ANTI-FRAUD POLICY

thinkproject

Management system: Compliance
ALL
Document ID: COMP_0006
Version: 1.0
Classification: Open

Created by	Peter Mezger	27.05.2022
Approved by	Ralf Grüßhaber	27.05.2022
Date of original issue	27.05.2022	

Please do not print copies of this document.

CONTENT TABLE

1 INTRODUCTION

In a constantly changing environment, which is characterized by increasing internationality, decentralization and complexity of business activities, there are constantly increasing risks of white-collar crime in and against companies.

Thinkproject establishes this Anti-Fraud Policy (the "Anti-Fraud Policy") as a demonstration of its commitment to the highest ethical standards of openness, honesty and accountability in all of its affairs. Based on this commitment, this Anti-Fraud Policy outlines the principles to which we are committed in relation to preventing, reporting, and remediate fraud and corruption and establishing a corporate and working culture that improves the value of ethics and promote the individual responsibility. It also outlines the individuals' responsibility for dealing with such incidents.

If you have any questions about this Policy you should contact the Compliance or the Legal Department.

2 OBJECTIVE

The primary objective of the Anti-Fraud Policy is to prevent fraud, maintain integrity in business dealings, establish procedures and protections that allow to act on suspected fraud or corruption with potentially adverse ramifications and to achieve the legitimate Subject of this Policy.

Thinkproject works in accordance with the applicable legal regulations and acts, under special attention of

- Article 325 of the Treaty on the Functioning of the European Union (legal basis for the fight against fraud)
- U.K. Bribery Act impose
- The U.S Foreign Corrupt Practices Act (FCPA)

This Policy applies to Thinkproject's operations globally, including all legal entities worldwide owned or controlled by Thinkproject (including all group companies), and to all directors, officers, employees, contractors, and other third parties acting on behalf of the foregoing.

3 WHAT IS FRAUD?

In the broadest sense, fraud can encompass any crime for gain that uses deception as its principal method of operation. More precisely, fraud is defined as: "A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment". Indicatively, for the purpose of this document, fraud may involve:

- manipulation, falsification or alteration of accounting records or documents
- suppression or omission of the effects of transactions from records or documents
- recording of transactions without substance
- misappropriation (theft) or wilful destruction or loss of assets including cash
- deliberate misapplication of accounting or other regulations or policies
- bribery and corruption
- usurpation of corporate interests for personal gain

- payment or receipts of bribes, kickbacks or other inappropriate payments
- participation in sham or fraudulent transactions, and
- disclosing confidential and proprietary information to outside parties

There is no set monetary threshold that defines a fraud. There is no need for the fraud to be successful to be viewed as corrupt; the offering can be enough to amount to a criminal offense in certain jurisdictions. These principles apply equally in any country in which Thinkproject operates or carries on business.

4 PREVENTION AND CONTROL OF FRAUD

Management shall advocate and develop a corporate culture of honesty and integrity, establish controls and procedures designed to eliminate the likelihood of fraud and to receive, investigate, report and recommend a remedial course of action in respect to suspected or voiced concerns of fraud or fraudulent behavior. More specifically:

- Management shall lead by example in complying with the Partnership's rules and regulations, including this Anti-Fraud Policy;
- Management shall notify Personnel of the opportunity and procedures for anonymously reporting wrongdoings and dishonest behavior through the established whistle-blower policy and the channels of communication defined thereto;
- In connection with the annual risk assessment process management shall identify and assess the importance and possibility of fraud risk at entity level, at business department level and at process level;
- Management shall establish procedures to reduce the potential occurrence of fraud through protective approval, segregation of duties and periodic compliance reviews. For those risk areas of fraud occurrence, such as inaccurate financial reporting, exceeded authorization, and information systems, management shall establish necessary internal control activities.

In terms of establishing and maintaining effective controls it is generally desirable that:

- Wherever possible, there must be a separation of duties so that control of a key function is not vested in one individual
- Back-logs should not be allowed to accumulate and
- Whenever designing any new system, consideration must be given to building in safeguards.

The Audit Committee (Member of Compliance and Legal Department; Member of CxO, the CFO will be the Chairman of the Audit Committee) is responsible for establishing and maintaining a sound system of internal controls that supports the achievement of aims and objectives. The system of internal controls is designed to respond to the fraud risks that Thinkproject is faced. The system of internal controls is based on an on-going process designed to identify the principal fraud risks, to evaluate the nature and extent of those risks and to manage them effectively by:

- Establishing appropriate mechanisms for reporting fraud risk issues and significant incidents of fraud
- Making sure that all staff is aware of the Partnership's anti-fraud policy and understand what their responsibilities are in relation to combating fraud
- Ensuring that vigorous and prompt investigations are carried out if fraud occurs or is suspected
- Ensuring that appropriate legal and/or disciplinary action is taken against perpetrators of fraud
- Ensuring that appropriate action is taken to minimize the risk of similar frauds occurring in future

The Internal Audit function is responsible for the following:

- Assisting in the deterrence and prevention of fraud by examining and evaluating the effectiveness of controls commensurate with the extent of the potential exposure/risk in the various activities of the department's operations
- Ensuring that management has reviewed its risk exposure and identified the possibility of fraud as a business risk
- Assisting management in conducting fraud investigations.

