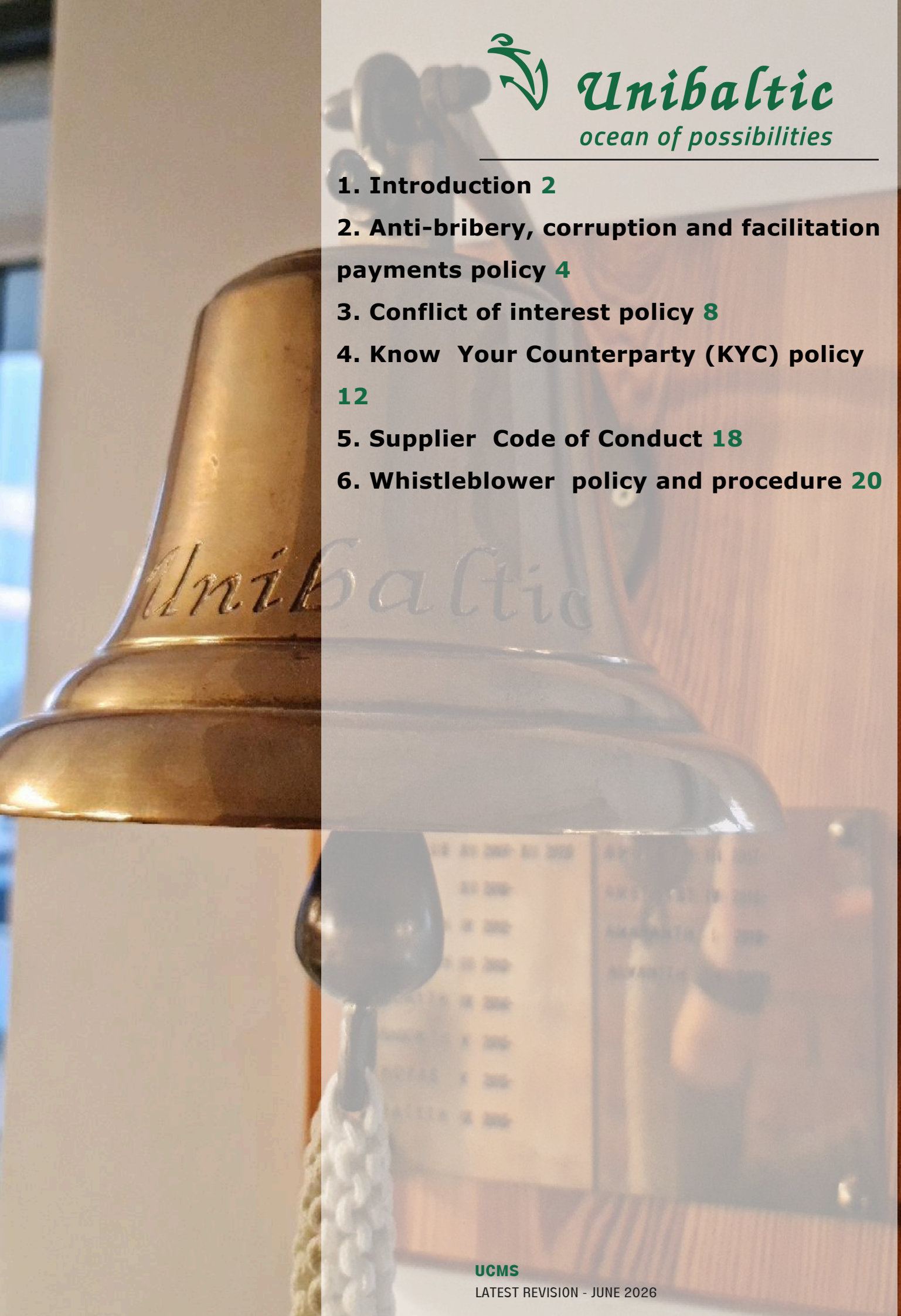
UCMS
UNIBALTIC COMPLIANCE MANAGEMENT SYSTEM



Unibaltic
ocean of possibilities

UCMS
LATEST REVISION - JUNE 2026

UNIBALTIC COMPLIANCE MANAGEMENT SYSTEM (UCMS)

Introduction

The Unibaltic Compliance Management System (hereinafter: "UCMS") constitues a set of principles, procedures and measures supporting the conduct of business in compliance with applicable laws, internal regulations and ethical standards. The UCMS applies to the Unibaltic Holding Group, consisting of nine entities registered in Cyprus, as well as — due to existing business links and their operation within a common value chain — Unibaltic Sp. z o.o., acting as the ISM Manager of the fleet, and Unibaltic Crewing Sp. z o.o., acting as the Crewing Agent. For the purposes of this document, these entities are collective reffered to as the "Unibaltic Group", the "Group", the "Company" or the "Unibaltic". The purpose of the UCMS is to support the organisation in identifying, mitigating and managing compliance risk, as well as minimising the risk of financial losses and reputational damage.

The UCMS is addressed to all employees of the Unibaltic Group, management staff and persons cooperating with the Group, to the extent that their activities are connected with the organisation's operations and the applicable compliance principles. For a better understanding of the assumptions underlying the UCMS, the fundamental concept on which this system is based — compliance — is explained below.

Compliance means the fulfilment of all obligations imposed on the organisation. It includes both requirements arising from generally applicable laws and obligations voluntarily assumed, such as good governance principles, recognised industry standards and ethical standards. A breach of such obligations may result in consequences comparable to a breach of law.

Responsible person

The Chief Compliance Officer is responsible for the development and oversight of the compliance management system within the Unibaltic Group. For the purposes of our organisation, this system has been named the Unibaltic Compliance Management System.

It should be emphasised that compliance matters are not the responsibility of the Chief Compliance Officer alone. This system is co-created by all employees, as sustainable compliance can only be achieved by embedding it in the organisational culture and rooting it in the attitudes and conduct of the members of the organisation. Every employee of the Unibaltic Group should be aware both of the existence of this system and of their own role and contribution to its effectiveness.

The main responsibilities of the Chief Compliance Officer include:

- developing compliance policies and procedures,
- preventing and mitigating compliance risk,
- conducting investigations and remedial actions in the event of irregularities,
- integrating compliance requirements into business processes,
- organising training for employees and cooperating persons.

Benefits of establishing the UCMS for the Unibaltic Group

ISO 37301:2021 is a standard that supports organisations in developing and promoting a culture of compliance. It identifies the following benefits resulting from the implementation of a compliance management system:

- improving business opportunities and supporting sustainable development,
- protecting and strengthening the organization's reputation and credibility,
- considering 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 disputes, together with the related costs and reputational damage.

