ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICY
OF
NORGINE
LAST UPDATED: 3 JULY 2023

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 anti-money laundering ("**AML**") and counter-terrorist financing ("**CTF**") laws and regulations in all countries in which Norgine does business, both directly and indirectly through a third party (as defined below). This Policy addresses what we must do in order to comply with those laws and regulations. This Policy should be read in combination with the Norgine Business Code.

Norgine takes a zero-tolerance approach to money-laundering and terrorist financing. 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 counter money laundering and terrorist financing.

2. About this Policy

The purpose of this Policy is to set out Norgine's expectations and rules concerning the prevention, detection, and reporting of money laundering and counter-terrorist financing, and to demonstrate Norgine's commitment to operating within the requirements of all applicable AML and CTF laws and regulations, including by:

(a) setting out the responsibilities of Norgine Personnel in observing and upholding Norgine's requirements on preventing money laundering and terrorist financing; and

(b) providing information and guidance on how to recognise and avoid money laundering and terrorist financing and respond appropriately if money laundering or terrorist financing is uncovered.

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) (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 eGSOP training platform, Norgine's Compliance SharePoint site and on Norgine's website.

Our zero-tolerance approach to money-laundering and terrorist financing 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 AML and CTF laws and regulations and so expose (i) Norgine to, without limitation, criminal sanctions, significant 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 money laundering and terrorist financing.

Management at all levels is 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.

6. What is money laundering and terrorist financing?

The broad scope of AML and CTF laws and regulations means that lawfully operating companies such as Norgine may interact with third parties seeking to launder the proceeds of criminal activity. Criminals may seek to involve Norgine at any stage in the money laundering and terrorist financing process, for example by using illegal funds to purchase goods and services.

For the purposes of this Policy:

> "**Money laundering**" is the practice of concealing or disguising the origins of proceeds derived from criminal activity by creating the appearance that the proceeds are derived from a legitimate source. The underlying criminal activity can include obvious crimes such as drug trafficking, fraud, bribery or organised crime. In some jurisdictions, it can also include tax evasion, export control offences or regulatory crimes.
>
> If successful, money laundering sustains a variety of criminal or terrorist activities by allowing criminals to maintain control over and use their illicit funds, oftentimes to finance additional criminal activity, and to prevent their illegal activities from being detected. Various jurisdictions have enacted AML laws directed at preventing the use of the financial system for money laundering, terrorist financing, and other financial crimes.
>
> "**Terrorist financing**" is often linked to money laundering. Money laundering is generally intended to obscure the origin of illicit funds. Although terrorists may launder money gained from illegal activities such as drug trafficking, the focus of terrorist financing is on which activities the funds are used for.

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 money laundering and terrorist financing, including by monitoring for potential "red flags" (as defined below); and

(c) report any suspected or actual violations of applicable AML and CTF laws and regulations and/or this Policy (see Section 10 (*Mandatory reporting*) for further details).

A "**red flag**" is a fact pattern, situation, request, or other circumstance that indicates a possible money laundering or terrorist financing risk. 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 or Chief Financial Officer (or, if unavailable, another member of the Legal Department). 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 be raised with the Chief Legal Officer or Chief Financial Officer (or, if unavailable, another member of the Legal Department).

Please see the "red flags" listed in the Appendix (*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 money laundering and terrorist financing.

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 money laundering or terrorist financing;

(b) aid, abet, counsel or procure the commission of money laundering or terrorist financing by another person;

(c) fail to promptly report any request or demand from any third party to aid, abet, counsel or procure the commission of money laundering or terrorist financing, or any suspected money laundering or terrorist financing (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 engage in money laundering or terrorist financing or who has raised concerns under this Policy.

9. Policy on AML and CTF

Norgine's policy on AML and CTF is as follows:

(a) Engaging in transactions or activities which you know or suspect constitute money laundering or terrorist financing is strictly prohibited.

(b) All payments to and from third parties should be reviewed to ensure that the correct amounts have been transmitted from or to the correct entity or individual and the correct bank account. Whenever a counterparty that receives funds from Norgine wishes to alter their payment details, Norgine must first conduct a thorough review consistent with the Finance Department's policies to understand the reasons for any changes. A counterparty may seek to alter their payment details so as to avoid the new details being subject to the scrutiny of any initial due diligence conducted in respect of that counterparty.

(c) Due diligence must be carried out on third parties in accordance with the "*Instructions for Norgine Compliance & Financial Assessments*" document.

10. Mandatory reporting

10.1 Why report?

The success of this Policy in preventing money laundering and terrorist financing relies on the diligence and commitment of all Norgine Personnel, who have a responsibility to report any suspected or actual violations of applicable AML and CTF laws and regulations and/or this Policy, and should do so without fear of any form of retaliation.

10.2 When to report?

Norgine Personnel must notify the Chief Legal Officer or Chief Financial Officer (or, if unavailable, another member of the Legal Department) 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 a suspected or actual violation of applicable AML and CTF laws and regulations and/or this Policy (or any other applicable Norgine policies).

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

10.4 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. It is Norgine's policy to employ a fair process by which to determine violations of this Policy.

10.5 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 facilitate money laundering, terrorist financing 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).

11. 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.

12. 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.

We will ensure that mandatory training on this Policy is offered to those Norgine Personnel who have been identified as being at risk of exposure to money laundering and terrorist financing, such as those working in finance and procurement, at least annually.

13. 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: 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 money laundering and terrorist financing and which merit further enquiry. The list is not intended to be exhaustive and is for illustrative purposes only.

(a) The counterparty to a transaction or contract is or has been the subject of any known formal or informal allegations (including in the reputable media) regarding possible criminal, civil or regulatory violations or infractions.

(b) The counterparty to a transaction or contract makes unreasonable/unsupported objections to due diligence or AML/CTF representations or warranties being included in the agreement.

(c) The counterparty to a transaction or contract does not reside or have a significant business presence in the country where the service is to be provided or goods are to be supplied.

(d) Recommendations to rely on the customer's and/or an intermediary's due diligence without written evidence of what that due diligence has encompassed or the written results of the due diligence.

(e) Requests that funds be transferred to a third party, such as an unrelated party, or to a jurisdiction other than the one in which the party is located, particularly if located in an "offshore" bank secrecy jurisdiction or tax haven.

(f) The placing of large orders or significant overpaying of an invoice followed by a request for a refund.

(g) Requests for payments that cannot plausibly be justified vis-à-vis the role undertaken.

(h) The use of a shell company or some other non-transparent corporate structure.

(i) The use of nominees or proxies with no obvious commercial purpose.

(j) The suggestion of a complicated or unclear payment or transaction structure, with no adequate rationale for the suggestion.