

FRAUD POLICY OF NORGINE

1. POLICY STATEMENT

It is the policy of Norgine B.V. and its affiliates (excluding any entity above the level of Spinnaker Topco Limited) (collectively, “**Norgine**”) to comply with all applicable laws in all countries in which Norgine does business, both directly and indirectly through a third party (as defined below) relating to fraud.

This Policy addresses fraud, what it is and our responsibilities to protect Norgine and what we must do if we become aware of an instance of fraud. This Policy should be read in combination with the Norgine Business Code, Anti-Bribery and Corruption Policy, Anti-Money Laundering Policy and Whistleblowing Policy.

Norgine takes a zero-tolerance approach to fraud and undertakes to ensure that opportunities for fraud are reduced to the lowest possible level of risk through the policies and controls we have in place. We are committed to acting professionally, fairly, and with integrity in all our business dealings and relationships wherever we operate, and to implementing and enforcing effective systems and controls to prevent fraud. This includes being mindful to changes in the business to make sure our systems and controls remain effective and fit for purpose.

2. ABOUT THE POLICY

The purpose of this Policy is to set out Norgine’s expectations and rules concerning the prevention of fraud, and to demonstrate Norgine’s commitment to operating within the requirements of all applicable fraud laws, including by:

- (a) setting out the responsibilities of Norgine Personnel in observing and upholding Norgine’s requirements on preventing fraud;
- (b) providing information and guidance on how to recognise and avoid fraud and respond appropriately if fraudulent activity is uncovered or suspected; and
- (c) implementing and enforcing effective systems and controls to mitigate the risk of fraud.

In this Policy, “**third party**” means any individual or entity that Norgine Personnel come into contact with during the course of their work for or on behalf of Norgine, and includes actual and potential clients, customers, agents, partners, distributors, licensees, contractors, suppliers, professional advisers, consultants, business contacts, and government and public bodies, including their advisers and representatives, officials, politicians and political parties.

3. WHO MUST COMPLY WITH THIS POLICY AND HOW WILL IT BE COMMUNICATED?

This Policy applies to all directors, officers and employees of Norgine (whether their role is permanent or temporary) and Genpact personnel (collectively, “**Norgine Personnel**”).

Norgine Personnel will be provided with a copy of this Policy on or before on-boarding/the start of Norgine’s engagement with them and as appropriate after that. A copy of this Policy is

also available on Norgine's DMS/TMS training platform, Norgine's Compliance SharePoint site and on Norgine's website.

Our zero-tolerance approach to fraudulent activity must be communicated to, and a copy of this Policy must be shared with, third parties on a risk-based approach at the outset of our business relationship with them and as appropriate after that.

4. VIOLATIONS OF THIS POLICY

Any Norgine Personnel who violate this Policy will face disciplinary action, which could result in dismissal or termination of their relationship with Norgine.

Violations of this Policy may also constitute violations of applicable laws relating to fraud and the prevention of fraud and so expose (i) Norgine to, without limitation, criminal sanctions, unlimited fines, loss of reputation, the termination of business relationships, and exclusion from contracts, and (ii) Norgine Personnel and other third parties to, without limitation, fines, imprisonment, and loss of reputation.

5. WHO IS RESPONSIBLE FOR THIS POLICY?

The Board of Directors of Spinnaker Topco Limited has overall responsibility for ensuring that this Policy complies with our legal and ethical obligations, and that all Norgine Personnel comply with it.

Norgine's Compliance Management Committee has primary and day-to-day responsibility for implementing this Policy, for monitoring the Policy's use and effectiveness (including a documented annual review) and for auditing internal control systems and procedures to ensure that they are effective in preventing/minimising the possibility of fraud.

Management at all levels are responsible for ensuring that those reporting to them understand and comply with this Policy and are given adequate and regular training on it as is deemed appropriate.

It is the responsibility of Norgine Personnel to act honestly and with integrity at all times and to safeguard Norgine's reputation and assets for which they are responsible.