Compliance principles

The following fundamental compliance principles apply within the Unibaltic Group:

1. **Respect for the law** – conducting business in accordance with applicable laws.
2. **Ethics and integrity** – conducting business in accordance with the adopted Code of Business Conduct and Ethics.
3. **Transparency** – conducting business in a transparent manner, including by ensuring appropriate communication channels for receiving reports concerning breaches or potential breaches of the UCMS.
4. **Zero tolerance** – no acceptance of conduct inconsistent with the UCMS.

The list documents constituing the Unibaltic Compliance Management System

The Unibaltic Compliance Management System consists of the following documents:

1. Code of Business Conduct and Ethics,
2. Anti-Bribery, Anti-Corruption and Gratuities Policy,
3. Conflict of Interest Policy,
4. Know Your Customer Policy,
5. Supplier Code of Conduct,
6. Whistleblower Protection Policy and Procedure.

Anti-Bribery, Anti-Corruption and Facilitation Payments Policy

Policy statement

The Unibaltic Group (hereinafter: "Unibaltic", the "Group" or the "Company") applies a zero-tolerance approach to all forms of bribery, corruption and facilitation payments. The Company conducts its business in an honest, transparent manner and in accordance with the highest ethical standards. All persons covered by this Policy are required to act with due care, professionalism and integrity.

Application

This Policy applies to the Group's employees, management staff, members of corporate bodies, as well as customers, suppliers and all third parties acting on behalf of or for the benefit of Unibaltic. The provisions of this Policy shall be interpreted and applied with due regard to the laws applicable in the jurisdictions in which the Company conducts its business, including the United Kingdom anti-bribery legislation, the *UK Bribery Act*.

Definitions

Bribery means offering, giving, receiving or requesting any financial or personal advantage with the intention of influencing the act or omission of a person performing a public function or another person obliged to act in accordance with a specific legal or official duty. Other improper advantages, including gifts or actions taken with the purpose of unlawfully influencing the decision or conduct of the recipient, may also be considered bribery.

Corruption means the abuse of an entrusted position, function or authority for the purpose of obtaining a private, financial or personal advantage.

Facilitation payments usually mean small amounts of money or other benefits provided to public officials or officers in order to expedite or facilitate the performance of routine official duties which they are legally obliged to perform. Such payments are prohibited, including under the *UK Bribery Act*, regardless of their value, frequency or local practice.

Third party means any external entity that provides services to Unibaltic, acts on its behalf or supports the Group in conducting its operational activities. This term includes, in particular, consultants, agents, representatives, intermediaries and subcontractors.

UK Bribery Act means the Act of the Parliament of the United Kingdom regulating matters relating to bribery and corruption. The Act criminalises both the giving and receiving of corrupt advantages, whether in the public or private sector, and also applies to entities conducting business or providing services in the territory of the United Kingdom.

Policy details

The purpose of this Policy is to define the rules of conduct concerning the prevention of bribery, corruption and facilitation payments, as well as to increase the awareness of persons covered by this Policy as to the consequences of breaching its provisions. Every Unibaltic employee is required to complete training on this Policy, appropriate to their position, and to comply with its provisions.

Accounting requirements

The Group is required to keep and maintain its books, records and accounts in an accurate, complete and appropriately detailed manner, so that they fairly reflect all transactions and the manner in which the Company's assets are disposed of. It is prohibited to use false documents or invoices, to make accounting entries that are unreliable, ambiguous or misleading, or to apply any accounting procedures or techniques that may lead to the concealment of illegal payments or give them the appearance of legality.

Actions or conduct to be avoided

Corruption may be prevented by complying with the Unibaltic Group Code of Business Conduct and Ethics and the provisions of this Policy. Each person covered by this Policy is required to apply a zero-tolerance approach to all forms of corruption, including bribery and facilitation payments, and to observe the following principles:

- not to offer, give, request or accept any bribes, even if such conduct is suggested by a superior or another person,
- not to engage in fraudulent, dishonest or unfair conduct, or in conduct that may result in a breach of fair business practices,
- not to accept corrupt actions or conduct, nor to ignore potential corrupt conduct by third parties acting on behalf of or for the benefit of Unibaltic,
- not to undertake any actions that could facilitate corruption, including entering into unlawful arrangements, submitting fraudulent claims, falsifying documents or evidence, or giving false testimony in proceedings,
- not to conceal corrupt activity or actions that may indicate a risk of corruption,
- not to consent to accepting or giving prohibited gratuities, as they are inconsistent with the law, this Policy and Unibaltic's values,
- to exercise due diligence when selecting agents, contractors and other third-party service providers, both at the stage of establishing cooperation and throughout the business relationship,
- to ensure that all agreements concluded with third parties are made in writing and contain an undertaking to comply with the provisions of this Policy.

Extortion

Unibaltic acknowledges that demands of a corrupt nature may, in certain circumstances, be connected with extortion, including — in extreme cases — a threat of violence or personal harm. Subject to situations in which an employee's life, health or safety is directly endangered, extortion shall not constitute a circumstance justifying the payment of a bribe.

If the threat concerns only the interests of the Group, and not the life, health or safety of an employee, any payment made shall be treated as an impermissible benefit of a corrupt nature. However, if a payment was made in good faith, in a justified belief that there was a direct threat to life, health or safety, this fact must be reported without delay to the Chief Compliance Officer. In such situations, employees should act with due prudence, while respecting the standards applicable at Unibaltic and seeking to limit the risk to life, health and safety.

Gifts and entertainment

Gifts

When offering, giving or accepting gifts, anti-bribery and anti-corruption laws applicable in the jurisdictions in which the Group conducts its business must be taken into account in each case. Accordingly, the giving of any gift requires prior assessment of compliance with the relevant provisions of local law and the principles set out in this Policy.

As a general rule, offering any gifts or gratuities to public officials is prohibited. The only exception may be promotional items of minor value, such as inexpensive pens, mugs, T-shirts or calendars bearing the Company's name and logo, provided that their provision is not prohibited by local law and is not intended to exert improper influence on the recipient.

It is also prohibited to offer gifts or provide favours outside the ordinary course of business to current or potential customers, their employees, agents and any other persons with whom the Group has a contractual relationship or conducts negotiations concerning the conclusion of an agreement.

Unibaltic employees are required to refuse gifts and gratuities from persons cooperating or intending to cooperate with Unibaltic, including suppliers and potential suppliers, except for promotional items of minor value. The acceptance or giving of cash gifts is strictly prohibited and, if offered, such gifts must be refused.

Entertainment

Business entertainment, including in particular meetings involving meals and beverages, is permitted provided that it complies with applicable local law, has a legitimate business purpose, remains within reasonable limits, occurs incidentally and — where possible — is based on the principle of reciprocity.

