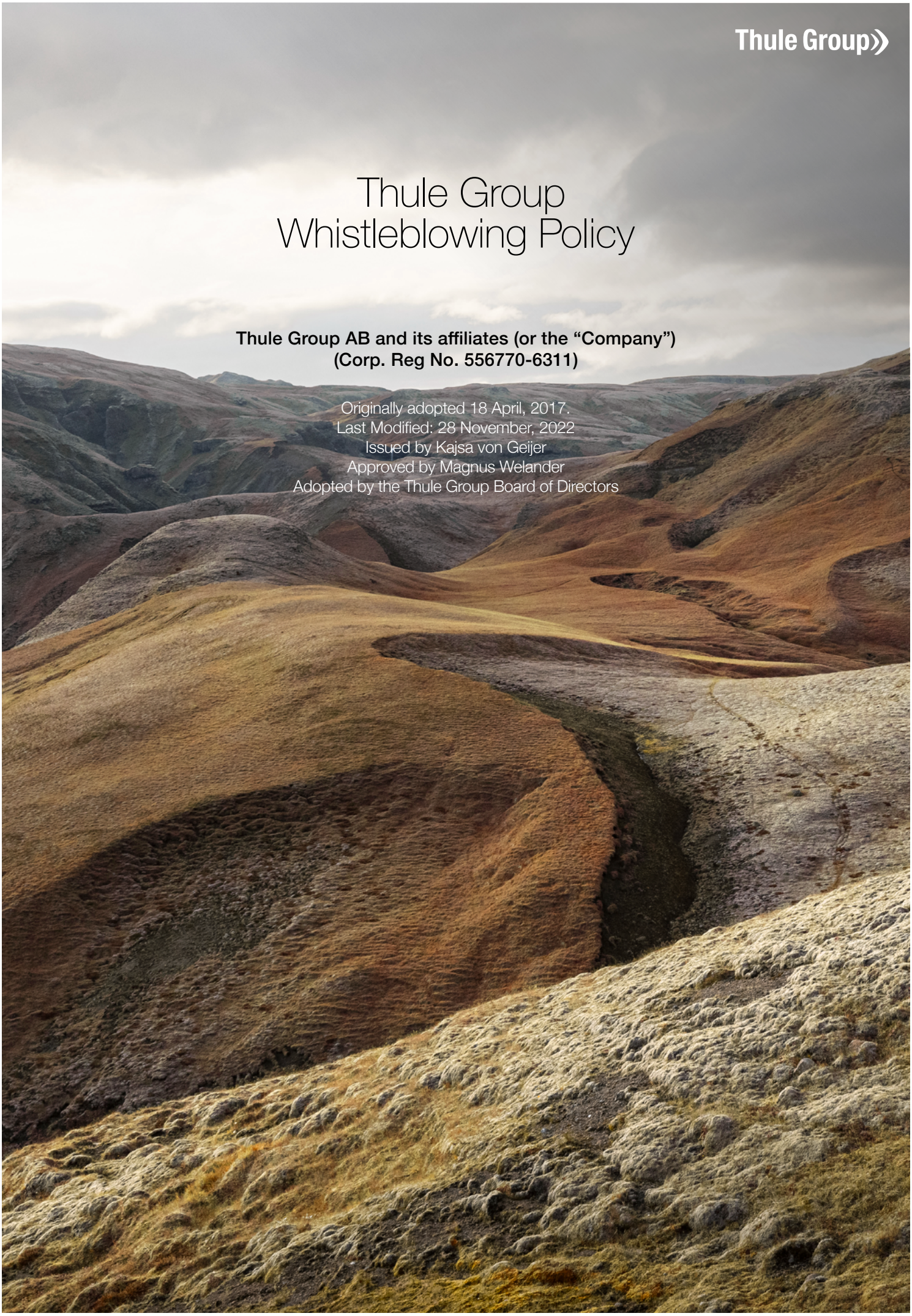

Thule Group Whistleblowing Policy

Thule Group AB and its affiliates (or the "Company")
(Corp. Reg No. 556770-6311)

Originally adopted 18 April, 2017.
Last Modified: 28 November, 2022
Issued by Kajsa von Geijer
Approved by Magnus Welander
Adopted by the Thule Group Board of Directors

Introduction

This whistleblowing policy, which is drafted in line with the principles articulated in the Company's Code of Conduct, is a vital part of the Company's Corporate Compliance Program.

Employees are often the first to discover misconduct at their workplace, and it is important that an employee who discovers wrongdoing by the Company or any of its employees, consultants, contractors, or suppliers is able to report the event without risk of retaliation or discrimination.

The purpose of this policy is to encourage employees to raise concerns about matters occurring within or related to the Company, rather than overlooking a problem or seeking a resolution of the problem outside the Company.