6. WHAT IS FRAUD?

For the purposes of this Policy:

"Fraud" is a form of corruption that includes any unlawful or illegal intentional or deliberate act or omission that misleads, or attempts to mislead, in order to obtain a financial or other benefit or to avoid an obligation or incurring an obligation. Fraud can also take the form of manipulation of financial information or accounting records.

The term fraud is often used to describe acts such as deception, forgery, extortion, corruption, theft, embezzlement, misappropriation, false representation, concealment of material facts, misrepresenting financial statements and collusion. For the purpose of this Policy, fraud may be defined as the use of deception with the intention of obtaining an advantage or causing loss to Norgine or another party.

There is a material risk that the criminal offence of fraud or failing to prevent fraud may be committed by Norgine where an "associated person" of Norgine – such as any Norgine Personnel or any other person (including any third party) performing services for or on behalf of Norgine – commits fraud by false representation, by failing to disclose information or by abuse of power, with the intention to benefit Norgine or any person who receives goods or

services from Norgine¹. For the offence to arise, Norgine does not itself have to commit fraud; the fact that the “associated person” does so creates the liability for Norgine.

7. YOUR RESPONSIBILITIES

Norgine Personnel must:

- (a) read, understand, comply with, and avoid any activity that might lead to a violation of, this Policy;
- (b) prevent and detect fraud, including by monitoring for potential “red flags” (as defined below); and
- (c) report any suspected or actual violations of applicable fraud and/or prevention of fraud laws and/or this Policy (see Section 11 ([Mandatory] reporting) for further details).

A “**red flag**” is a fact pattern, situation, request, or other circumstance that indicates a possible fraud or risk of fraud. In some circumstances, further enquiries may confirm why there is a potential red flag. Further enquiries and the responses to them must be documented and the information provided to the Chief Legal Officer and/or Chief Financial Officer (or, if unavailable, another member of the Legal Department and Group Financial Controller). In other circumstances, concerns may still exist or Norgine Personnel may be unsure as to what steps to take. In case of doubt as to whether a certain fact or information known to Norgine Personnel constitutes a “red flag”, the matter should still be raised with the Chief Legal Officer and/or Chief Financial Officer (or, if unavailable, another member of the Legal Department and Group Financial Controller).

Please see the “red flags” listed in the Appendix 1 (*Red Flags – Potential Risk Scenarios*), which provide illustrative examples of situations that may arise during the course of performing due diligence or other services for or on behalf of Norgine which relate to fraud or suspected fraud.

Management are responsible for ensuring that the required Financial Controls are adequate and complied with as per Appendix 2, Clause 1 (*Financial Controls*). All Norgine employees are as per Appendix 2, Clause 2 (*Financial Controls*).

8. WHAT YOU MUST NOT DO

It is not acceptable for Norgine Personnel (or someone on behalf of Norgine Personnel) to:

- (a) engage, or attempt to engage, in any form of fraud;
- (b) aid, abet, counsel or procure the commission of fraud by another person;
- (c) fail to promptly report any request or demand from any third party to commit an act of fraud (or any attempt of the same) by another person, in accordance with this Policy;
- (d) engage in any other activity that might lead to a violation of this Policy; or
- (e) threaten or retaliate against another individual who has refused to commit a fraud or who has raised concerns under this Policy.

¹ A company will not commit the offence if it is the target or victim of the intended fraud.