Reporting irregularities

Any actions, omissions or planned conduct that breach or may breach the provisions of this Policy must be reported without delay to the immediate supervisor and to the Chief Compliance Officer. Reports may be made by e-mail (e-mail: coc@unibaltic.eu), by telephone (+357 25357717) or in writing to the following address: UNIBALTIC GROUP, 229 Arch. Makarios III Ave., Meliza Court, 3105 Limassol, Cyprus. In the territory of Poland, reports may also be sent to the following address: UNIBALTIC GROUP, ul. Wojska Polskiego 83, 70-481 Szczecin, Poland.

Consequences of non-compliance

A breach of the provisions of this Policy may result in disciplinary, civil or criminal liability, in accordance with the applicable laws of the relevant jurisdiction. Any Unibaltic employee who breaches this Policy may be subject to disciplinary proceedings, including termination of employment in cases justified by the seriousness of the breach. In the case of third parties, a breach of this Policy may constitute grounds for the immediate termination of cooperation or of the legal relationship connecting them with Unibaltic. Without prejudice to the foregoing, a breach of the Policy may also result in an obligation to remedy any damage and in the application of other measures provided for under applicable law.

Policy review

This Policy shall be reviewed annually by the Chief Compliance Officer in order to ensure that it remains up to date, adequate and effective in relation to the needs of the organisation and applicable requirements.

Conflict of Interest Policy

Policy statement

Employees of the Unibaltic Group (hereinafter: "Unibaltic" or the "Group") are required to perform their duties in an honest, independent, professional manner and in accordance with ethical principles. They are also required to avoid any actual, potential or perceived conflicts of interest and to report such situations without delay to their immediate supervisor and to the Chief Compliance Officer.

Application

This Policy applies to all Unibaltic employees, as well as to third parties and partners conducting business with or on behalf of the Group. All persons covered by this Policy are required to comply with its provisions and to act in a manner that prevents the occurrence of conflicts of interest.

Definition

A conflict of interest occurs where the personal interest of a person or entity affects, may affect, or may be perceived as affecting impartiality, objectivity or independence in the performance of professional duties. Such a conflict may arise in particular from financial benefits, status, knowledge, personal or professional relationships, as well as reputational considerations.

A conflict of interest does not necessarily involve an intention to breach official duties or to cross the boundary between the professional and private sphere. It may be not only **actual**, but also:

- **potential** – where, based on the circumstances, its occurrence may reasonably be anticipated, although it has not yet materialised in practice,
- **perceived** – where, from the perspective of a reasonable person, the circumstances may give the impression of influencing the manner in which duties towards Unibaltic are performed, irrespective of whether a conflict actually exists.

The mere existence of a personal, family or social relationship between Unibaltic employees or another person connected with Unibaltic does not in itself constitute a conflict of interest. The assessment of whether a conflict exists must in each case take into account the specific circumstances of the relevant situation.

Actions or conduct to be avoided

Persons covered by this Policy are required to avoid situations, actions and conduct that may lead to an actual, potential or perceived conflict of interest. This applies in particular to the following areas:

a) Personal interest

Employees are required to ensure that their personal interests do not conflict with the interests of Unibaltic and do not influence decisions concerning current or potential competitors, customers, partners, sellers, suppliers or other business entities in which they hold a direct or indirect financial interest. In particular, it is prohibited to:

- participating in decision-making or influencing Unibaltic's decisions concerning an entity in which the employee holds a direct or indirect financial interest,
- using Unibaltic premises, equipment, resources or services of other Unibaltic employees for the purpose of pursuing personal interests,
- using confidential information for personal gain, both during employment and after its termination,
- remaining in a situation in which the employee may directly or indirectly derive benefits from business transactions carried out by Unibaltic, in particular as a supplier of goods or services, a party to an agreement or a partner in a venture,
- giving preferential treatment to a supplier or another person conducting business with Unibaltic for the purpose of pursuing personal interests.

b) Family, friends and romantic relationships

Employees and persons holding managerial positions may not use their position, authority or professional relationships for the purpose of pursuing their own personal interests or the interests of persons with whom they have family, personal, social or romantic relationships. In particular, it is prohibited to:

- use one's position or professional contacts within Unibaltic to promote one's own interests or the interests of family members or other persons with whom the employee has a close personal or professional relationship,
- participate in decision-making or influence decisions concerning business transactions that may benefit a relative, close friend or an enterprise with which such person is connected or in which such person holds a direct or indirect financial interest.

If an employee becomes aware that Unibaltic intends to employ their relative or a person with whom they are in a romantic relationship in a position that would be directly subordinate to that employee, the employee is required to disclose this circumstance without delay to their immediate supervisor and to the Chief Compliance Officer.

If, during employment, a romantic relationship arises between Unibaltic employees who are within a direct or indirect reporting line, both persons are required to disclose this circumstance without delay. Failure by a person holding a managerial position to make such a disclosure may constitute grounds for the application of appropriate disciplinary measures.

c) Relationships and favouritism

Employees must not grant, or create the appearance of granting, preferential treatment to any person with whom they have a close personal or professional relationship. Relationships that existed in the past may also, in certain circumstances, give rise to a perceived conflict of interest and require appropriate assessment.

If an employee is in a position to make a decision directly or indirectly concerning a person with whom they have a close personal or professional relationship, in particular in matters relating to employment, performance evaluation, disciplinary liability, promotion, remuneration, other discretionary benefits or the award of a contract, the employee is required to:

- disclose the potential conflict of interest to their supervisor and to the Chief Compliance Officer,
- refrain from making recommendations, opinions or other statements that may influence the resolution of the matter.

Identification and disclosure of conflicts of interest

All employees and third parties acting on behalf of or for the benefit of the Group are required to identify, disclose and appropriately manage any actual, potential or perceived conflict of interest that may concern them.

If an employee has a reasonable suspicion that they are in a situation which may constitute an actual, potential or perceived conflict of interest, they are required to discuss this situation without delay with the Chief Compliance Officer. For this purpose, a conflict of interest disclosure form should be submitted, enabling a full assessment of the situation and determination as to whether a conflict of interest actually exists. The disclosure should include at least the following information:

- the full name of the person making the disclosure,
- an indication of the source and cause of the conflict of interest,
- an indication of the person or entity to which the conflict of interest relates.

Until the assessment of the disclosed situation has been completed, the person making the disclosure is required to refrain from participating in the decision-making process to which the conflict may relate.

Management of conflicts of interest

If the Chief Compliance Officer determines that an actual, potential or perceived conflict of interest exists, they shall prepare a plan for managing such conflict. This plan shall be discussed with the employee concerned, who is required to comply with it. The plan requires approval by the Company's Management Board.

