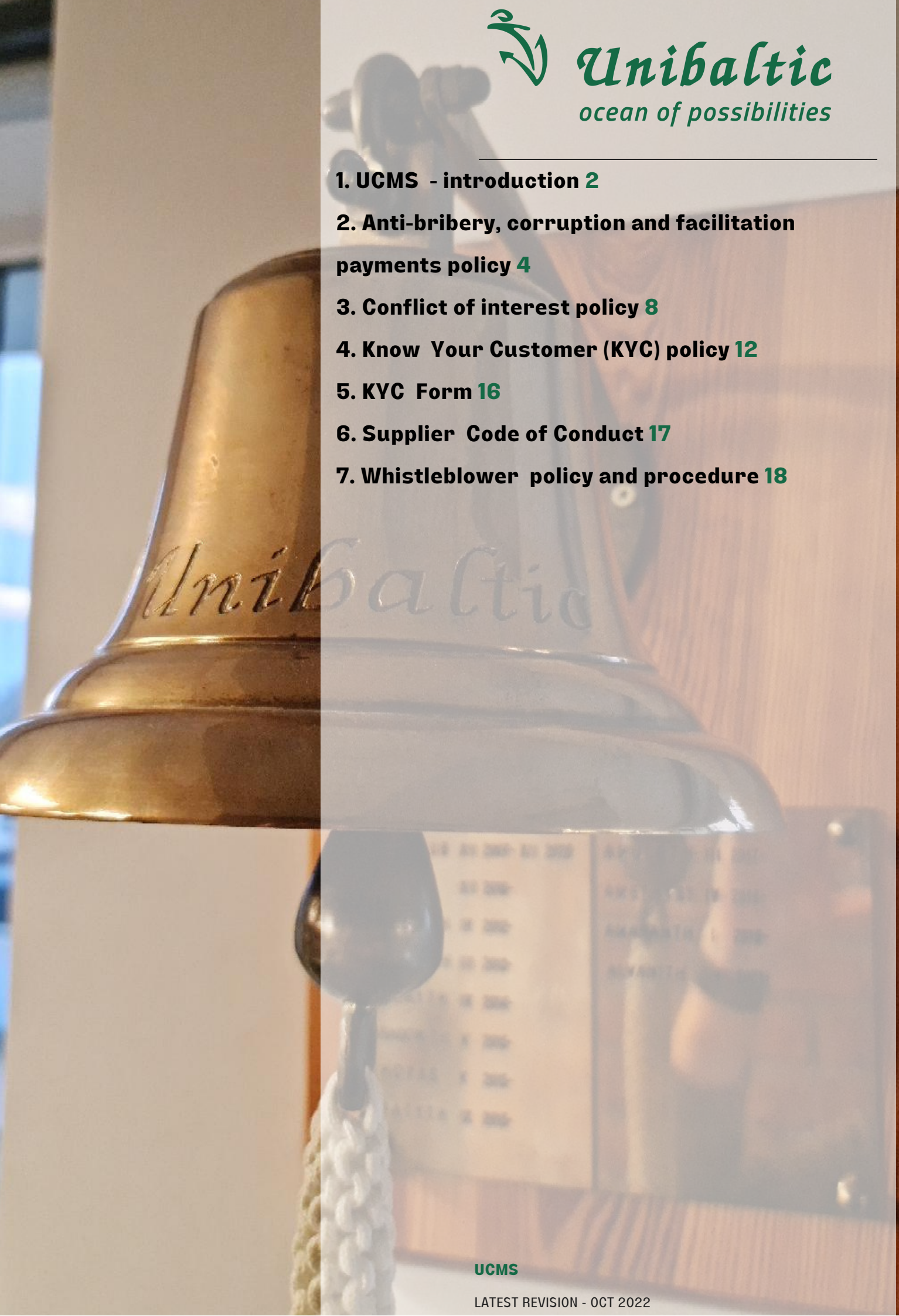
Unibaltic

ocean of possibilities

UCMS

UNIBALTIC COMPLIANCE MANAGEMENT SYSTEM



Unibaltic
ocean of possibilities

UNIBALTIC COMPLIANCE MANAGEMENT SYSTEM

(UCMS)

Introduction.

Compliance means fulfilling of all obligations of the organization. Compliance obligations are understood as requirements that the organization must meet (applicable legal regulations), as well as those that it wants to meet (voluntary commitments, principles of good governance, recognized industry and ethical standards, etc.). It is worth to mention that the requirements that a given organization voluntarily accepts as binding are included in the "compliance canon", and failure to meet them will result in the same consequences as breaking the legal rules.

Compliance Management System includes all the measures, structures and processes that an organization establishes to ensure compliance.

Why this is an important feature of the company?

It is a compliance risk management tool. Its main purpose is to prevent and detect irregularities.

Responsible person.

The responsible person takes care of the development and supervision of the compliance management system within the Unibaltic Group as the Compliance Officer. This function is performed by Mr. Adam Barecki. For the purposes of our organization, this system was named Unibaltic Compliance Management System, hereinafter referred to as UCMS.

It is worth to mention that it is not only the Compliance Officer obligation to be responsible for compliance. This system is created by all employees because long-term compliance can only be achieved by embedding it in the organizational culture and anchoring it in the attitude and behavior of the members of the organization. Each employee of the Unibaltic Group should be aware of the compliance policy, but also of their own role and contribution to the effectiveness of UCMS.