9. POLICY ON FRAUD:

Norgine's policy on fraud is as follows:

- (a) Engaging in transactions or activities which you know or suspect constitute fraud is strictly prohibited.
- (b) If Norgine Personnel are asked to make payments/provide anything of value to, or receive payments/anything of value from, third parties for or on behalf of Norgine, they must always:
 - (i) follow Norgine's policies with regards to procure-to-pay specifically ensuring engagement of the Procurement team in accordance with the specific policies in place and not committing the company to any payments without ensuring such expenditure has been appropriately approved in accordance with Norgine authority level – no payments should be made without an approved Purchase order or by exception an appropriately approved Manual Payments Request form;
 - (ii) consider the purpose and whether the request is proportionate to the goods or services being provided (including following Norgine's policies with regards to payments to Healthcare Professionals, Healthcare Organisations, Patient Organisations and Charitable Donations);
 - (iii) maintain appropriate records which evidence the business reason for making/receiving payments/anything of value; and
 - (iv) (where applicable) obtain/request a receipt.
- (c) Invoices received from third parties should be checked to ensure that (a) they accurately reflect the services performed, and (b) there is no indication of improper payments being made.

10. DUE DILIGENCE

As mentioned in Section 6 (*What is Fraud?*), third parties performing services for or on behalf of Norgine can create liability for Norgine in respect of the offences of fraud or failing to prevent fraud. It is therefore very important that risk-based due diligence is conducted on third parties prior to engagement. When considering engaging third parties, Norgine Personnel **must** refer to and follow the "*Instructions for Norgine Compliance & Financial Assessments*" document, which sets out Norgine's due diligence procedure.

11. MANDATORY REPORTING

11.1 Why report?

The success of this Policy in preventing fraud relies on the diligence and commitment of all Norgine Personnel, who have a responsibility to report any suspected or actual fraud and/or violations of this Policy, and should do so without fear of any form of retaliation. It is important to report even small instances of fraud, as these may be part of a pattern which leads to uncovering a larger fraud which may not on its own be apparent. There is no acceptable *de minimis* fraud level.

11.2 When to report?

Norgine Personnel must notify the Chief Legal Officer and/or Chief Financial Officer (or, if unavailable, another member of the Legal Department and Group Financial Controller) or raise a concern as provided for in the Norgine Whistleblowing Policy as soon as possible, if they:

- (a) encounter a situation or are considering a course of action where the appropriateness is unclear; or
- (b) are aware of any suspected or actual fraud and/or violations of this Policy (or any other applicable Norgine policies).
- (c) Time is of the essence to ensure that Norgine are able to take any necessary steps in protecting itself from further financial losses or other adverse consequences including blocking payments to a suspected party, removing approval rights from an employee suspected of wrongdoing, ceasing trading with a party who is suspecting of wrongdoing and making notifications as required by the applicable laws and regulations governing Norgine.

11.3 What to do after making a report?

After making a report, Norgine Personnel should take no further action (such as paying a questionable invoice, filling a suspicious order etc.) without further instruction. The individual should also not communicate their suspicions of the fraud to anyone else, including the suspected individual.

The Chief Legal Officer and/or Chief Financial Officer (as applicable) will consider the circumstances, including whether a report should be made internally to relevant Norgine committees or to the relevant authorities, and decide on the appropriate next steps. This determination will consider:

- (a) The size of the potential fraud
- (b) the complexity
- (c) The impact on customers or suppliers
- (d) The involvement of Norgine Personnel and/or third parties
- (e) The reputational impact
- (f) Any potential legal considerations

11.4 What happens after making a report?

The Chief Legal Officer and/or Chief Financial Officer (as applicable) or their respective delegate will investigate all reports promptly and with the highest degree of confidentiality that is possible under the specific circumstances. No Norgine Personnel may conduct any preliminary investigation, unless authorised to do so by the Chief Legal Officer and/or Chief Financial Officer (as applicable). Cooperation by Norgine Personnel in the investigation will be expected. As needed, the Chief Legal Officer and/or Chief Financial Officer (as applicable) will consult with the Legal Department, the Human Resources Department, the Finance Department and/or the Compliance Management Committee. If needed Norgine may bring in external advisors to support with the investigation. It is Norgine's policy to employ a fair process by which to determine violations of this Policy.

11.5 What happens after an internal investigation?

If any investigation indicates that a violation of this Policy has probably occurred, Norgine will take such action as it believes to be appropriate under the circumstances, which may include disciplinary action (including dismissal or termination of the relationship) against any Norgine Personnel involved in the breach.