The conflict of interest management plan should ensure appropriate mitigation of risk and effective management of the conflict, taking into account the nature of the specific situation. Depending on the circumstances, it may include in particular the following measures:

- recording and disclosing conflicts of interest, ensuring that all information relating to the relevant conflict has been reported and properly documented; the Company should maintain a register of conflicts of interest,
- limiting the employee's involvement in the relevant matter, changing the scope of duties, changing the reporting relationship or restricting access to specific information,
- assigning oversight over all or part of the process to another impartial manager,
- excluding the employee from the relevant matter, in particular from a recruitment or decision-making process,
- the employee's withdrawal from the private interest giving rise to the conflict; where this is not possible, in particular due to family relationships, and the conflict

cannot be resolved otherwise, the employee should fully withdraw from the relevant process.

Conflict of interest management plans, including disclosure forms, should be reviewed annually to ensure that they remain up to date and effective.

Consequences of non-compliance

Failure to comply with the provisions of this Policy may result in disciplinary liability, including termination of employment, taking into account the nature and seriousness of the breach. All persons covered by this Policy are required to familiarise themselves with its content and to comply with it.

Reporting irregularities

Any actions, omissions or planned conduct that breach or may breach the provisions of this Policy must be reported without delay to the immediate supervisor and to the Chief Compliance Officer. Reports may be made by e-mail (e-mail: coc@unibaltic.eu), by telephone (+357 25357717) or in writing to the following address: UNIBALTIC GROUP, 229 Arch. Makarios III Ave., Meliza Court, 3105 Limassol, Cyprus. In the territory of Poland, reports may also be sent to the following address: UNIBALTIC GROUP, ul. Wojska Polskiego 83, 70-481 Szczecin, Poland.

Policy review

This Policy shall be reviewed annually by the Chief Compliance Officer in order to ensure that it remains up to date, adequate and effective in relation to the needs of the organisation and applicable requirements.

Know Your Counterparty Policy (KYC)

Policy statement

Verification of a potential counterparty constitutes a preventive measure aimed at limiting the risk of establishing or maintaining a business relationship with an unreliable or dishonest entity, or with an entity acting contrary to the law, good business practices or the standards adopted within the Unibaltic Group. Risks associated with cooperation with such an entity may include, in particular, non-performance or improper performance of an agreement, failure to pay for services provided, participation — including unintentional participation — in tax fraud, breach of sanctions regulations, as well as financial losses or reputational damage.

The Unibaltic Group undertakes to conduct the verification process of potential customers in accordance with this Policy, with due diligence and on the basis of information and documents originating from reliable sources. The purpose of the verification is to ensure that, before cooperation is established, each potential counterparty is subject to an adequate assessment of possible risks.

Application

This Policy applies to all employees of the Unibaltic Group, as well as to third parties and business partners acting for the benefit of the Group or maintaining commercial relationships with it. All persons covered by this Policy are required to comply with its provisions and to cooperate in the process of identifying and mitigating risks connected with establishing and maintaining business relationships with counterparties.

Before commencing cooperation with an external entity, the relevant employee is required to initiate the verification process by sending the appropriate KYC form to the counterparty (the template of which constitutes Appendix No. 1 to this Policy). Upon receipt of the required information and documents, the verification process is conducted by the Chief Compliance Officer, who assesses the counterparty in accordance with the principles set out in this Policy.

If a potential customer refuses to complete the KYC form or persistently fails to respond to verification-related inquiries, each such entity must be verified on the basis of publicly available information. Subsequently, before a decision is made to establish cooperation, an appropriate risk assessment must be carried out. Each such case should be considered individually in consultation with the head of the relevant department and the Chief Compliance Officer. In the case of agreements with a value exceeding EUR 15,000, consent to commence cooperation must be granted by the Management Board.

Purpose of the Policy

The purpose of this Policy is to establish uniform rules for the verification of counterparties before cooperation is established and during the course of the business relationship. This Policy is intended to ensure that decisions concerning cooperation are made in an informed and documented manner and are preceded by an assessment of the risks associated with the relevant counterparty. In particular, this Policy aims to:

- reduce the risk of cooperation with entities acting contrary to the law, good practices or fair commercial practices,

- ensure that due diligence is exercised when making a decision to enter into an agreement,
- reduce the risk of unintended involvement in tax fraud, money laundering, sanctions violations or other unlawful activities,
- exclude from cooperation entities subject to sanctions or connected with persons or entities subject to sanctions,
- protect the legal, financial and reputational interests of the Unibaltic Group.

Verification and onboarding processes

Verification activities should be carried out both before entering into an agreement with a counterparty and — in justified cases — during the course of the business relationship. The scope of verification should be adequate to the nature of the cooperation, the counterparty's profile, country of registration, ownership structure, business activity and potential risks.

During the course of cooperation, the assessment of the counterparty should take into account any changes in its ownership structure, manner of conducting business, financial standing, business links, sanctions status and any other circumstances that may affect the level of risk for the Unibaltic Group.

Before commencing verification, the information obligation must be fulfilled towards natural persons whose personal data will be processed as part of the KYC process. This obligation arises from Regulation (EU) 2016/679 of the European Parliament and of the Council, i.e. the GDPR, and includes, in particular, informing such persons about:

- the categories of personal data processed,
- the legal basis for processing the data,
- the purpose of processing the data,
- the data retention period,
- the recipients of the data, where the data may be disclosed to them,
- the rights of the data subjects.

Scope of information obtained as part of KYC

After the information obligation has been fulfilled, the Chief Compliance Officer may commence the counterparty verification process on the basis of information obtained through the KYC form and documents provided by the counterparty. The scope of required information should include in particular:

- the full legal name of the counterparty,
- the registration number or other identification number,
- the registered office address and contact details,
- the date of incorporation or registration,
- the principal business activity,
- the ownership structure,
- details of persons forming part of the management bodies,
- details of the ultimate beneficial owners,
- the VAT number or other tax identification number,
- bank details,
- information concerning any links with public officials or politically exposed persons,

- information necessary to conduct sanctions screening.

Where access to the business register competent for the counterparty's country of registration is restricted, the counterparty should be requested to provide current registration documents or other documents confirming its legal status.

Verification of information

All information obtained in the course of the KYC process should be verified on the basis of documents or data originating from reliable and independent sources. Verification should include, in particular, checking the counterparty's registration details, tax status, ownership structure, ultimate beneficial owners, bank details and sanctions status.

Depending on the counterparty's country of registration and the availability of data, verification may be carried out using official public registers, tax registers, sanctions databases, information made available by competent public administration authorities, the counterparty's website, its social media profiles and other reliable sources of information.

Due diligence levels

On the basis of the information and documents collected, the Chief Compliance Officer assesses the counterparty in terms of risk level. This assessment should take into account, in particular, the nature of the counterparty's business, its country of registration, ownership structure, scope of the intended cooperation, history of relations with the Group, tax status, market reputation and any links with persons or entities subject to sanctions.