Each employee is responsible for the following:

- Acting with propriety in the use of resources and the handling and use funds whether they are involved with cash or payments, receipts or dealing with suppliers. Staff should not accept gifts, hospitality or benefits of any kind from a third party which might be seen to compromise their integrity
- Being alert to the possibility that unusual events or transactions could be indicators of fraud
- Reporting details immediately through the appropriate channel if they suspect that a fraud has been committed or see any suspicious acts or events and
- Co-operating fully with whoever is conducting internal checks, reviews or fraud investigations.

5 PROHIBITED ACTIONS, RED FLAGS, WARNING SIGNS

5.1 Providing Advantages

- No Personnel or any Third Party Associate shall directly or indirectly, give, offer, promise, request or approve a payment of Anything of Value or any other advantage to a Government Official, in order to influence any act or decision of the Government Official in their official capacity for the purpose of obtaining or retaining business for or with Thinkproject, or securing any improper business advantage
- No Personnel or any Third Party Associate shall directly or indirectly, give, offer, promise, request or approve a payment of Anything of Value or any other advantage to a Commercial Party, in order to obtain or retain business for the Thinkproject or any improper commercial advantage or benefit for the Partnership
- No Personnel or any Third Party Associate shall directly or indirectly, give, offer, promise, request or approve a payment in circumstances where they have any reason to suspect that any portion of that payment will be used for any of the purposes described above
- No Personnel or any Third Party Associate shall directly or indirectly, receive or agree to receive Anything of Value or other advantage that may reasonably be regarded as a bribe.

The prohibition on bribery applies to the giving of anything of value, not only money. This includes also providing business opportunities, favourable contracts, stock options, gifts and entertainment.

5.2 Facilitating Payments

Facilitating payments are modest payments made for the purpose of expediting or facilitating the provision of services or routine non-discretionary government action which a Government Official is normally obliged to perform. Making facilitating payments of any kind are not permitted under this Policy unless the prior written approval of CEO and CFO has been received.

Where such approval is granted, the Group Director Finance must inform the appropriate supervisor, who must ensure that the payment is accurately recorded in relevant books and records, and that all supporting documentation, including the written approval, is retained in the appropriate files.

5.3 Business Hospitality, Travel, Meals and Gifts

This Policy allows certain exceptions to general anti-fraud principles when paying for entertainment, meals, travel or a gift for a Government Official and/or a Commercial Party. Expenses of this kind are permitted if they are of modest value, reasonable, a matter of simple common courtesy under local custom, incidental to conducting legitimate and bona fide business, building business relationships or showing appreciation, and not used with the aim of exerting improper influence, or the expectation of reciprocity, and always provided that any such expenses payment does not contravene the anti-fraud policy of any Commercial Party involved.

Before offering or receiving any gift and/or entertainment to/from a third party, employees should consider whether it is necessary for them to obtain appropriate management approval and/or approval from the departmental supervisor. It is vital to avoid even the appearance of improper conduct with any Government Official and/or Commercial Party, and if in doubt, please seek guidance to the departmental supervisor or avoid making any such payment.

5.4 Indirect Payments via Third Parties – red flags

Some acts (e.g. FCPA) prohibits corrupt payments made indirectly through an agent or other intermediary such as a consultant acting for or on behalf of related parties. Under the Act, it is unlawful to make a payment of anything of value to any person, knowing that all or any portion of the payment will be offered, given, or promised to a government official or any other person for a corrupt purpose. The term "knowing" includes conscious disregard, deliberate ignorance, and wilful blindness. In other words, individual employees may violate the FCPA if they have "reason to know" or "should have known" that an agent will bribe a government official.

Accordingly, the most important step to protect ourselves from liability for improper payments made by third parties is to choose carefully our business partners, including agents and consultants.

The U.S. Justice Department has identified certain circumstances that may suggest reason to know of an illegal payment made by an intermediary. These "red flags" warrant further investigation when selecting or working with a third party. The following are examples of red flags:

- The transaction involves a country known for corrupt payments;
- The Third Party has a close family, personal or professional relationship to a government official or relative of an official;
- The Third Party objects to anti-corruption representations in Partnership agreements;
- The Third Party requests unusual contract terms or payment arrangements that raise local law issues, such as a payment in cash, payment in another country's currency, or payment in a third country;
- The Third Party is suggested by a government official, particularly one with discretionary authority over the business at issue;
- The Third Party's commission or fee exceeds fair and reasonable compensation for the work to be performed.

In all cases, whether or not any of these red flags are present, consult and seek approval from the CEO and CFO before entering into any arrangement with a Third Party which will have contact with a government official.