UCMS responsibility is as follows but not limited to:

- development of compliance policies and procedures,
- establishing a compliance programme,
- counteracting the risk of non-compliance and reducing its occurrence,
- conducting explanatory proceedings and corrective actions in the event of irregularities,
- incorporating requirements into business processes,
- conducting periodic compliance audits,
- organization of training for associates.

Benefits of establishing UCMS for the Unibaltic Group.

The document that helps the organization in developing and disseminating a culture of compliance is the ISO 37301:2021 standard. It lists the following benefits of implementing a compliance management system:

- improving business opportunities and sustainable development,
- protecting and enhancing the reputation and credibility of the organization,
- taking into account the expectations of interested parties (stakeholders),
- demonstrating the organization's commitment to effective and efficient compliance risk management,
- increasing third-party confidence in the organization's ability to achieve sustainable success,
- minimizing the risk of a dispute with accompanying costs and damage to the image.

Compliance rules.

The basic principles of compliance in the Unibaltic Group are:

1. Respect for the law - the Group's operations are conducted in accordance with applicable laws,
2. Ethics and honesty - the Group's operations must be conducted in accordance with the adopted Group Code of Business Conduct and Ethics,
3. Transparency - the Group's activities must be conducted in a transparent manner, e.g. by providing appropriate communication channels to receive reports that constitute or may constitute a breach of UCMS.
4. Zero tolerance - for activities inconsistent with UCMS.

What documents creates the UCMS?

The compliance management system consists of the following documents:

1. Code of Business Conduct and Ethics,
2. Anti-bribery, corruption, and gratuity policy,
3. Conflicts of Interest Policy,
4. Know Your Customer Policy,
5. Supplier code of conduct,
6. Whistleblower Policy and Procedure.

Anti-bribery, corruption, and facilitation payments policy.

Introduction.

The company has a zero-tolerance policy toward any form of bribery, corruption, and facilitation payments. Unibaltic strives to conduct all its business activities honestly and ethically. We are committed to acting professionally and fairly and enforcing this policy to counter these issues.

Applicability.

This policy applies to Unibaltic Group (hereinafter referred to as "Unibaltic") employees, officers, directors, customers, suppliers, and any third parties acting on behalf of Unibaltic. It complies with the national law in which the company operates, including the UK Bribery Act.

Definitions.

Bribery is offering, giving, receiving, or soliciting anything of value with the intent to influence the actions of an official, or another person, in charge of public or legal duty. Bribery is an illegal and unethical gift or lobbying effort bestowed to influence the recipient's conduct.

Corruption is defined as the misuse of power by someone to whom it has been entrusted, for his private gain.

Facilitation payments are payments that facilitate a normal governmental function, such as speeding up paperwork. They are all illegal under the UK Bribery Act, regardless of their size or frequency.

A Third-party is a company or entity with whom you have a written agreement to provide a service on behalf of your organization to your customer or upon whom you rely on a service to maintain daily operations, it includes, but is not limited to consultants, agents, representatives, subcontractors, and subadvisors.

UK Bribery Act is an act of the Parliament of the United Kingdom that relates to bribery, legislation that does not distinguish between bribes paid to a public official and those paid to those in the private sector and criminalizes both the receipt and payment of bribes. Applies to entities that provide services in the territory of the UK.

Policy detail.

The main purpose of this policy is to help Unibaltic comply with applicable laws. Under these laws it is illegal for all persons concerned to bribe any other person or entity and receive bribes. The policy also educates all concerned about laws designed to prevent bribery and corruption. Each Unibaltic employee receives adequate training in respect of this policy, and it is the responsibility of each Unibaltic employee to ensure compliance with the terms of this policy.

Accounting requirements.

Unibaltic is also required to make and keep books, records, and accounts, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of Unibaltic. The use of false documents and invoices is prohibited, as is the making of inadequate, ambiguous, or deceptive bookkeeping entries and any other accounting procedure or technique that would hide or otherwise disguise illegal payments.

Actions or behaviour to avoid.

Corruption can be avoided by following the Unibaltic's Code of Business Conduct and Ethics, and this specific policy.

Each of us must adopt a zero-tolerance policy toward all forms of corruption, including bribery and facilitation payments by carrying out the following actions:

- never offering, paying, requesting, or receiving bribes, even if requested to do so by a senior manager or anyone else,
- never get involved in any fraudulent or dishonest activity,
- never authorizing any corrupt activities or behaviours, nor turning a blind eye to potentially corrupt behaviour by third parties acting on Unibaltic's behalf,
- never engaging in activities that could facilitate corruption, including drafting illegal agreements, fraudulent claims, falsifying evidence, and giving false evidence in legal proceedings,
- never concealing any corrupt or potentially corrupt activity,
- never agree on facilitation payments, they are illegal and contrary to our values,
- to conduct proportionate due diligence concerning agents, subsidiaries, contractors, and other third-party service providers to ensure appropriate measures can be taken; it covers not only new business partners but existing ones as well,
- any agreements with third parties must be in writing and should contain provisions related to this policy, for example, that the third party will remain in compliance with this policy,
- to conduct a risk assessment, if necessary, we shall assess the nature and extent of its exposure to potential external and internal risks of bribery and corruption; the purpose of the risk assessment is to identify major risk areas and to take mitigation actions focusing on these areas; if the case of doubt, discuss the matter with the Compliance Officer.

