SANCTIONS POLICY

1. INTRODUCTION

1.1 Company Policy

Our Company has implemented clear policies and procedures in order to ensure compliance with all applicable sanction rules. We employ a risk-based approach to sanctions compliance by developing, implementing, and routinely updating our sanctions compliance program. Our Policy entails strict observance of all applicable laws relating to trade restrictions and the fight against terrorism. The Policy is not exhaustive, but provides an insight into and an overview of the legal framework in this area. The trade restrictions relate to cross-border trade in products, money, technology and services. In order to avoid violations of sanctions for the company, it is important to comply with the high standard set by the company through this Policy.

In this Policy, "Business Activities" include investing, financing, concluding contracts, operating, performing services, exporting and importing, as well as other similar activities. “Business Partners” include our contractors, banks, charterers, agents, managers, brokers and other intermediaries and third parties involved in a transaction. Our business partners may expose us to risk by violating trade restrictions and applicable legislation, for example anti-corruption legislation. Accordingly, this Policy should be read and used in conjunction with our Financial Crime Policy, the Know Your Business Partner Policy and the Dow Jones RiskCenter. This Policy must also be read in conjunction with our other compliance policies, including our Audit Committee Charter, Complaints Procedure and Code of Business Ethics and Conduct.

We are cooperating with external counsels as deemed necessary in the implementation and follow-up of our compliance program.

1.2 Your obligations

You must familiarise yourself with applicable sanctions rules and follow the procedures described in this Policy. You should be aware of illicit and suspicious shipping practices and take them into account in the performance of our operations ensuring compliance with applicable sanction rules at all times. Illicit practices include:

- STS[1] transfers used to conceal the origin and nature of the cargo
- AIS[2] dark activity without legitimate reasons
- Financial system abuse[3]
- Falsifying documentation which should accompany maritime transactions
- Concealment of cargo onboard a vessel

This Policy is taking account of such illicit practices in order to minimise the risks of non-compliance with applicable sanction rules.

2. LEGAL FRAMEWORK

Economic sanctions and trade restrictions are measures implemented as a foreign policy response to situations that create international concern.

1 Ship to Ship
2 Automatic Identification System
3 Deliberate attempst to interfere with the operation of the platforms, servers, the purpose of which is use the system(s) limitations to own advantage and to hack and/or deceive and/or cheat on the systems, platform, technical and their settings.

Trade restrictions are penalties or restrictions imposed by a country or a group of countries against another country. The restrictions tend to take the form of import duties, prohibitions on exports or imports of certain goods and technologies, arms embargo, prohibitions on investments or restrictions on the transfer of funds and financing, or other administrative regulations.

In addition to the restrictions imposed on countries, there are international trade restriction rules that may restrict transactions with certain individuals, companies, entities, groups, organisations, etc. This may occur, among other things, on suspicion of complicity in promoting terrorism, unlawful arms trade, organised crime, proliferation of weapons of mass destruction, human rights violations, suspicion of opposing democratic processes in certain countries or suspicion of affiliation with certain governments, such as the former governments of Libya and Liberia. The list of such "restricted persons" or "Specially Designated Nationals" are regularly subject to updates.

Two examples of such lists are «Specially Designated Nationals[4]» and the EU's consolidated list of individuals, groups and entities subject to EU trade restrictions[5].

Sanctions to fight terrorism includes, for example, an obligation to freeze bank accounts or financial instruments controlled or used by individuals affiliated with al-Qaida, Taliban or other terrorists/terrorist groups. The sanctions mainly belong to three categories:

- Sanctions that incorporate UN Security Council decisions into nationallegislation;
- Sanctions adopted by the European Union as part of the common foreign and security policy[6],and
- American sanctions monitored by the U.S. Office of Foreign Assets Control(OFAC)[7],

The shipping industry has been a focus of the US authorities, see OFAC Advisory to the Maritime Petroleum Shipping Community[8] and the Guidance to Address Illicit Shipping and Sanctions Evasion Practices[9]. This Policy is based on the recommendations in the guidance from OFAC.

Typically, the sanctions take the form of import tariffs, export or import bans on certain goods and technology, prohibitions on investments or restrictions on the transfer of funds and financing, or other administrative regulations. By way of example only, Iran is currently subject to trade embargos and there are extensive sanctions imposed by the UK, EU and US against Russia, targeting Russian entities and individuals, banks and products such as coal and crude oil.

Several countries are subject to economic and financial sanctions, currently including Afghanistan, Burundi, Egypt, Eritrea, Yemen, Democratic Republic of Congo, Libya, North Korea, Russia, Belarus, South Sudan and Syria.