For the purposes of this Policy, counterparties are classified as low-risk or high-risk entities. Simplified due diligence shall be applied to low-risk counterparties. Re-verification of such counterparties should be carried out at least once every two years, unless circumstances arise earlier that justify updating the data. Enhanced due diligence shall be applied to high-risk counterparties. It includes an in-depth analysis of the counterparty, additional verification of its ownership structure, ultimate beneficial owners, business links, financial standing, sanctions status and media information. The data of high-risk counterparties should be updated at least once a year or more frequently where justified by the level of risk.

Sanctions screening of the counterparty

As part of the KYC process, the Chief Compliance Officer verifies the counterparty, persons forming part of its management bodies, ultimate beneficial owners and — in justified cases — other entities or persons connected with the counterparty in order to determine whether they are subject to sanctions or have links with persons or entities subject to sanctions.

Sanctions screening should be carried out before cooperation with the counterparty is established and should also be repeated during the course of the business relationship, in particular in the event of a change in the ownership structure, a change in the ultimate beneficial owners, a change in the nature of the cooperation, the occurrence of new circumstances increasing the level of risk, or an update of the relevant sanctions lists.

The screening should include, at a minimum, checking the counterparty and the persons and entities connected with it against the relevant sanctions lists, in particular those maintained by:

- the Office of Foreign Assets Control of the United States of America (OFAC),
- the United Nations Security Council,
- the European Union,
- the Office of Financial Sanctions Implementation of the United Kingdom (OFSI),
- the Minister of the Interior and Administration of the Republic of Poland.

If it is established that the counterparty, a person forming part of its management bodies, the ultimate beneficial owner or another person or entity connected with the counterparty appears on a sanctions list or is connected with a person or entity subject to sanctions, cooperation with such counterparty is prohibited. If such circumstance is identified during the course of cooperation, the matter should be referred without delay to the Chief Compliance Officer for an assessment of further actions, including the suspension or termination of cooperation.

The result of the sanctions screening should be appropriately documented and retained in accordance with the rules set out in this Policy and with due regard to applicable personal data protection laws.

Data collection

All information and documents obtained as part of the verification process conducted under this Policy shall be collected, processed and retained in compliance with generally applicable laws, including in particular the GDPR and the Company's privacy policy. The Chief Compliance Officer is required to ensure that the documentation of the verification process is maintained in a reliable, complete manner and in a form which — in justified cases — enables the Unibaltic Group to demonstrate that due diligence has been exercised.

For evidentiary purposes, the results of the verification, including information, documents, statements and findings made in the course of the KYC process, should be recorded in a reliable and complete manner that enables the course of the activities performed to be demonstrated. Materials collected as part of the verification process shall be retained in electronic form for a period of 5 years from the date of completion of the verification or from the date of termination of cooperation with the counterparty, whichever occurs later.

Decision-making regarding cooperation

After completion of the counterparty verification process in accordance with the principles set out in this Policy, the Chief Compliance Officer assesses the result of the verification and the level of risk associated with establishing cooperation. The decision to commence cooperation is made by the person who initiated the verification process, following the positive completion of the KYC process.

If circumstances are identified that may indicate increased legal, financial, reputational, tax or sanctions risk, the decision to establish cooperation should be preceded by additional analysis and, in justified cases, consultation with the Company's Management Board. Cooperation with a counterparty that has not successfully completed the verification process may not be established.

Reporting irregularities

Any actions, omissions or planned conduct that breach or may breach the provisions of this Policy must be reported without delay to the immediate supervisor and to the Chief Compliance Officer. Reports may be made by e-mail (e-mail: coc@unibaltic.eu), by

telephone (+357 25357717) or in writing to the following address: UNIBALTIC GROUP, 229 Arch. Makarios III Ave., Meliza Court, 3105 Limassol, Cyprus. In the territory of Poland, reports may also be sent to the following address: UNIBALTIC GROUP, ul. Wojska Polskiego 83, 70-481 Szczecin, Poland.

Consequences of non-compliance

A breach of the provisions of this Policy may result in the application of appropriate disciplinary, organisational or legal measures, proportionate to the nature, seriousness and consequences of the breach. In the case of employees of the Unibaltic Group, the consequences may include, in particular, the initiation of disciplinary proceedings and, in justified cases, termination of employment.

With respect to counterparties or other external entities, a breach of this Policy, refusal to provide information or documents necessary to conduct verification, provision of false information, or a negative outcome of the KYC process may constitute grounds for refusing to establish cooperation, suspending its performance or terminating it with immediate effect, taking into account the provisions of the relevant agreement and generally applicable laws.

Policy review

This Policy shall be reviewed annually by the Chief Compliance Officer in order to ensure that it remains up to date, adequate and effective in relation to the needs of the organisation and applicable requirements.

Appendix No. 1

KYC FORM	
GENERAL INFORMATION	
Entity name	
Date of incorporation	
Registration number	
Registered address	
Principal business activity	
VAT number	
Bank account details (bank name, IBAN, SWIFT)	
Does any public official or politically exposed person (PEP) hold any ownership/financial interest or management position in your organisation?	
OWNERSHIP STRUCTURE AND MANAGEMENT	

Management Board	
Ownership structure	
Ultimate beneficial owner	

CODE OF BUSINESS CONDUCT AND ETHICS

The counterparty shares the values and principles described in the Unibaltic Group Code of Business Conduct and Ethics.

SANCTIONS

The undersigned (hereinafter referred to as the "Charterer") hereby undertakes to comply with sanctions imposed by the EU, the USA, the UK and the UN, including sanctions imposed on Russia in connection with the war waged against Ukraine. Furthermore, the Charterer undertakes to exercise enhanced due diligence when verifying the origin of the cargo and the entities connected with any Russian links.
The Charterer confirms that the cargo is not of Russian origin ☒
The Charterer confirms that no Russian entity/person subject to sanctions participates in this carriage or is connected with it ☒

By signing this document:

a. you declare that the information contained herein is true and up to date,
b. you confirm that the information obligation arising from the GDPR has been provided to you,
c. you consent to the disclosure of the above information, in particular personal data, for the purpose of enabling the Unibaltic Group to exercise due diligence, and you warrant that you will inform the relevant persons about the transfer of their data to the Unibaltic Group in connection with the pursuit of its legitimate interests and about the recording and processing of such data for this purpose,
d. you declare that you are duly authorised to make declarations of intent on behalf of the entity.

Full name:
Position:
Place:
Date:
Signature:

Supplier Code of Conduct

This Code sets out the fundamental standards of conduct which the Unibaltic Group expects from its suppliers and other entities cooperating within the supply chain. Its purpose is to ensure that suppliers conduct their business in accordance with the values adopted by the Unibaltic Group, in particular with regard to ethical business conduct, respect for human rights and labour rights, environmental protection, integrity and compliance with the principles arising from the Code of Business Conduct and Ethics, the current version of which is available on the Company's website.