Extortion.

Unibaltic recognizes that corruption-related demands in any form are often backed by a form of extortion, in some cases including the threat of violence or personal harm. Except when the life, health or safety of an employee has been threatened, extortion is no excuse to pay a bribe.
When the threat is aimed at the business and not at the personal safety or health of the employee, the payment will be considered a bribe. A payment made in the good faith belief that life, health, or safety may be in imminent danger must immediately be reported to the Compliance Officer. Such employees will need to use their best judgement to abide by Unibaltic's business standards while ensuring any risks to life, safety and health are minimized.

Gifts and Entertainment.

Gifts.

We shall comply with the anti-corruption laws of the countries where the Group does business. Therefore, gifts should not be given without a prior review of the local anti-corruption law and rules set on this point.

No gifts and gratuities should be offered to government officials except for promotional items of little value, such as inexpensive pens, mugs, T-shirts, calendars, etc., that bear the company's name and logo, provided that this is not prohibited by local law and that it is not made with a corrupt purpose.

Unibaltic also prohibits offering a gift or granting favours outside the ordinary course of business to current or prospective customers, their employees or agents, or any person with whom the company has a contractual relationship or intends to negotiate an agreement.

Unibaltic's employees must also refuse gifts and gratuities from persons who deal or seek to deal with Unibaltic such as suppliers or potential suppliers, except for promotional items of little value. Cash gifts to anyone are prohibited and, if offered to you, must be refused.

Entertainment.

As a general guideline, business entertainment in the form of meals and beverage is acceptable if it is in line with local law, reasonably, and as far as possible on a reciprocal basis.

Whistleblowing.

Any behaviour that violated / would violate this policy should be properly reported to the immediate superior and Compliance Officer (by sending an e-mail: coc@unibaltic.eu, phone: +357 25357717, or standard post: UNIBALTIC GROUP, 229 Arch. Makarios III Ave., Meliza Court, 3105 Limassol, Cyprus; in case of reports addressed from Poland, it is possible to send it to the following address: GRUPA UNIBALTIC, ul. Tama Pomorzanska 14E, 70-030 Szczecin, Poland.

Consequences of non-compliance.

In most jurisdictions, both companies and individuals can be liable for a criminal offence. The exact extent of criminal liability will depend on the law of a particular country. Any Unibaltic employee who violates this policy may be subject to disciplinary action, up to and including employment termination, as applicable. Third parties who violate this policy are subject to termination of all relationships with Unibaltic. Violations of this policy may also result in civil penalties and criminal liability, civil liability damages for such individuals.

Policy review.

This policy is subject to regular annual review and audit by the Compliance Officer, to ensure it remains suitable, effective, and proportionate to the company's needs. The

Compliance Officer is responsible to conduct training for Group's employees on this procedure, as well as verifying compliance with it through periodic audits. Any changes to the content of this policy should be recorded in the form of a register of changes, where the date of the change and the subject of the change will be specified.

Conflict of interest policy.

Policy statement.

All employees of Unibaltic Group (hereinafter referred to as "Unibaltic", "the company ") are required to perform the duties and activities of their position with the highest level of integrity and independence, in a professional and ethical manner. They must also ensure that they avoid or eliminate any conflict of interest or situation that could reasonably be perceived as a conflict of interest and immediately report it to their line manager and Compliance Officer.

Applicability.

This policy applies to all employees of Unibaltic, as well as contractual third parties or partners doing business with the company. All are expected to abide the provisions of this policy that are reasonably applicable to them.

Definition.

A conflict of interest occurs when an entity or individual becomes unreliable because of a clash between personal interests and professional duties or responsibilities. Such a conflict occurs when a company or person has a vested interest—such as money, status, knowledge, relationships, or reputation—which puts into question whether their actions, judgment, and/or decision-making can be unbiased.

Conflict of interest can arise without intent to 'cross the line between professional and personal interest. In other words, conflict of interest can be not only **actual** but also:

- **potential** is foreseeable from the circumstances but has not yet become actual (for example, where a job applicant is related to a recruitment team member, but the applications have not yet been processed),
- **perceived** is one where the circumstances indicate to a reasonable person that an employee's duty to the Unibaltic is affected, whether there is an actual conflict of interest or not

To sum up the above, the fact that an employee of Unibaltic has a relationship (e.g., family, friendship, etc) with someone connected with Unibaltic does not necessarily mean there is a conflict of interest. Whether a conflict of interest exists depends on the circumstances.

Actions or behaviours to avoid.

