation, track record, reputation and integrity. During this process, potential red flags may be identified such as:

- past involvement in misconduct;

- appearance on applicable sanctions list (note: any transactions with sanctioned persons require group level review under the sanctions & export controls policy);
- past involvement in bribery and corruption, fraud, anti-competition or other types of illegal activities or misconduct;
- compliance breaches, suspicious background or reputational issues;
- the third party is located in, or has material connections to, a sanctioned or high-risk territory;
- the third party is beneficially owned or represented by public officials, or has other close connections to public officials;
- the third party refuses to provide information on its beneficial owners, business or operations;
- the third party does not agree with adequate contractual clauses regarding compliance;
- the third party or its beneficial owners or controllers do not have experience providing the services proposed or in the geography where the services should be provided;
- red flags related to payments include requests for: payments in cash (or cash equivalents); payments via offshore structures; payment to be made to another party; and payments that are not in line with the market or agreed rates (for example unusually high or low);
- the third party uses or suggests that we use other parties for work that we would expect to be executed by the third party itself; and
- for third parties providing technology services, a history of availability and security incidents and lack of an independent third party assurance report.

Depending on the red flags and risk level, additional due diligence may be required.

After all required due diligence is completed, the group company should decide whether, based on the outcome, the relationship should proceed and which measures should be taken to mitigate the risks identified, if any. Such measures can include, but are not limited to:

- general contractual provisions, including representations and warranties about the third party and its business, compliance with laws, termination rights, payment, documentation and information rights;
- contractual provisions or undertakings covering adherence to the Group Anti- Bribery & Anti-Corruption Policy;
- anti-bribery & anti-corruption training (particularly for high risk third parties);
- acknowledgement of, and commitment to, our code of business ethics and conduct and/or supplier code
- periodic due diligence and business case review; and
- reviews and/or monitoring of payments.

7. APPROVAL

The process for review and approval after due diligence is completed must be clearly defined and signed off to ensure an independent view on the risks related to the third party relationship. Where red flags are identified, group companies must have an escalation process in place.

The due diligence and risk analysis should be recorded and retained in accordance with records management policies and procedures. This applies both to accepted and rejected third party relationships. Final decisions and the underlying rationale (and where relevant approvals) must always be documented and retained.

8. CONTROLS

Group companies must have appropriate controls in place, including:

- payments should be documented, including with the appropriate underlying documentation;
- third parties should be categorised appropriately; and
- controls around onboarding and offboarding and periodic review.

9. APPLICABILITY

This policy applies to all group companies and to (temporary and permanent) employees, directors, officers, trainees, and secondees, contract workers, consultants, agents and any other third party acting on our behalf on a risk-based approach. Group companies, in agreement with the group Ethics & Compliance function, may outline specific sets of low-risk counterparties which may not be in scope of this policy.

10. FURTHER GUIDANCE AND DEVIATIONS

The group chief ethics and compliance officer may set out additional requirements, processes or guidelines from time to time with respect to this policy, which group companies must implement. The approval of the group chief ethics and compliance officer is required for any deviation from this policy.

11. NON-COMPLIANCE

Non-compliance with this policy is a serious matter and will lead to disciplinary action, including, where appropriate, dismissal and/or termination of contract. Violations of anti-bribery and anti-corruption laws can have additional legal consequences for individuals involved, including civil or criminal liability, monetary fines and imprisonment.

12. 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 to internally, you may use the external speak up service operated by an independent third party at: <https://speakup.prosus.com>

13. POLICY OBJECTIVE

The objective of this policy is to:

- set out the principles to which the group is committed and to which the group expects all employees, officers and directors (as well as anyone working for or on behalf of the group) to observe and to adhere; and
- set out the minimum standards that we expect group companies to implement with respect to anti-bribery and anti-corruption.

14. WHAT IS BRIBERY & CORRUPTION?

Corruption is 'the illegal use of entrusted power for private gain'. This means the illegal use of power or a position for an undue or illicit advantage.

Bribery involves promising, offering, authorising or giving something of value in order to illegally obtain an undue private or business advantage or to illegally influence decision-making. Bribes can be promised, offered, authorised or given to public officials (see Section 5.3 below) as well as (employees of) private enterprises.

Bribes can take many forms, including cash or payments, but it is not limited to these and may also include things such as:

- gifts, entertainment, travel expenses;
- providing goods, services or advantages;
- overpayments or discounts;
- hiring decisions; or
- any other tangible or intangible thing that has value to the recipient.