The Unibaltic Group exercises the highest level of due care in its business operations and expects the same approach from its suppliers. By accepting this Code, suppliers confirm that they have familiarised themselves with the values and standards set out in the Code of Business Conduct and Ethics, that they share them and undertake to comply with them, including within their own supply chain.

Suppliers of the Unibaltic Group undertake to conduct their business in accordance with applicable laws, ethical standards and the principles set out in this Code. In particular, suppliers undertake to comply with the following requirements:

1. Labour practices and standards
Suppliers undertake to:

- apply a zero-tolerance approach to child labour, human trafficking, modern slavery, discrimination, forced labour and all other forms of violations of human rights and labour rights;
- conduct their business in accordance with generally applicable laws, relevant regulations and recognised international standards concerning labour law and the protection of human rights, including the principles of the United Nations Global Compact;
- ensure a safe and healthy working environment, with due regard to applicable occupational health and safety requirements.

2. Environmental protection
Suppliers undertake to:

- comply with generally applicable laws and regulations concerning environmental protection;
- conduct their business with due regard to its impact on the natural environment and undertake measures aimed at limiting adverse environmental effects, to the extent appropriate to the nature and scale of their business activities.

3. Ethics and compliance
Suppliers undertake to:

- apply a zero-tolerance approach to corruption, bribery, facilitation payments, money laundering and any other activities inconsistent with the law or ethical standards;
- exercise due diligence when selecting and verifying their own suppliers, subcontractors and other business partners;

- promptly inform the Unibaltic Group of any actual, potential or perceived conflicts of interest that may affect cooperation with the Group;
- refrain from conducting business with persons or entities subject to sanctions or connected with persons or entities subject to sanctions.

Any actions, omissions, suspicions or information indicating a breach or possible breach of the provisions of this Code should be reported without delay to the Chief Compliance Officer. Reports may be made by e-mail to: coc@unibaltic.eu, by telephone at: +357 25357717, or in writing to the following address: UNIBALTIC GROUP, 229 Arch. Makarios III Ave., Meliza Court, 3105 Limassol, Cyprus. In the territory of Poland, reports may also be sent to the following address: UNIBALTIC GROUP, ul. Wojska Polskiego 83, 70-481 Szczecin, Poland.

DECLARATION

We hereby confirm that we have read the Unibaltic Group Supplier Code of Conduct and undertake to comply with its provisions on behalf of the entity indicated below.

Company name: …….
Full name of representative: …….
Place and date: …….

Whistleblower Protection Policy and Procedure

Policy statement

The Unibaltic Group is committed to conducting its business in compliance with generally applicable laws, internal regulations, principles of integrity and transparency, and the highest ethical standards. An element of this commitment is to ensure safe, confidential and effective channels for reporting breaches, irregularities or reasonable suspicions thereof.

The purpose of this Policy is to enable persons covered by its scope to report breaches in a manner ensuring protection against retaliation, protection of the confidentiality of identity and reliable handling of the report. The Unibaltic Group undertakes to take appropriate follow-up actions where breaches are confirmed and to prevent all forms of retaliation against persons making reports in good faith.

This Policy applies exclusively to companies governed by Cypriot law belonging to the Unibaltic Holding Group. A separate procedure has been developed for Unibaltic Sp. z o.o., adapted to the requirements of Polish law, and constitutes an appendix to this Policy.

Purpose of the Policy

The purpose of this Policy is to define the rules for reporting breaches, irregularities or reasonable suspicions thereof connected with the activities of the Unibaltic Group, as well as the rules for protecting persons making such reports.

This Policy is intended, in particular, to ensure safe and confidential channels for reporting breaches, enable the early identification and reliable verification of irregularities, ensure the protection of whistleblowers against retaliation, define the rules for conducting investigations and follow-up actions, and limit legal, organisational, financial and reputational risks connected with breaches of generally applicable law, the Code of Business Conduct and Ethics, and the internal policies and procedures of the Group.

This Policy also defines the manner of reporting breaches, the rules for receiving and examining reports, the protection measures available to whistleblowers, and the rules for providing information on follow-up actions taken.

Application

This Policy applies to persons who have obtained information about a breach or a reasonable suspicion of a breach in a context connected with work or cooperation with the Unibaltic Group.

The scope of this Policy includes, in particular, current and former employees of the Company, persons applying for employment, members of company bodies, shareholders, volunteers, trainees, persons providing services under civil law contracts, as well as contractors, suppliers, subcontractors and other persons or entities cooperating with the Group.

This Policy also applies to persons assisting in making a report, persons connected with the whistleblower, and legal entities or other organisational units assisting the whistleblower or connected with them, to the extent provided for by the applicable laws.

Definitions

Whistleblower means a natural person who reports or publicly discloses information about a breach obtained in a context connected with work or cooperation with the Unibaltic Group, acting in good faith and having reasonable grounds to believe that the information reported is true at the time of making the report.

Facilitator means a natural person who assists a whistleblower in making a report or disclosure in a work-related context, in particular by providing organisational, informational or technical support.

Report means the oral, telephone, electronic or written provision of information concerning a breach or a reasonable suspicion of a breach. A report made within the Unibaltic Group constitutes an internal report, a report submitted to the competent authority constitutes an external report, whereas making information available to the public constitutes a public disclosure.

Breach / irregularity means an act or omission that is contrary to law, ethical principles, the Code of Business Conduct and Ethics, policies and procedures of the Unibaltic Group, as well as any other conduct that may affect the legal, financial, organisational or reputational interest of the Group.

Retaliation means any direct or indirect act or omission, occurring in a work-related or cooperation-related context, caused by an internal report, external report or public disclosure, which causes or may cause unjustified harm to the whistleblower or another person covered by protection.

EU law means Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, as well as other relevant acts of European Union law falling within the scope of that Directive.

National law means the provisions of Cypriot law implementing Directive (EU) 2019/1937, as well as other provisions of national law applicable to the reporting of breaches and the protection of reporting persons.

Reporting breaches

A person who has reasonable grounds to suspect the occurrence of a breach, irregularity or other improper conduct connected with the activities of the Unibaltic Group should make a report in accordance with the rules set out in this Policy. A report may be submitted to the immediate supervisor, who shall promptly inform the Chief Compliance Officer thereof, or directly to the Chief Compliance Officer.