Some situations, behaviours or events should be always avoided by persons/entities obliged by this policy. In the case of:

a) personal interest
employees must ensure that no conflict exists or could appear to exist between their interests and those of Unibaltic, potential competitor, customer, partner,

vendor, supplier, or other business entity in which you have a direct or indirect financial interest. It is forbidden to:

- take part in or attempt to influence any Unibaltic decision or any business dealings with a current or potential competitor, customer, partner, vendor, supplier, or other business entity in which you have a direct or indirect financial interest,
- use the premises, equipment, supplies or services of other employees of Unibaltic to promote their interests,
- use of confidential information for their benefit during or after employment with Unibaltic,
- to be in a position where they could benefit directly or indirectly from a Unibaltic business transaction (e.g., supplier of goods or services, contract, partnership),
- give preferential treatment to any supplier or other person doing business with Unibaltic to serve their interests,

b) family, friends, and romantic relationships
employees and managers must not:

- use their position or contacts at Unibaltic to promote their interest or those of a family member or person with whom they have a close personal or professional relationship,
- take part in or attempt to influence any Unibaltic-related decision or business dealings that may benefit or appear to benefit a relative, close friend or a business enterprise in which a relative or close friend is involved or has a direct or indirect financial interest,
- if you are aware that Unibaltic plans to hire your relative or a person for a position with whom you have a romantic relationship that directly reports to you, you must disclose that information immediately to your line manager and Compliance Officer,
- if during your employment, a romantic relationship develops between you and another Unibaltic employee within your direct or indirect reporting chain, you both must promptly disclose that information. If a manager fails to report such a relationship will be grounds for appropriate disciplinary action.

c) relationship and favouritism
employees shall not grant or appear to grant preferential treatment to a person with whom they have a close personal or professional relationship. In some situations, the past relationship may also give rise to a perceived conflict of interest and should be treated as such. If an employee is in a situation where s/he could decide (e.g., hiring, evaluation, discipline, promotion, reward, any other form of discretionary control or the awarding contract) involving, directly or indirectly, a person with whom he or she has a close personal or professional relationship, the employee must:

    - disclose the potential conflict to his / her manager, and Compliance Officer,
    - refrain from making any recommendations, or conveying views related to the decision.

Identification and disclosure of conflict of interest.

All employees and third parties acting on behalf of the company have a responsibility for identifying, declaring, and managing any potential or perceived conflict of interest that applies to them.

Where an employee suspects that they may have a potential/perceived/actual conflict of interest, the employee needs to discuss it the Compliance Officer. It requires to fulfil a relevant disclosure form to the identified conflict of interest, to allow the Compliance Officer to fully assess whether a conflict of interest exists. Such notification should include the following information at least:

- name and surname of the applicant,
- an indication of the source and cause of the conflict of interest,
- an indication of the person/entity with which there is a conflict of interest.

Until it is determined whether the conflict of interest exists, the reporting person should withdraw from the decision-making process.

Managing conflict of interest.

If the Compliance Officer determines there is a potential/perceived/actual conflict of interest, it will be prepared and proposed a conflict of interest management plan. It should be discussed with the concerned employee who is obliged to follow this plan. Such a plan must be approved by the Management Board.

Conflict of interest management plans will ensure conflicts are managed and resolved based on the following strategies:

- record and disclose, ensure all information surrounding the conflict of interest has been disclosed and documented appropriately, the company should keep a register of conflict of interest,
- restrict, restrictions are placed on the employee's involvement in the matter, or the scope of the work is reformulated or change the hierarchical relationship is imposed or there is a restriction on access to certain information,
- recruit and monitor, a non-conflicted manager is used to oversee part or all the process that deals with the matter,
- remove, the employee removes themselves, or is removed, from the matter (e.g., in a situation in which a job applicant is related to a member of the recruitment team for that position, a conflict of interest management plan might be for that member to step down from their position during the selection process for that position only),
- relinquish, the employee relinquishes the private interest that is creating the conflict. Where relinquishing the interest is not possible (e.g., relationship with family) and the conflict cannot be managed using one of the above options, the employee should consider removing themselves from the process.

Conflict of interest management plans including the disclosure form should be reviewed annually to ensure they remain effective.

Consequences of non-compliance.

Failure to comply with these provisions may result in disciplinary action, up to and including termination of employment, depending on the seriousness of the circumstances. Employees need to be aware of this policy.

Whistleblowing.

Any behaviour that violated/would violate/is planned to violate/ this policy should be properly reported to the immediate superior and Compliance Officer (by sending an e-mail: coc@unibaltic.eu, phone: +357 25357717, or standard post: UNIBALTIC GROUP, 229 Arch. Makarios III Ave., Meliza Court, 3105 Limassol, Cyprus; in case of reports addressed from Poland, it is possible to send it to the following address: GRUPA UNIBALTIC, ul. Tama Pomorzanska 14E, 70-030 Szczecin, Poland.

Policy review.

This policy will be reviewed by the Compliance Officer every year to consider of any changes in legislation, expectations, or practices. The compliance Officer is responsible to conduct training for Group's employees on this procedure, as well as verifying compliance with it through periodic audits. Any changes to the content of this policy should be recorded in the form of a register of changes, where the date of the change and the subject of the change will be specified.

Know Your Customer (KYC) policy

Policy statement.

Verification of a potential contractor is a preventive action, allowing to minimize the risk related to establishing a business relationship with an unreliable entity. The consequences of cooperation with such an entity can be severe, starting from non-performance of the subject of the contract, failure to pay and unconscious participation in VAT offences.

An agreement with a dishonest business partner is not only a spectre of measurable financial losses but also significant public image consequences that are more difficult to estimate. Unibaltic Group ensures that verification of potential clients is carried out under this policy. We make every effort to ensure that the potential contractor is properly verified.

Applicability.

This policy applies to all employees of Unibaltic Group (hereinafter referred to as "Unibaltic", "Company"), as well as contractual third parties or partners doing business with the company. All are expected to comply with this policy.