This policy applies to **everyone at the Company** – all employees, managers, executive officers, and members of the board of directors *(all of whom are included in the term "employees" as used in the remainder of this policy)*.

The Company's whistleblowing system also allows for **external partners and stakeholders** to file a complaint. Consequently, this policy also applies for these matters and reports.

The Whistleblowing System

In order to allow employees to raise concerns about wrongdoing, the Company has established a whistle-blowing system that serves as a contact interface designed specifically for receiving and handling employees' reports on suspected misconduct. The whistleblowing system is a channel for receiving reports and conduct follow-ups which are designed, established and operated in a secure manner that ensures that the confidentiality of the identity of the reporting person and any third party mentioned in the report is protected and prevents access thereto by non-authorized staff members.

However, laws and regulations on protection of personal data set limitations on the circumstances under which a company may process information indicating that one of its employees has been involved in suspected misconduct.

For this reason, the whistleblowing system may only be used in the following circumstances:

Only serious misconduct may be reported through the whistleblowing system. Serious misconduct involves irregularities or improper actions concerning the Company's vital interests or individuals' health and safety. This may for example include:

1. financial crime and accounting irregularities;
2. the offering or acceptance of bribes;
3. environmental risks or crimes;
4. security vulnerabilities which constitute a risk for employees' or customers' health or safety;
5. serious forms of harassment or discrimination;
6. violations of the Company's Supplier Code of Conduct; or
7. violations of the Company's Code of Conduct.

The whistleblowing system should only be used to the extent that it is justified not to turn to the Company's internal information and standard reporting channels, as described in this policy. This may for example be the case when the reported person is part of the management or the suspected misconduct, for that or other reasons, runs the risk of not being properly handled .

The whistleblowing system complements the Company's internal information and standard reporting channels and is available for use on a voluntary basis.

Who may report a misconduct?

To report a concern related to an issue which fits the description above, the reporting person shall use the Whistleblowing reporting system, which is found HERE.

Depending on the reporting person's geographical location and what local legal entity the reporting person belongs to, separate local reporting channels will be provided within the Whistleblowing reporting system. If there are uncertainties on what channel to report thru, the Company assures that the reported concern will always be handled in accordance with this Policy in order to care for that the proper investigating activities are initiated.

The reporting person will receive a randomly selected code that will enable them to track the process of the report. The reporting system will automatically erase all information regarding a reported case two months after it was first reported.

It is important that the reporting person include all relevant facts in their report. Claims should be carefully described and all documentation that may be relevant should be attached.

The process

The Company will act upon any concerns raised and conduct a diligent follow-up. Follow-up and feedback will take place within a reasonable timeframe, given the need to promptly address the matter that is the subject of the report.

The Company can assess a concern only after having conducted an initial inquiry and, most likely, after properly investigating the matter in question. If urgent action is required, it will be initiated before any investigation is conducted. Where appropriate, matters raised may:

1. be investigated by management, the board of directors, internal audit, or through the disciplinary process;
2. be referred to the police or other law enforcement authorities;
3. be referred to an independent auditor;
4. be referred to an external advisor; or
5. become the subject of an independent inquiry.

The reporting person will able to report both in writing or orally, and if requested the Company will arrange for a physical meeting within a reasonable time.

The reporting person will, within seven days from filing the report, get a confirmation on that the Company has received the reported matter. The Company will within a reasonable timeframe, and subject to legal constraints, provide relevant feedback to the reporting person, not exceeding three months from the acknowledgment of receipt.

When a complaint is entered into the whistleblowing system, the reporter will receive a key-code to be able to track the reporting of the issue and allow for communication between the reporter and the receiving organization.

The Company will keep records of the reports received, in a way which ensure that the identity of the reporting person is not disclosed to anyone beyond the authorized staff members competent to receive or follow up on the reports.

Reports are not stored for a longer time than it is necessary and proportionate in order for the Company to conduct the necessary follow-up actions and allow for a proper investigation of the reported matter.

Prevention of retaliation

The Company will not tolerate any form of, including attempts and threats, to penalize, or discriminate against, an employee who has used the whistleblowing system to report a genuine concern regarding wrongdoing. Any such retaliation may be subject to disciplinary action by the Company, up to and including termination of employment.

Anonymous reports

Complaints are made anonymously through the whistleblowing system and the whistleblower does not have to reveal its identity. However, it normally facilitates any subsequent investigation and handling of the matter if contact details have been provided. Therefore, the Company encourages employees to provide name and contact details when reporting a complaint.

False and malicious allegations

The Company strives to meet the highest standards of honesty and integrity and will ensure that sufficient resources are put into investigating any complaint received.

However, it is important for any employee considering making allegations to ensure that they are sincere. The making of any deliberately false or malicious allegations may result in disciplinary action.

Standard reporting channels

Employees with a concern related to a person or issue which does not fit the description of matters which may be reported through the whistleblowing system should not use the whistleblowing system.

