Third Party Risk Management Policy

Last reviewed and approved on 27 November 2024

NASPERS

NASPERS

Third Party Risk Management Policy

1. OBJECTIVE

Naspers Limited (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 is 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.naspers.com