The Compliance Officer is responsible for carrying out the client verification process. Before starting cooperation with an entity, the employee is obliged to send a verification inquiry to the Compliance Officer at the e-mail address coc@unibaltic.eu.

Purpose.

The main goals of this policy are:

- to increase the protection against the risk of cooperation with entities acting against the law, good manners, and commercial practices,
- to increase the probability of exercising due diligence when making decisions regarding the conclusion of a contract,
- avoiding the abuse of tax fraud,
- exclusion of sanctioned entities.

KYC checks and onboarding processes.

Verification activities should be carried out both before concluding the contract with the client, as well as during its duration. Assessment of the client during the term of the contract should consider the existing economic relations with Unibaltic Group.

Before starting the KYC process, the Compliance Officer is required to fulfil the information obligations towards natural persons whose data is processed. It results from the Regulation (EU) 2016/679 on the protection of natural persons concerning the processing of personal data and the free movement of such data (hereinafter referred to as the « GDPR act »). The Compliance Officer should inform a potential client about:

- categories of data that are processed include the data of persons running a business, such as name and surname, e-mail address (general addresses are

excluded), tax number, residence address and other data of persons who are members of the contractor's management bodies, including ultimate beneficial owners,
- legal basis for the processing of personal data related to the verification of business partners, which is generally Art. 6 (1) (f) of the GDPR act, that is processing is necessary for the legitimate interests pursued by the administrator,
- period of data processing, which is the same as the period of cooperation, and 1 year after its termination.

After fulfilling the above obligation in accordance with the GDPR act, the Compliance Officer start the verification process by obtaining the following data:

- business registration number,
- legal name,
- business address,
- operational status,
- key management personnel,
- date of incorporation,
- shareholders structure and ultimate beneficial owners,
- VAT number,
- determining whether a contractor is sanctioned,
- bank details.

The above information should be obtained based on the appropriate KYC form, the specimen od which is attached as Appendix 1 to this policy. Additionally, the client should be requested for an up-to-date basic registration document. All gathered information shall be verified based on documents, or data obtained from a reliable and independent source, e.g.:

- client's registration documents can be verified on e-justice.europa.eu portal: https://e-justice.europa.eu/489/EN/business_registers__search_for_a_company_in_the_eu
- information on business registers in EU countries can be obtained on e-justice.europa.eu portal: https://e-justice.europa.eu/106/EN/business_registers_in_eu_countries
- customer's website / fan page in social media,
- verification of customer's VAT number:
  - European entities https://ec.europa.eu/taxation_customs/vies/?locale=en
  - Polish entities https://www.podatki.gov.pl/wykaz-podatnikow-vat-wyszukiwarka

Levels of due diligence.

In the case of a low-risk client, re-verification of its data should take place every year. In respect of such entities, the Compliance Officer shall provide simplified verification by using the approved KYC form only.

As regards to more risky entities, enhanced due diligence is required. It is recommended to update information twice a year. The Compliance Officer is obliged to collect additional

information for higher-risk customers to provide a deeper understanding of customer activity to mitigate associated risks (e.g., adverse media screening; PEP screening; sanction screening; use of professional verification service providers in case of high-value contracts; financial statements; wider verification of client's bank account; tax residency).

Sanctions screening.

All necessary information regarding current sanction lists can be obtained on the following websites:

- US sanction list (led by Office of Foreign Asset Control - OFAC): https://sanctionssearch.ofac.treas.gov/
- UN sanction list (led by United Nations Security Council): https://www.un.org/securitycouncil/content/un-sc-consolidated-list
- UE sanction list (led by the European Commission): https://www.sanctionsmap.eu/#/main
- UK sanction list (led by the Foreign, Commonwealth and Development Office): https://www.gov.uk/government/publications/the-uk-sanctions-list
- Polish sanction list (led by the Ministry of the Interior and Administration): https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami

Collection of data.

All information collected by the Compliance Officer under this policy should be obtained and stored respecting generally applicable law, including the GDPR act, and the company's privacy policy. Records concerning KYC policy shall be properly maintained. It is Compliance Officer responsibility to retain data in such a manner that in certain situations can be demonstrated due diligence during the screening process. Appropriate documentation of the verification results is essential for evidence purposes.

Decision making.

After the verification of a client under this procedure, it is an employee responsibility to decide on cooperation.

Whistleblowing.

Any behaviour that violated / would violate this policy should be properly reported to the immediate superior and Compliance Officer (by sending an e-mail: coc@unibaltic.eu, phone: +357 25357717, or standard post: UNIBALTIC GROUP, 229 Arch. Makarios III Ave., Meliza Court, 3105 Limassol, Cyprus; in case of reports addressed from Poland, it is possible to send it to the following address: GRUPA UNIBALTIC, ul. Tama Pomorzanska 14E, 70-030 Szczecin, Poland.

Consequences of non-compliance.

Failure to comply with these provisions may result in disciplinary action, up to and including termination of employment, depending on the seriousness of the circumstances and the consequences of non-compliance for the company.

The Unibaltic Group does not establish cooperation with entities that have not successfully passed the verification process. If during the cooperation period, it turns out that this policy is violated, it will result in immediate termination of cooperation.

Policy review.

This policy will be reviewed by the Compliance Officer every year to consider of any changes in legislation, expectations, or practices. The Compliance Officer is responsible to conduct training for Group's employees on this procedure, as well as verifying compliance with it through periodic audits. Any changes to the content of this policy should be recorded in the form of a register of changes, where the date of the change and the subject of the change will be specified.