Instead, employees should raise these issues through their standard reporting channel, which consists of the employee's human resources department. The Company will provide separate reporting channels for this kind of matters. Information on the available internal reporting channels will be published on Thule Group Intranet.

Processing of personal data

Reports made through the whistleblowing system are likely to contain personal data – data which directly or indirectly pertains to an identified or identifiable individual. The personal data may pertain to the person who has made the notification, and/or to a person suspected of the alleged wrongdoing. The types of personal data which may be processed in conjunction with an investigation are typically the following:

- The name, position, and contact details *(for example e-mail and telephone number)* of the employee who submitted the complaint and the individual to whom the compliant relates, as well as any witnesses or other individuals affected.
- Description of the reported matter, including names of any persons involved in the misconduct, as well as date and place.
- Other details, documentation or evidence relating to the reported misconduct.

The Company will only process personal data which is correct and relevant to the investigation. Superfluous personal data will not be processed. Sensitive personal data, such as an individual's race or ethnic origin, political views, religious or philosophical conviction, membership of a trade union, or data relating to an individual's health or sex life, will, as a general rule, not be processed by the Company.

The Company is the data controller of any personal data collected via the whistleblowing system, and is responsible to ensure that the personal data collected is processed in accordance with applicable laws and regulations on data protection.

The details of Thule Group AB *(org. no 556770-6311)* for purposes of its role as data controller are as follows:

How Thule process your personal data

Any personal data collected via the whistleblowing system will be processed for the purpose of administering and investigating allegations raised, and dealing with discovered misconduct, as described in this manual. Thule takes both technical and organizational security measures to protect the personal data processed.

The personal data collected will be processed only by those specifically appointed individuals at Thule who are involved in the investigation and a third party IT service provider engaged by Thule. In this context and for the purpose of investigating the reported matter, personal data may be transferred to a department within Thule *(such as internal audit)*, management, the board of directors, or other persons closely related to Thule.

Thule will generally not disclose the personal data to third parties, however, we will transfer your personal data to our IT service providers, and/or Thule's entities that are established outside of the EU/EEA. When third party services providers and/or Thule's entities process your personal data outside of the EU/EEA, such transfer of personal data will be subject to EU privacy law.

Thule may transfer your data to our external legal counsels, consultants and auditor in connection with the processing of the reported matter. In addition, personal data may be transferred to the police or other relevant authorities.

Legal basis

Thule collects and processes personal data about you for the purpose of pursuing a legitimate interest of the Company, in ensuring compliance with applicable laws throughout all of the Thule's operations and facilitating the provision of information by data subjects from Thule regarding a suspected breach of such compliance and in order to provide a response to the requests made by you which interests in processing the personal data overrides your interests. Under the GDPR this is in accordance with article 6(1) (f).

Thule collect and process personal data about you for the purpose of complying with legal requirement in order to meet a legal obligation imposed by law, by regulation or by community and/or national rules specific for the reported concern if applicable. Under the GDPR this is in accordance with article 6(1) (c).

Time of storage

The personal data which is compiled and processed will not be retained longer than is necessary. Complaints, reports, and information regarding misconduct which have been investigated will as a general rule be deleted within two months of the conclusion of the investigation or, if the investigation results in action being taken against the individual who has been reported, when the information is no longer needed for the purpose of carrying out an investigation and taking action. If it is decided that no investigation will be initiated, the information will be deleted immediately after such decision has been made.

Your rights

When personal data pertaining to an individual is collected via the whistleblowing system, the individual must be informed. If it is not possible to inform the individual immediately, for example if such information could jeopardize Thule's investigation, information will be provided at a point of time where it would no longer constitute a risk to the investigation.

You have the right to ask us for information about or access to your personal data. There are some exemptions, which means you may not always receive all the personal data that we process.

You have the right to object to Thule's processing *(using)* your personal data. This effectively means that you can stop or prevent us from using your personal data. However, it only applies in certain circumstances, and we may not need to stop the processing of your personal data if we can give legitimate reasons to continue using your personal data.

You have the right to ask us to erase your personal data in certain circumstances.

You have the right to ask us to rectify personal data you think is inaccurate. You also have the right to ask us to complete personal data you think is incomplete.

You have the right to ask us to restrict the processing of your personal data in certain circumstances.

If you have any complaints about Thule's processing of your personal data, you may contact Thule Privacy Officer, Kajsa von Geijer, or the Swedish Data Protection Agency.

Related documents

This policy should be read in connection with the following documents.

- Corporate Compliance Program Description
- Code of Conduct
- Data Protection Policy

Malmö January 1, 2023

Thule Group

Magnus Welander
CEO & President

Thule Group HQ
Fosievägen 13
SE – 214 31 Malmö
Telephone: +46 40 635 90 00
www.thulegroup.com