We have a zero tolerance approach to bribery and corruption. Participating in any corrupt behaviour (whether giving or receiving) is strictly prohibited. These behaviours may also constitute an offence under anti-bribery laws.

Bribery and corruption can take place both by direct contact between a group representative and another party, as well as by indirect contact through a third party such as an agent, intermediary or even a family member or friend. This behaviour is also prohibited.

15. WHY IS ANTI-BRIBERY AND ANTI-CORRUPTION IMPORTANT FOR PROSUS GROUP?

The group considers violations of anti-bribery and anti-corruption rules to be a very serious matter. Bribery and corruption: (1) negatively impact social, economic and environmental development; (2) undermine societal trust; (3) divert resources to improper purposes; (4) lead to a distortion of the economy, environmental mismanagement and state failures; (5) undermine labour standards; and (6) restrict access to basic human rights.

We are building leading companies that empower people and enrich communities. Any involvement in bribery or corruption is contrary to our values and is not the right thing to do. Bribery and corruption can result in fines, criminal proceedings and prison sentences. In addition, bribery and corruption can cause serious damage to the reputation of the group, which may result in loss of trust of business partners, consumers, and ultimately loss of business.

16. HOW DO WE COMPLY WITH ANTI-BRIBERY AND ANTI-CORRUPTION LAWS?

Each group company must comply with the minimum standards set out in this policy. In addition, the scope and requirements of anti-bribery and anti-corruption laws differ between the jurisdictions in which the group operates. This means that group companies must determine, on an ongoing basis, which specific bribery and corruption legislation applies to them, bearing in mind that some laws have broad extra-territorial reach. All group companies must have a suitable anti-bribery and anti-corruption programme, which must be reviewed annually by management.

Where this policy sets out requirements or standards that are not explicitly prescribed by local law, the requirements or standards in this policy prevail. In jurisdictions where local laws or regulations are stricter than the rules in this policy, local 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 group ethics & compliance before taking any action.

16.1. GIFTS, HOSPITALITY, TRAVEL & ENTERTAINMENT

Gifts, hospitality, travel, entertainment or other things of value can be used to influence business decisions in an illegal way. We do not permit anything that goes beyond what is legally permitted, customary and generally accepted in the relevant business environment.

Courtesy gifts, relatively limited hospitality, travel, and entertainment are allowed for legitimate business purposes but should:

- not include cash payments (or cash equivalents);
- not be designed or intended to illegally influence business decisions or outcomes; and
- be provided in connection with a legitimate business purpose;
- be in line with laws, regulations and generally accepted policies for professional courtesy; and
- be reasonable under the circumstances.

Group companies that give or receive gifts must define threshold values and guidelines that apply to gifts (whether offered or received), hospitality, travel, and entertainment. If gifts, hospitality, travel or entertainment exceed these thresholds, or if they are not in line with the guidelines, then employees should contact their ethics & compliance officer for advice.

16.2. CHARITIES/CHARITABLE DONATIONS, POLITICAL CONTRIBUTIONS, AND SPONSORING ACTIVITIES

We carefully consider any payment to charities/charitable donations, political contributions or

sponsorships and follow the below principles:

- they must not illegally influence (or attempt to influence) a business decision or outcome; and
- they must be made to a legitimate organisation which has undergone an appropriate level of due diligence.

All charitable donations and sponsorships must be approved by the group company's management and accurately recorded in the books of the relevant group company. Charitable contributions and any sponsorships are also subject to the requirements set out in the Third Party Risk Management Policy.

Political contributions (which include any contributions of group company funds or other assets for political purposes, encouraging individual employees to make any such contributions, and/or reimbursing an employee for any contribution) made directly or through trade associations are prohibited unless pre-approved by the relevant committee of the Prosus board. Political contributions must be accurately recorded in the books of the relevant group company.

16.3. PUBLIC OFFICIALS

We need to be particularly careful when dealing with public officials as this can bring a higher risk or perceived risk of corruption. The definition of public official is broad and includes:

- any officer or employee – regardless of rank - of a government entity or public organization;
- elected officials, politicians and candidates for political office;
- any officer or employee of entities that are government -owned or government-controlled; and
- any private person acting on behalf of a government entity or public organisation, even if temporarily.

It is prohibited to provide or promise any gifts, services, travel or hospitality (other than meals and refreshments of nominal value) to public officials, without the prior written authorisation of the relevant group company's ethics & compliance officer. These pre-approvals should be documented and appropriate records should be maintained.

16.4. THIRD PARTIES

Illegal conduct by third parties with whom we do business can seriously affect the group's reputation.