Appendix no. 1

KYC FORM

GENERAL INFORMATION	
Entity full name	
Date of incorporation	
Entity registration number	
Registered address	
Main activities	
VAT number	
Bank details	
TRAC number	
OWNERSHIP STRUCTURE AND MANAGEMENT BOARD	
Management Board	
Shareholders structure	
Entity ultimate beneficial owners	

CODE OF BUSINESS CONDUCT AND ETHICS

Charterers agree to act in compliance with the Unibaltic's Code of Business Conduct and Ethics. ☒ https://unibaltic-shipping.eu/images/download/CODE-OF-BUSINESS-CONDUCT-FINAL-VERSION.pdf

SANCTIONS

Undersigned counter-party (hereinafter referred to as "Charterer") hereby undertakes to abide by effective sanctions imposed by EU, US and UN, including those imposed against Russia in relation to the war waging against Ukraine. Furthermore, Charterers commit themselves to enhanced due diligence in the course of cargo origin verification along with the entities related to any Russian links.

Charterers confirm that cargo is not of Russian origin ☒

Charterers confirm that there is no Russian entity/person involved in this shipment (or affiliated with the aforementioned) ☒

By signing this document, you:

a. declares that all information provided is correct and actual,
b. confirms that you have been provided with the information obligation resulting from the GDPR Act,
c. agree to process the above information (especially personal data) for Unibaltic's due diligence purposes, and you guarantee that you will inform the appropriate persons that their data have been transferred to the Unibaltic Group in connection with the implementation of its legitimate interests and that they will be registered and processed for their implementation.
d. are duly authorized to sign this document.

Name and surname:
Job position:
Place:
Date:
Signature:

Supplier Code of Conduct.

This code is created to ensure that company's suppliers share with us the same values such, as respect for ethical business, honesty, health and safety work conditions, integrity, and much more as set out in our Code of Business Conduct and Ethics. Below you will find a link to its current version:

https://unibaltic-shipping.eu/images/download/CODE-OF-BUSINESS-CONDUCT-FINAL-VERSION.pdf

In our business, we try to exercise the highest diligence, and we expect our suppliers to do the same. By signing this Code, our suppliers ensure that they fully share the values described in our Code of Business Conduct and Ethics and that they will adhere to them in their supply chain.

Our suppliers should ensure that:

1. in respect of labour practice and standards:
    - they have a zero-tolerance policy on child labour, human trafficking, modern slavery, discrimination,
    - ensure compliance with applicable laws and regulations and international standards related to labour practice and protection of human rights standards as defined in the principles of the United Nations Global Compact (https://www.unglobalcompact.org/what-is-gc/mission/principles),
    - provide a safe, secure, and healthy working environment.
2. in respect of environmental policy:
    - they will follow the applicable environmental laws and regulations.
3. in respect of ethics:
    - they have a zero-tolerance policy to corruption, extortion or bribery, money laundering, properly verification of a clients,
    - disclose any potential or actual conflict of interest to Unibaltic,
    - you do not do business with sanctioning entities, or do not offer embargoed cargoes.

We welcome concerns from anyone within or outside of Unibaltic Group if they suspect or know of any potential or actual violations of this Code. You can report your concerns to Compliance Officer by using the following sources:
e-mail: coc@unibaltic.eu
phone: +35725357717
standard post: UNIBALTIC GROUP, 229 Arch. Makarios III Ave., Meliza Court, 3105 Limassol, Cyprus; in case of reports addressed from Poland, it is possible to send it to the following address: GRUPA UNIBALTIC, ul. Tama Pomorzanska 14E, 70-030 Szczecin, Poland.

Company name: ……
Authorized signatory: ……
Signature: ……
Date, place: ……..

Whistleblower policy and procedure.

Policy statement.

Unibaltic Group (hereinafter referred to as " Unibaltic", " the company ", " the Group") is committed to always conducting its business with honesty and integrity. If at any time, this commitment is not respected or appears to be in question, Unibaltic will endeavour to identify and remedy such a situation.

Purpose.

This policy is intended for the reporting of serious irregularities, or misconduct **related to the Group's activity**, in particular violations of the Group Code of Business Conduct and Ethics, applicable law (EU and national law where the Group conduct business), as well as the Group's policies and procedures.

Reports of violations as set out above are an element of proper and safe management. Its purpose is to increase the effectiveness of detecting irregularities and taking action to eliminate them and reduce the risk.

Whistleblower policy describes how the report can be submitted, the protections available to whistleblowers and how Unibaltic will support and protect you and inform you on follow-up actions taken.

Applicability.

This policy applies to all employees of Unibaltic Group (current and former, as well those who have passed the recruitment stage and have not started work yet, the Management Board members, shareholders), their volunteers and trainees, as well as contractual third parties or partners doing business with the Group.

Definition.

A whistleblower is someone who speaks up about suspected wrongdoing in the context related to the work performed, by internal, external, or public disclosure, is acting in good faith and is making a disclosure in the manner described in this policy.

An assisting person is understood as a natural person assisting a Whistleblower in a report in a work-related context.

Whistleblowing means disclosure of misconduct or breach of rules.