If, upon further investigation of a suspicious transaction, the Chief Legal Officer and/or Chief Financial Officer (as applicable) determines that the transaction is designed to involve the use of Norgine to commit or enable fraud or another illegal activity, they will recommend to the Compliance Management Committee that Norgine terminate, withdraw from, or refuse to consummate such transaction, as appropriate. The final decision rests on the Compliance Management Committee (subject to any shareholder consent where required).

12. SAFEGUARDS AGAINST RETALIATION

In accordance with our “Safe to Speak Up” approach, Norgine encourages openness and will support anyone who raises genuine concerns in good faith, even if those concerns turn out to be mistaken. As set out in the Norgine Business Code and the Norgine Whistleblowing Policy, Norgine has put in place procedures to encourage Norgine Personnel to report known or suspected wrongdoing as soon as possible, in the knowledge that their concern will be taken seriously and investigated as appropriate, and that their confidentiality will be respected.

It is understandable that Norgine Personnel who raise concerns or report another’s wrongdoing are sometimes worried about possible repercussions. Norgine Personnel must not suffer, and Norgine takes a zero-tolerance approach to, any detrimental treatment as a result of raising a concern, including threats and attempts of retaliation. Detrimental treatment includes suspension or dismissal, disciplinary action, coercion, intimidation or harassment, withholding of promotion, permanent position or training, demotion or change in duties or other working conditions, discrimination, or other unfavourable or unfair treatment connected with raising a concern. If you believe that you have suffered any such treatment, you should inform your Line Manager, the HR Department or one of the Internal Reporting Channels designated under the Norgine Whistleblowing Policy immediately. If the matter is not remedied, you should raise it formally using the respective local Grievance Procedure. Norgine will take prompt disciplinary action (which may include dismissal or termination of the relationship) against any Norgine Personnel who retaliate against other Norgine Personnel for having raised a concern.

13. TRAINING

Training on this Policy forms part of the induction process for all Norgine Personnel, and regular training will be provided as necessary. Such training may form part of wider financial crime detection and prevention training.

14. QUESTIONS ABOUT THIS POLICY

If Norgine Personnel have any questions about this Policy or Norgine’s expectations, they should contact their Line Manager, the relevant Department Head and/or the Compliance Management Committee.

APPENDIX 1: RED FLAGS – POTENTIAL RISK SCENARIOS

The following is a list of possible red flags that may arise in connection with due diligence of, or dealings with, third parties which relate to fraud and the prevention of fraud which merit further enquiry. The list is not intended to be exhaustive and is for illustrative purposes only.

- (a) You become aware that a third party has made, or intends to make, a false statement or representation.
- (b) You become aware that a third party has failed to disclose information or intends to deliver false documentation, or has set up or intends to set up a structure to try to hide income, gains or assets.
- (c) You become aware that a third party has deliberately failed to register for VAT (or the equivalent tax in the relevant jurisdiction) or failed to account for VAT.
- (d) A third party requests payment in cash and/or refuses to sign a formal commission or fee agreement, or to provide an invoice or receipt for a payment made.
- (e) You become aware that a third party working for Norgine as an employee, or a prospective employee, asks to be treated as a self-employed contractor, but without any material changes to their working conditions.
- (f) A supplier or other subcontractor is paid gross when they should have been paid net.
- (g) A third party requests that payment is made to a country or geographic location different from where the third party resides or conducts business.
- (h) A third party to whom Norgine has provided services requests that their invoice is addressed to a different entity, where we did not provide services to such entity directly.
- (i) A third party to whom Norgine has provided services asks us to change the description of services rendered on an invoice in a way that seems designed to obscure the nature of the services provided.
- (j) You receive an invoice from a third party that appears to be non-standard or customised. For example, the invoice from the third party differs in material respects from those previously supplied by the third party, with no explanation provided for the change.
- (k) A third party insists on the use of side letters or refuses to put terms agreed in writing or asks for contracts or other documentation to be backdated (without justification).
- (l) A third party requests or requires the use of an agent, intermediary, consultant or supplier that is not typically used by or known to us.
- (m) You receive payment instructions which contain discrepancies in the customer information, e.g. multiple customers with different names using the same contact information.
- (n) You are asked to process payments not in accordance with Norgine's normal policies and procedures.
- (o) You are asked to not record or report transactions (e.g. sales invoices, supplier invoices) not in accordance with Norgine's normal policies and procedures.