Reports may be made orally, by telephone, electronically or in writing, using the following contact channels: e-mail address: coc@unibaltic.eu, telephone number: +357 25357717, correspondence address: UNIBALTIC GROUP, 229 Arch. Makarios III Ave., Meliza Court, 3105 Limassol, Cyprus. In the territory of Poland, reports may also be sent to the following address: UNIBALTIC GROUP, ul. Wojska Polskiego 83, 70-481 Szczecin, Poland.

The report should, where possible, contain information enabling its reliable assessment and the undertaking of follow-up actions, in particular:

- the whistleblower's details and contact details, unless the report is anonymous;
- details of the person to whom the report relates, if known;
- a description of the breach or irregularity together with the factual circumstances;
- an indication of the date and place of the event, if known;
- an indication of persons who may have knowledge of the matter, if known;
- documents, evidence or other information that may facilitate verification of the report.

Anonymous reports may be accepted. If a report is made by telephone, the Chief Compliance Officer — with the consent of the reporting person — records its content by preparing a full and accurate record of the conversation. In the case of a non-anonymous report, the reporting person is given the opportunity to review, correct and approve the record of the conversation by signing it.

Reports to the competent external authority

Irrespective of the possibility of making an internal report, irregularities falling within the competence of the Cypriot Shipping Deputy Minister may be reported directly to that authority. Reports may be submitted by e-mail to: whistleblowers@dms.gov.cy, by telephone at: +357 25848263, or by traditional mail to the following address: Cyprus Shipping Deputy Ministry, Kyllinis Street, Mesa Geitonia, 4007 Limassol, Cyprus, in a sealed envelope marked "CONFIDENTIAL".

A report concerning a breach of European law should, where possible, include:

- details of the reporting person, including full name and contact details;
- details of the person or entity to whom the report relates;
- a description of the breach, including an indication of the relevant provisions and factual circumstances;
- documents or other materials supporting the report, if held by the reporting person.

A detailed list of legal acts falling within the competence of the Shipping Deputy Minister was published in Circular No. 8/2024 of 28 February 2024, available on the website of the competent authority.

External report and public disclosure

In addition to an internal report and a report to the competent sectoral authority, the reporting person may — under the terms set out in the applicable laws — make an external report to the competent public authority or make a public disclosure.

An external report means the provision of information about a breach to the competent public authority. Public disclosure means making information about a breach available to the public. The protection provided for under this Policy shall apply to a person making an external report or public disclosure only to the extent and under the conditions laid down in the applicable laws.

Investigation procedure

The Chief Compliance Officer confirms receipt of the report to the whistleblower within 7 days from the date of its receipt, unless the whistleblower has not provided contact details enabling such confirmation to be delivered.

Upon receipt of a report, the Chief Compliance Officer conducts a preliminary assessment to determine whether the report falls within the scope of this Policy and whether it contains sufficient information to undertake further actions. If the report is manifestly unfounded, does not concern matters covered by this Policy, or it is not possible to obtain the information necessary to conduct the proceedings, the Chief Compliance Officer may discontinue further processing of the report. The whistleblower shall be informed of this decision, provided that the whistleblower has provided contact details enabling feedback to be delivered.

If the report requires further clarification, the Chief Compliance Officer initiates an investigation and undertakes follow-up actions adequate to the nature and circumstances of the matter. Feedback concerning planned or undertaken follow-up actions should be provided to the whistleblower within 3 months from the date of confirmation of receipt of the report, provided that the whistleblower has provided contact details.

In the course of the investigation, the Chief Compliance Officer is authorised to review documents and information connected with the report, including documents containing confidential information or constituting business secrets, to the extent necessary to clarify the matter. The Chief Compliance Officer may request explanations from employees or associates of the Unibaltic Group who may have knowledge relevant to the matter, and may also undertake other actions necessary to establish the facts.

Employees and associates of the Unibaltic Group are required to cooperate with the Chief Compliance Officer in the course of the investigation, in particular by providing explanations and submitting documents and information in their possession. Any difficulties in obtaining the required information or documents should be reported without delay to the Company's Management Board.

In justified cases, the Chief Compliance Officer may conduct an interview with the whistleblower in order to clarify the reported information, as well as with the person to whom the report relates, in order to enable that person to present their position. Such interviews should be recorded in the form of an internal note or minutes, with due regard to confidentiality and personal data protection principles.

After completion of the investigation, the Chief Compliance Officer assesses the material collected, establishes the facts and determines whether the breach covered by the report has occurred. Where a breach is confirmed, the Chief Compliance Officer recommends or undertakes — within the scope of their competence — follow-up actions, in particular:

- calling upon the persons responsible to cease actions leading to a breach of law, policies or procedures;
- indicating the actions necessary to remedy the breach, repair the damage or reduce the risk of its recurrence;
- submitting a request to the Company's Management Board to take appropriate actions against the persons responsible, including a change of position, change of scope of duties, application of disciplinary measures or termination of the agreement;
- notifying the competent public authority if the nature of the matter justifies such action or where this results from applicable laws.

If the breach is not confirmed, the Chief Compliance Officer closes the investigation, recording the reasons for such decision in the register of reports.

Register of reports

The Chief Compliance Officer shall maintain a register of all reports made under this Policy, in compliance with the principles of confidentiality, data integrity and restricted access to information covered by the report. The register is intended to ensure proper recording of reports, the course of investigations and the follow-up actions taken.

Documents, information and materials collected in connection with a report and the investigation conducted shall be retained for a period of 5 years from the date of completion of the investigation, unless a longer retention period results from generally applicable laws or is necessary for the establishment, exercise or defence of claims.

The register should include in particular:

- case number;
- date of receipt of the report;
- details of the whistleblower, if disclosed;
- details of the person to whom the report relates, if known;
- subject matter of the report and a brief description of the reported circumstances;
- information on how the report was handled;
- case status;
- follow-up actions taken and the date of case closure.

Protection of identity

The Unibaltic Group ensures the protection of the confidentiality of the identity of the whistleblower, the person to whom the report relates, and other persons identified in the report, in accordance with the applicable laws, the Group's Privacy Policy and Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR). Access to personal data and information enabling the identification of such persons may be granted only to authorised persons and only to the extent necessary to receive the report, conduct an investigation or undertake follow-up actions.

The identity of the whistleblower may be disclosed only with the whistleblower's express consent or in cases where the obligation to disclose results from generally applicable laws. Where it is necessary to disclose the whistleblower's identity to the competent public authority, the whistleblower should be informed thereof before the disclosure is made, unless providing such information could jeopardise the ongoing proceedings or is excluded by law.

A report may be made anonymously. In such a case, the reporting person benefits from the protection provided for under this Policy to the extent that such protection can be applied. At the same time, the Unibaltic Group indicates that the absence of contact details may hinder the verification of the report, obtaining additional explanations, providing feedback and ensuring full protection against retaliation.