Disclosure/report means the oral or written communication of information on violations. If it is filed within the organization, it is an internal declaration. If it is submitted to the competent authorities, it is an external report. On the other hand, disclosure of information to the public is called public disclosure.

Misconduct/irregularities is illegal, unfair conduct, such as a crime or misdemeanour, violation of applicable laws, violation of the Unibaltic Group's contractual obligations, violation of the Code of Business Conduct and Ethics, Group policies and procedures, and any other unethical or unfair behaviour.

Retaliation means any direct, or indirect act, or omission in a work-related context that is caused by internal or external reporting or public disclosure, and which causes or may cause undue harm to the reporting person.

EU law European Parliament Directive 2019/1937 dated 23.09.2019, establishing common minimum standards for the protection of persons reporting the following abuses of Union law: public procurement; services, products and financial markets; prevention of money laundering and terrorist financing; product safety and compliance with the requirements; transport safety; environmental protection; radiological protection and nuclear safety; food and feed safety; animal health and welfare; public health; consumer protection; protection of privacy and personal data; security of networks and ICT systems; interests financed by the European Union; the internal market of the European Union, including the rules of competition, state aid and corporate taxation.

National law means generally applicable law in the country where the Group operates.

Reporting.

A person who has serious and reasonable grounds to suspect possible irregularities, violations, or misconduct should report them to an immediate supervisor who should then contact with Compliance Officer. Employees wishing to remain their confidentiality, including anyone outside the organization covered by this policy, are pleased to directly contact the Compliance Officer. The notification can be submitted orally (during the meeting, or by phone), electronically, as well as a traditional post by using the following contact details:

Mr. Adam Barecki
e-mail: coc@unibaltic.eu
phone: +357 25357717
correspondence address: UNIBALTIC GROUP, 229 Arch. Makarios III Ave., Meliza Court, 3105 Limassol, Cyprus; in case of whistleblowers from Poland, it is possible to send it to the following address: GRUPA UNIBALTIC, ul. Tama Pomorzanska 14E, 70-030 Szczecin, Poland; with a note on the envelope "Reporting of irregularities".

Such a report should contain the following information:

- personal data of the Whistleblower and contact details,
- personal data of the person to whom the report relates to,
- the nature of your concern and why you believe it to be true,
- when and where the described incident took place,
- brief description of the incident that may cause a breach or misconduct,
- list of potential witnesses,
- evidence that may facilitate proper verification of the report.

It is allowed to accept anonymous reports. If the report is made by phone, then, with the consent of the person making the notification, it should be commented by means of a complete and accurate transcript of the conversation prepared by the Compliance Officer. The reporting person may check, correct, and approve the transcription of the telephone conversation by signing it in the absence of anonymity.

Consideration of report.

The Compliance Officer is obliged to confirm the receipt of the report within 7 days to the Whistleblower unless s/he has not indicated the address to which such confirmation should be provided.

Then the report is subject to initial verification. If the notification is untrue or it is impossible to obtain the information necessary to conduct such a procedure (in the case of an anonymous report), its conduct should be abandoned. Such a decision should be notified to the Whistleblower not later than 1 month from the date of confirmation of receipt of the report. If the notification is justified, the Whistleblower should be notified of the initiation of the investigation within the same time frame.

Compliance Officer recognizes the notification and undertakes follow-up actions. Feedback should be given to the Whistleblower within 3 months from the date of confirmation of receipt of the notification if s/he has left a contact.

The Compliance Officer can familiarize himself with all documents relating to the notification, including those of the nature of classified information or business secrets. The person conducting the proceedings has the right to demand explanations from employees or associates of the Unibaltic Group who may be knowledgeable about the report, as well as perform any other activities necessary to clarify the matter. Employees or co-workers are required to provide explanations and provide documents and information at the request of the person conducting the investigation. Any difficulties in this connection should be immediately reported to the company's Management Board.

After collecting the evidence, meetings with the Whistleblower should be organized, during which it will be possible to specify the information and then with the person whom the report concerns. Such a meeting must be recorded and signed by the persons participating in it.

Based on the material collected, the Compliance Officer determines the facts and determines whether the breach covered by the notification took place, or not. If the violation has taken place, the person conducting the investigation:

- submits requests to responsible persons to stop practices leading to violations of law, policies, procedures,
- indicates the steps that should be taken to remedy the damage or remove the problem,
- requests the Management Board to take action against persons who have committed these violations, in particular transferring to another position, changing the scope of duties, imposing sanctions or terminating employment contracts/contracts with them,

- in matters relating to the commission of a crime, notification of the appropriate state authority.

Register of notifications.

The Compliance Officer keeps a register of all notifications, following the confidentiality requirements. Documents and information gathered during the investigation are kept for 5 years from the end of the investigation. The register should contain basic information such as:

- case number,
- Whistleblower data,
- infringer data,
- the subject of the notification,
- facts,
- the status of the disclosure (confirmed / not confirmed, open/closed),
- follow-up actions are taken and the end date of the case.

Identify protection.

Unibaltic protects the confidentiality of the identity of the reporting person and the third party mentioned in the report, as per the company's GDPR policy, and prevents unauthorized staff members from gaining access to them. When you make a disclosure, your identity will only be shared if you consent to it, or if Unibaltic is required to do so by law.