APPENDIX 2: FINANCIAL CONTROLS

1. Management is responsible for:

- (a) Assessing the types of fraud risk involved in the operations for which they are responsible.
- (b) Implementing an effective control environment to prevent fraud.
- (c) Reviewing the controls for which they are responsible regularly to ensure these remain fit for purpose.
- (d) Reporting all incidents of Fraud to any of the Compliance Manager, Senior Director, Due Diligence, the Chief Financial Officer or Chief Legal Officer .
- (e) Ensuring that vigorous and prompt investigations are carried out if fraud occurs or is suspected.
- (f) Implementing new controls to reduce the risk of similar fraud occurring where frauds have taken place.

2. All Norgine Personnel are responsible for:

- (a) Being alert to the possibility that unusual events or transactions could be indicators of fraud.
- (b) Reporting details immediately through the appropriate channel if they suspect that a fraud has been committed or see any suspicious acts or events.
- (c) Application of key controls in management of the following areas to minimise opportunities for fraud:
 - (i) **Cash and bank accounts:** through period end reconciliations, authorisation of payments, ensuring mandates are up to date and monitoring levels of cash held in our businesses. Ensuring all changes to bank mandates or opening of new bank accounts is done in accordance with the Group's Treasury Manual.
 - (ii) **Assets:** to ensure that purchase, disposal and general security over assets are appropriately managed, approved and accounted for through the asset lifecycle.
 - (iii) **Third Party Partners:** to ensure that they are appointed and managed in accordance with our *Instructions for Norgine Compliance & Financial Assessments*".
 - (iv) **Sales contracts:** to ensure that they are agreed and signed off at the appropriate levels of authority in accordance with the Contract Approval and Signing Form and authorised signatory delegations.
 - (v) **Purchase contracts:** to ensure that Norgine's procurement policies are followed at all times.
 - (vi) **Invoicing and credit notes:** to ensure that there is appropriate authorisation and segregation of duties in the raising and approval of invoices and credit notes.
 - (vii) **Debt management:** to ensure that we collect monies due from our customers appropriately.
 - (viii) **Expenses Claims:** to make sure that expenses are supported by receipts and are submitted in accordance with the Global Expense Policy.
 - (ix) **Payroll:** employee details should be accurate, processing is secure with appropriate segregation of duties and payroll payments are reviewed and authorised.

- (x) **Financial reporting & management:** operation of sound financial reporting processes and following Norgine's guidance and policies in this area. Also, from preparation of key account reconciliations and their review, preparation and posting of journals and review of the Monthly Management pack by Finance and the Executive Committee.
- (xi) **Physical access and security controls:** preventing unauthorised access into our buildings and protection of our assets.
- (xii) **General IT access controls (including to financial systems)** such as JD Edwards to ensure that access to systems is appropriate, monitored and managed.
- (xiii) **Information security controls:** to ensure that our IT systems are reliable, resilient and recoverable.

3. **Upon termination of Employment:**

When Norgine Personnel leave Norgine's employment, all physical access permissions and computer passwords must be revoked immediately and all company property and assets must be returned (e.g. company identity card, security access card/keys, mobile telephones, laptops etc). When an employee is suspended, physical access permissions and computer passwords must be revoked. Bank mandates, company signature lists, directorships, and delegated authorities must be changed or cancelled.