3. COMPANY POLICY

Our Policy entails strict compliance with sanctions adopted by the UK, UN Security Council, the EU Council, the US authorities and any applicable national sanction legislation.

[4] http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx

[5] http://eeas.europa.eu/cfsp/sanctions/index_en.htm.

[6] http://eeas.europa.eu/cfsp/sanctions/index_en.htm

[7] http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx

[8] https://www.treasury.gov/resource-center/sanctions/Programs/Documents/iran_advisory_09032019.pdf

[9] Of 14 May 2020, seehttps://www.treasury.gov/resource-center/sanctions/Programs/Documents/05142020_global_advisory_v1.pdf

Adherence with these sanctions will also ensure compliance with relevant sanctions adopted by Norwegian authorities.

Our Company shall not:

- Engage in business that result in violation of applicable sanctions, trade restrictions or export control regulations;
- Engage in business with individuals or legal entities listed on sanctions lists introduced by the UK, the UN, the EU, Norway or the US in violation with applicable sanctions;
- Engage in business with companies located in, owned or controlled by the government of a country subject to OFAC sanctions without the prior consent of our Compliance Officer.

Violations of trade restriction regulations is a criminal offence, and such violations may result in the Company or the employees being subject to investigation. Both intentional and unintentional/negligent violations may be punishable pursuant to applicable regulations.

The penalties that may be imposed on the Company and its employees are severe, and includes fines and imprisonment. A charge may also significantly damage the Company's reputation.

Violation of this Policy may result in dismissal or have other consequences for your employment.

Our Company shall:

- Ensure that an appropriate and effective sanctions and/or trading compliance clause is included in all contracts that may involve a risk of violating sanctions and/or trading restrictions, e.g. in charterparties
- Ensure that charterers warrant the trade is not sanctioned and that cargo does not originate from any sanctioned country
- Ensure that an appropriate "AIS switch-off" or "dark activity" clause is included in all charterparties

For any assistance in respect of the above mentioned contractual clauses, please contact the Compliance Officer.

4. KNOW YOUR BUSINESS PARTNER – INTEGRITY DUE DILIGENCE

When onboarding new Business Partners as part of a business activity for which you are responsible, you must carry out an Integrity Due Diligence («IDD»).

The Company has implemented the Dow Jones RiskCenter for integrity due diligence, screening and monitoring of our Business Partners. This will provide for a structured tracking of Business Partners from onboarding (prior to concluding the contract) throughout the entire lifecycle of the business relationship. Our Know Your Business Partner Policy is part of our risk management aimed at ensuring the integrity of our Business Partners.

A Business Partner could include any entity or individual that our company enters into a business relationship with. We use third party monitoring tools including Infospectrum and Dow Jones RiskCenter for the purpose of carrying out standard IDD checks.

For larger contracts, we apply a combination of the above mentioned tools, as well as more conventional due diligence and background checks. In cases which are potentially high risk,

we use external legal counsel on case by case basis, including for the purpose of carrying out identity/KYC and sanctions checks of relevant entities and individuals.

The Compliance Officer will review the result of the IDD, including assessing and mitigating red flags identified. The Approval Group consists of the Compliance Officer and the CFO. The Approval Group will approve high risk Business Partners and the Compliance Officer will approve low and medium risk Business Partners.

5. MONITORING AND REVIEW

5.1 Annual risk assessment

The Compliance Officer is responsible for conducting an annual assessment of the sanction risks associated with our activities.

The Compliance Officer is responsible for monitoring the implementation of the Sanctions Policy and supplementary procedures. Compliance with policies and procedures must be subject to internal control and supervision. A review of certain activities must be made to identify potential non-conformances.

5.2 Internal control

Whenever a breach, or risk of breach, is identified whether by the Compliance Officer, an employee of the company, or by an outsider, the matter shall be brought to the attention of the CEO, the Compliance Officer and / or the Chief Legal Counsel for discussion and further handling. Depending on the severity, the Company will either handle the situation internally or lift the matter to the attention of the Company's Board of Directors. The Company will in these situations seek external legal and/or compliance advice to assess the situation as deemed necessary.

5.3 AIS tracking and STS screening - Maritime Intelligence Risk Suite (MIRS)

An important part of sanctions compliance is to ensure that vessels are not traded in sanctioned areas or otherwise in breach of sanctions.

AIS is a tracking system installed on vessels which broadcasts its location and details. It also displays the location and details of nearby vessels. There are legitimate reasons for AIS to be turned off or go dark. This could include (but is not limited to) passage through waters at high risk of piracy, or when weather interferes with satellite connectivity. However, AIS is often intentionally disabled by vessels that seek to obfuscate their whereabouts, and is often practised by vessels seeking to conduct illicit trade. Vessels conducting ship- to-ship transfers will also typically switch off their AIS to evade detection if they are conducting illicit trade, and there have also been recorded attempts to manipulate the data transmitted via AIS.