Due Diligence

Thinkproject should never enter into any relationship with a Third Party which will have substantive interaction with government officials without an inquiry into the third party's background, qualifications and reputation.

Any issues raised during this due diligence review must be addressed to the satisfaction prior to entering the relationship. The amount of time and effort required for due diligence will depend on the number and complexity of issues raised during the review process.

Management should inform and seek for approval from CEO/CFO once it has identified a third party which will have substantive interaction with government officials.

5.5 Warning signs for fraud

There are warning signs that can indicate a fraud may be taking place, these can include:

- Staff under stress without a high workload
- Reluctance to take annual leave
- Being first to arrive in the morning and last to leave in the evening
- Refusal of promotion
- Unexplained wealth
- Sudden change of lifestyle
- Suppliers/ contractors who insist on only dealing with one staff member
- A risk taker or rule breaker
- Disgruntled at work / not supportive of Conciliation Resources mission

Fraud Indicators can include:

- Staff exhibiting unusual behaviour (see list above)
- Missing key documents (invoices/ contracts)
- Inadequate or no segregation of duties
- Documentation which is photocopied or missing key information
- Missing expenditure vouchers
- Excessive variations to budgets / contracts
- Bank and ledger reconciliations not regularly preformed and cannot be balanced
- Numerous adjustments or exceptions
- Overdue pay or expense advances
- Duplicate payments
- Ghost employees on payroll
- Large payments to individuals
- Crisis management coupled with a pressured work environment
- Lowest tenders or quotes passed over without adequate explanation
- Single vendors
- Climate of fear / low staff morale
- Consistent failure to implement key controls
- Management frequently overriding controls

6 RECORDKEEPING AND REPORTING REQUIREMENTS

Some Acts and laws (The U.S Foreign Corrupt Practices Act (FCPA) and U.K. Bribery Act impose) strict accounting requirements. In particular, the FCPA requires:

- The keeping of books and records that, in reasonable detail, reflect the transactions and asset dispositions, and
- The development and maintenance of a system of internal accounting controls including periodic audits.
- Each Employee is personally accountable for the accuracy of his or her records and reports. Accurate information is essential to ability to meet legal and regulatory obligations and all reports must be made honestly, accurately and in reasonable level of detail.

To comply with these requirements, **all accounting related employees** must:

- Follow the accounting requirements as set out in the Company's Accounting Manual
- Accurately record all transactions, even when the transaction might laws or regulations
- Accurately record all payment receipts and requests with sufficient detail to permit full transparency
- Never agree to requests for false invoices or for payment of expenses that are unusual, excessive, inadequately described, or otherwise raise questions under these guidelines and
- Never make any payments to anonymous (i.e., "numbered") accounts that are in the name of neither the payee nor an entity known to be controlled by the payee.

7 RAISING A CONCERN – WHISTLEBLOWER CONTACT

If you believe that there has been a violation (or an intention to do so) of this Policy, you may, at any time, talk to your supervisor, manager, or Legal Compliance Officer to seek initial advice, information, or guidance. You can also make a formal complaint to the individuals as mentioned above.

If you do not feel comfortable raising a concern internally, you may use the independent Thinkproject external whistleblower contact:

https://Thinkproject.integrityline.com/

To ensure your anonymity, you must do the following: If possible, do not report from a PC provided by your employer. Do not use a PC that is connected to the company's network/intranet. Access the reporting system directly by copying or writing the URL address in an internet browser rather than clicking on a link. Do not write your personal details.

or internally

Head of Compliance
Peter Mezger
Tel. +49 175 2085579
peter.mezger@Thinkproject.com

The efficient and effective processing of reports is guaranteed as well as strictest confidentiality, particularly the anonymity of the employee, for reports of any kind.

8 INVESTIGATION AUTHORITIES AND RESPONSIBILITIES

8.1 Responsibility for the investigation

The CFO is the Chairman of the Audit Committee, which has the primary responsibility for the investigation of all suspected fraudulent acts as defined in the policy. If the investigation substantiates that fraudulent activities have occurred, these will be reported to appropriate designated personnel and, if appropriate, to the Board.

Decisions to prosecute or refer the examination results to the appropriate law enforcement and/or regulatory agencies for independent investigation could also be made in conjunction with legal counsel and senior management.

8.2 Authorization for investigating suspected fraud

Members of the Investigation team will have:

- Free and unrestricted access to all records and premises, whether owned or rented.
- The authority to examine, copy, and/or remove all or any portion of the contents of files, desks, cabinets, and other storage facilities on the premises without prior knowledge or consent of any individual who might use or have custody of any such items or facilities when it is within the scope of their investigation.

9 NON COMPLIANCE

Any Thinkproject employee or contractor, who violates this Policy may be subject to appropriate disciplinary action, independently from potential other penalties resulting from their behaviour.

Internal Audit shall conduct regular checks on local businesses to ensure compliance with Laws.

10 DOCUMENT CONTROL

Version	Date	Author	Approved by	Details of changes made
001	1.7.22	Peter Mezger	Ralf Grüßhaber	First version