Disclosure may be anonymous and if so, such person will be protected under this policy where possible. However, requiring complete anonymity may practically make it more difficult for Unibaltic to investigate the issue or take the action we would like to take. If you let us know who you are, we can contact you directly to discuss your concerns which will help us investigate the complaint more quickly and efficiently. You will also be properly protected from possible retaliation.

Whistleblower protection.

The Compliance Officer will take steps to protect the interest of individuals making reports under this policy. The Whistleblower who acts in good faith and has reasonable grounds to believe that the reported information on breaches is true at the time of reporting can count on appropriate protection. It consists in protecting the identity of Whistleblowers in accordance with the point described above. In addition, if irregularities reported by Whistleblowers are substantiated, they are protected against dismissal and change of job position, unless the second results directly from organizational changes.

If a disclosure is not true or is misleading the Whistleblower will not be protected. Such behaviour is a breach of this policy and will be considered a serious matter that may result in disciplinary action. There may also be a legal consequence if the Whistleblower makes a knowingly false report.

Unibaltic Group does not tolerate any form of negative and retaliatory conduct taken by any person against the Whistleblower or any other people who are involved in the

investigation. Taking any action of a repressive, discriminatory, or another kind of unfair treatment against the Whistleblower will be treated as a breach of this policy and may result in employee accountability, or termination of the employment contract.

The protection also covers whistleblowers who skipped the internal reporting patch and made it:

- externally, i.e., directly to the competent state authority receiving external reports on breaches in the areas within the scope of these bodies,
- in public, if the person first made internal and external reports or immediately external reports, but no appropriate action has been taken in response to his / her report, or if the reporting person has reasonable grounds to believe that the breach may pose an immediate or obvious risk to the public interest (e.g. an exceptional situation or the risk of irreversible damage) or, in the event of an external report, it will be at risk of retaliation or there is little likelihood of effective remedying the breach due to the specific circumstances of the case (concealment, destruction of evidence, collusion between the authority and the perpetrator).

An example of the catalogue of activities that are considered retaliatory actions:

- refusal to establish an employment relationship,
- termination of employment without notice,
- failure to conclude a fixed-term employment contract or an employment contract for an indefinite period after the termination of a trial period employment contract, failure to conclude another fixed-term employment contract or failure to conclude an employment contract for an indefinite period, after the termination of a fixed-term employment contract - in where the employee had a reasonable expectation that such a contract would be concluded with him,
- lowering the amount of remuneration for work,
- suspension of promotion, or omission from promotion,
- omission of work-related benefits other than remuneration or reduction in the amount of these benefits,
- transferring an employee to a lower job position,
- suspension in the performance of employment duties,
- transferring the employee's current duties to another employee,
- unfavourable change of place of work, or working schedule,
- the negative evaluation of work results or negative opinion about work,
- the imposition or application of a disciplinary measure, including a financial penalty, or a measure of a similar nature,
- coercion, intimidation, or exclusion,
- mobbing,
- discrimination,
- unfavourable, or unfair treatment,
- suspension of participation, or omission when selecting to participate in training courses aimed at improving professional qualifications,
- unjustified referral to medical examinations, including psychiatric examinations, provided that separate regulations provide for the possibility of referring an employee for such examination,
- the action aimed at making it difficult to find a job in a given sector, or industry in the future based on an informal or formal sector or industry agreement,

- causing financial loss, including economic loss, or loss of income,
- causing other non-material damage, including damage to reputation, especially on social media.

The above actions of the employer (as well as the threat or attempt to take such actions) will not be considered retaliatory actions if the employer proves that he was guided by objective and duly justified reasons.

Importantly, the prohibition of retaliation and protection against such activities applies not only to the Whistleblower but also to:

- the person assisting in making such a report,
- a person related to the Whistleblower,
- a legal person or other organizational unit assisting or related to the Whistleblower - in particular, being the property of or employing the Whistleblower.

The company takes all allegations of retaliatory actions very seriously. If the Whistleblower believes that is suffering negative actions s/he should report it to the Compliance Officer.

GDPR information clause.

The Administrator of personal data is Unibaltic Group. The Administrator processes the data under regulation EU 2016/679 of the European Parliament and EU Council of 27.04.2016 on the protection of individuals about the processing of personal data and on the free movement of such data (GDPR act).

The data will be processed for a purpose related to signalling irregularities, under:

- Article 6 sec. 1 letter a GDPR, for the purpose and in the scope of implementing the consent given by the subject data (in the event of the consent),
- Article 6 sec. 1 letter c GDPR, to fulfil Administrator's legal obligations imposed by binding regulations.

The data will be processed for 5 years from the date of the end of an investigation. The data may be disclosed by the Administrators to authorized entities, if it is necessary for connection with the verification of the notification, in the manner specified by mandatory provisions of law. The data will not be processed in an automated manner and will not be transferred to a third country, except Poland and Cyprus.

Consequences of non-compliance.

Any person obliged to comply with this policy must take liability into account. The consequences depend on the degree of guilt and type of action taken, ranging from disciplinary penalties to dismissal, and informing the relevant public authorities in the event of legal violations, including civil and criminal liability.

Policy Review.

This policy will be reviewed by the Compliance Officer every year to consider any changes in relevant legislation, expectations, or practices. The Compliance Officer is responsible to

conduct training for Group’s employees on this procedure, as well as verifying compliance with it through periodic audits. Any changes to the content of this policy should be recorded in the form of a register of changes, where the date of the change and the subject of the change will be specified.