We can be held liable for the illegal conduct of third parties that act on the group or any group company's behalf.

Third party agents, intermediaries, consultants, distributors or any other third party acting for or on behalf of the group or group company or engaging public officials on their behalf are prohibited from making payments to third parties ("relevant third parties") on behalf of the group or any group company if such payments violate the principles of this policy. The same prohibition also applies to any subcontractor acting on behalf of the group or any group company.

All third party relationships must undergo appropriate due diligence, in compliance with the Third Party Risk Management Policy.

Any payments made to relevant third parties must be appropriately documented, including with all applicable supporting documentation.

16.5. M&A

The group performs due diligence before acquiring or investing in third parties (including by way of mergers, acquisitions or joint ventures). Bribery and corruption risk and associated due diligence must be carried out in accordance with group requirements and standards, and with the involvement of the ethics & compliance function. The outcome of due diligence investigations, including mitigating measures and approvals, should be recorded and available to the relevant functions.

16.6. PAYMENTS

Facilitation payments are typically low-value payments requested by public officials to perform or expedite a routine business decision (for example issuing permits, licenses, visas, etc). Facilitation

payments are illegal and considered as a form of bribery in several jurisdictions and should therefore not be paid.

Where there is an imminent threat to safety, physical health or wellbeing, employees and contractors are expected to take reasonable steps to remove themselves from danger. In exceptional circumstances, this may include making a payment to a public official to avoid immediate harm (for example a threat of violence). Any such incident must be reported to group ethics & compliance as a matter of urgency.

17. ACCURATE BOOKS AND RECORD KEEPING

All transactions must be accurately, completely, and timely recorded in the books and records of the relevant group company. Appropriate documentation to support the transaction must also be obtained, reviewed and maintained.

18. MINIMUM STANDARDS

At a minimum, group companies must implement the following minimum standards:

- Management demonstrates a 'tone-at-the-top' that promotes a culture of business integrity; and emphasises compliance with this policy and speaking up on anti-bribery and anti-corruption compliance in the event of concerns.
- Management, relevant employees and anyone working for or on our behalf are made aware of anti-bribery and anti-corruption-related obligations and this policy and are responsible for compliance with this policy as it applies to their duties.
- Management, relevant employees and relevant high-risk third parties receive appropriate training on this policy and reporting mechanisms for any potential violations of this policy.
- Bribery and corruption-related risks are assessed on a regular basis and appropriate measures are taken to address the risks identified, such as risk-based due diligence of third parties, due diligence around charitable contributions, donations, sponsorships and investments; appropriate controls around gifts, entertainment and hospitality.
- Employees may not proceed with any transaction or other activity if they know that a violation of applicable bribery or corruption regulations has occurred or is likely to occur, or are aware of unresolved red flags related to the transaction (unless there is an imminent and unavoidable threat to safety, physical health or wellbeing).
- Appropriate records of transactions must be maintained at all times, including the relevant supporting documentation.
- Appropriate records must be maintained to demonstrate compliance with anti-bribery and anti-corruption regulations and this policy. In the event of a bribery or corruption-related investigation, inspection or request for information, the group chief ethics & compliance officer shall be notified immediately.
- Any actual or suspected violation of this policy or applicable anti-bribery and anti-corruption regulations, or breach of anti-bribery-related obligations is reported immediately to group ethics & compliance through the agreed channels, are thoroughly investigated and, if substantiated, prompt and appropriate action is taken, such as disciplinary action, remedial measures and organisational or process improvements.

Group ethics and compliance, along with group risk and audit will monitor the design, implementation, adequacy, and effectiveness of the anti-bribery and anti-corruption compliance programme.

19. APPLICABILITY

This policy applies to all group companies and to (temporary and permanent) employees, directors, officers, trainees, and secondees, contract workers, consultants, agents and any other third party acting on our behalf.

20. FURTHER GUIDANCE AND DEVIATIONS

The group chief ethics and compliance officer may set out additional requirements, processes or guidelines

from time to time with respect to this policy, which group companies must implement. The approval of the group chief ethics and compliance officer is required for any deviation from this policy.

21. NON-COMPLIANCE

Non-compliance with this policy is a serious matter and will lead to disciplinary action, including, where appropriate, dismissal and/or termination of contract. Violations of anti-bribery and anti-corruption laws can have additional legal consequences for individuals involved, including civil or criminal liability, monetary fines and imprisonment.

22. REPORTING CONCERNS

If you believe that there has been a breach of this policy (or intention to do so), 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 to internally, you may use the external speak up service operated by an independent third party at: <https://speakup.naspers.com>