The Company uses Maritime Intelligence Risk Suite (MIRS), which is an advanced software tool providing data on the global shipping fleet, ports and companies. The solution has been developed with the software manufacturer to include functionalities important to the Company. The system provides a tool to monitor our fleet in real time both in terms of movement and in terms of compliance status of ships and companies, including owners, charterers and ship managers:

- We have notifications set up for all our ships moving into restricted areas, for any dark activity (AIS switch-off) and for change in compliance status (ships and related entities).

- All alerts from the MIRS should be assessed, including when the compliance status

is amended to “Warning” or “Severe”. The assessment may include, but is not limited to; AIS tracking for a specific time period, requesting information from counterparties regarding any dark activity, suspicious port calls or STS transfers, or obtaining further information about listing of ships or entities on any sanctions list.

- If the assessment reveals any red flags, such as port calls to a sanctioned country or dark activity without a trustworthy reason, the Compliance Officer should immediately be informed and involved in the further risk handling.

- Appropriate and effective action to mitigate the identified red flags must be taken immediately. The red flag findings and risk mitigating actions should be properly documented.

- Prior to approving any vessel for STS operations, the suggested vessel needs to be screened in MIRS. If any red flags are identified, a reasonable due diligence must be completed in order to ensure compliance with applicable sanction laws.

Our Company also expects our Business Partners to monitor port calls, sanction lists and any AIS switch-off or dark activity closely and report immediately if any potential or actual issue arises.

5.4 Dow Jones RiskCenter - Know Your Business Partner

As mentioned above, the Company has implemented the Dow Jones RiskCenter. Each relevant Business Partner is continuously monitored against the Dow Jones Risk & Compliance database for any changes in compliance status. The entities monitored, companies and/or individuals, are linked and listed against the appropriate Business Partner record. The system provides notifications if the there are changes deemed to have a material impact on the Risk Level of the Business Partner requiring to be reviewed. This may be e.g. that the entity has become subject to sanctions.

If the compliance status of a counterparty has changed, appropriate and effective action to mitigate the newly identified risk must be taken immediately.

The Compliance Officer or CFO should be informed and involved in the further risk handling. The process will be documented within the RiskCenter.

6. RESPONSIBILITY

If you are responsible for a business activity, you have to be familiar with this Policy, exercise good judgment and do your best to ensure that it is complied with.

The primary contacts for sanctions related issues are the Compliance Officer, with responsibility for implementing and developing the compliance program, including this Sanctions Policy. Please contact the Compliance Officer if you have questions concerning the sanctions program. Nevertheless, it is everyone's responsibility to ensure that we never conduct business with countries, organisations and individuals listed on applicable sanctions lists or that are excluded according to this Policy.

If you think a transaction may involve an individual or a country comprised by sanctions regulations, you must notify the management immediately.

You must never conclude an agreement or carry out a transaction with a company without first ensuring that you know who has final control of the company or who the ultimate beneficial owner of the company is.

If you plan business activities in a country or a region with political and/or military unrest, you must first contact the Compliance Officer. An assessment will then be conducted of the

potential risk of violating trade restrictions and the relationship with human rights, terrorism and other mapped risksituations.

7. MERGERS AND ACQUISITIONS, SALE AND PURCHASE OF ASSETS

Whenever our Company is involved in a merger or acquisition, the management is responsible for ensuring that either the Compliance Officer and/or external legal advisors are involved for completing a risk assessment of potential sanction or trading issues in respect of the transaction.

The management is also responsible for ensuring that a due diligence has been completed in order to identify sanctions-related issues in respect of sale or purchase of assets. The Compliance Officer and/or external legal advisors shall assist in the due diligence process. Sanction-related issues shall be escalated to the relevant senior levels, addressed prior to the conclusion of any transaction, and incorporated into the organisation's risk assessment process.

8. TESTING AND AUDITING

The Compliance Officer is responsible for testing and auditing of the sanctions procedures. Testing and auditing is required in order to assess the effectiveness of current processes and check for inconsistencies between these and day-to-day operations. The purpose is to identify any weakness or deficiencies within the Sanctions Policy.

If any weakness or deficiencies are identified, the Company should enhance the compliance program and implement compensating controls in order to remediate any gaps, including updating, recalibrating or improving software and systems used for sanctions compliance purposes, such as the KYBP tool and the MIRS. External legal counsel may assist completing the testing and auditing.

9. TRAINING

Appropriate risk based communication and training will be provided to all employees and management. Certain business units and functions may require more extensive training than what is required for employees in general.