Protection of whistleblowers

A whistleblower shall be entitled to the protection provided for under this Policy if, at the time of making the report, they had reasonable grounds to believe that the information reported was true and that it concerned a breach falling within the scope of this Policy. Protection shall apply irrespective of whether the report was made internally, externally or — in cases provided for by law — by way of public disclosure.

The scope of protection includes, in particular, protection of the confidentiality of the whistleblower's identity, the prohibition of retaliation, attempts or threats of retaliation, as well as the obligation to ensure that a report made in good faith does not result in unjustified adverse consequences in the area of employment, cooperation or business relations.

The Unibaltic Group does not tolerate any form of retaliation, reprisals, discrimination or other unjustified adverse treatment against a whistleblower, a person assisting in making a report, a person connected with the whistleblower or other persons participating in the investigation. Any such action may constitute a breach of this Policy and may result in the application of appropriate disciplinary, organisational or legal measures.

Protection shall not apply to a person who makes a report in bad faith, in particular by knowingly providing false or misleading information or by making a report with the purpose of causing harm to another person or to the Unibaltic Group. Making such a report may result in disciplinary, civil or criminal liability, in accordance with the applicable laws.

Retaliation

It is prohibited to take any retaliation, attempt to take retaliation or threaten retaliation against a whistleblower, a person assisting in making a report, a person connected with the whistleblower or any other person covered by protection. Retaliation may include in particular:

- refusal to establish an employment relationship,
- termination of employment with or without notice,
- failure to conclude a fixed-term or indefinite-term employment contract after the probationary period, or failure to conclude another contract, despite a justified expectation that such contract would be concluded,
- reduction of remuneration,
- withholding promotion or being omitted for promotion,
- being omitted when work-related benefits are granted or having such benefits reduced,
- transfer to a lower position,
- suspension from the performance of official duties,
- transfer of existing duties to another employee,
- an unfavourable change in the place of work or work schedule,
- a negative performance assessment or work opinion,
- imposition of a disciplinary penalty or another measure of a similar nature,
- coercion, intimidation, exclusion, mobbing or discrimination,
- withholding participation in training or being omitted when referred for training,
- unjustified referral for medical examinations, including psychiatric examinations,
- actions hindering the finding of employment in a given industry or sector,
- causing financial loss, including loss of income,

- causing non-material damage, including damage to reputation, particularly on social media.

The actions indicated above shall not be considered retaliation if they were taken for objective, duly justified and documented reasons unrelated to the making of an internal report, external report or public disclosure.

The prohibition of retaliation and the protection of confidentiality of identity shall also apply to:

- a person assisting in making a report;
- a person connected with the whistleblower;
- a legal person or another organisational unit assisting the whistleblower or connected with them, in particular one owned by the whistleblower or employing them.

Any suspicion of retaliation should be reported without delay to the Chief Compliance Officer. The Unibaltic Group treats such reports with due seriousness and takes measures aimed at their prompt verification and the application of appropriate remedial measures.

GDPR information clause

The controller of personal data processed in connection with receiving and examining reports and conducting investigations is the Unibaltic Group. Personal data shall be processed in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR").

Personal data shall be processed for the purpose of receiving reports, verifying the information provided in a report, conducting an investigation, undertaking follow-up actions and fulfilling the legal obligations imposed on the Controller. The legal basis for processing is Article 6(1)(c) GDPR, i.e. the necessity of processing for compliance with a legal obligation to which the Controller is subject. To the extent that data processing goes beyond obligations arising from the law, the basis for processing may be the consent of the data subject, in accordance with Article 6(1)(a) GDPR.

Personal data may include, in particular, data of the whistleblower, the person to whom the report relates, persons identified in the report, persons participating in the investigation and other persons whose data prove necessary for the reliable verification of the report.

Access to personal data may be granted only to persons authorised to receive reports, conduct investigations or undertake follow-up actions, as well as to entities or authorities authorised under generally applicable laws. Data may be disclosed only to the extent necessary to achieve the purpose of processing or to fulfil legal obligations imposed on the Controller.

Personal data shall be retained for a period of 5 years from the date of completion of the proceedings, unless a longer retention period results from generally applicable laws or is necessary for the establishment, exercise or defence of claims.

Personal data shall not be processed by automated means, including profiling, nor shall they be transferred to a third country or an international organisation, unless such an obligation arises from generally applicable laws.

Data subjects shall have the rights provided for under the GDPR, including the right of access to data, the right to rectification, the right to restriction of processing and the right to lodge a complaint with the competent supervisory authority, subject to limitations resulting from laws concerning whistleblower protection, the confidentiality of reports and the protection of the identity of persons participating in the proceedings.

Consequences of non-compliance

A breach of the provisions of this Policy may result in the application of appropriate disciplinary, organisational or legal measures, proportionate to the nature, seriousness and consequences of the breach. In the case of employees of the Unibaltic Group, the consequences may include, in particular, the initiation of disciplinary proceedings and, in justified cases, termination of employment.

If a breach may constitute a prohibited act, give rise to civil liability or amount to another breach of generally applicable laws, the Unibaltic Group may take further action, including notifying the competent public authorities or pursuing its claims in accordance with the applicable laws.

Policy review

This Policy shall be reviewed annually by the Chief Compliance Officer in order to ensure that it remains up to date, adequate and effective in relation to the needs of the organisation and applicable requirements.

Appendix No. 1

All employees of Unibaltic Sp. z o.o., regardless of the basis of employment, are required to comply with the following procedure.

Procedure
for reporting breaches of law and protecting whistleblowers
in Unibaltic spółka z ograniczoną odpowiedzialnością in Szczecin

§ 1 General provisions

This Procedure sets out the rules for:

1. making internal reports concerning breaches of law;
2. ensuring protection for persons making such reports.

§ 2 Definitions

For the purposes of the Procedure, the following definitions shall apply:

1. **Company** – Unibaltic spółka z ograniczoną odpowiedzialnością in Szczecin, KRS 0000115954;
2. **Management Board** – the Management Board of Unibaltic spółka z ograniczoną odpowiedzialnością in Szczecin;

3. **Whistleblower** – a person providing information on a breach of law;
4. **Report** – internal information on a breach of law submitted to the Company;
5. **Information on a breach of law** – information or reasonable suspicion concerning an actual or potential breach of law in the Company or in an entity with which the Whistleblower had contact in a work-related context, including in particular:
    a. a suspicion of preparation, attempted commission or commission of a prohibited act,
    b. failure to fulfil duties or abuse of powers by the bodies of a collective entity or by persons acting on behalf of or for the benefit of a collective entity,
    c. failure by the bodies of a collective entity or other persons to exercise due diligence required in the circumstances,
    d. irregularities in the organisation of the activities of a collective entity that could lead to the commission of a prohibited act.
6. **Breach** – an unlawful or unethical act that violates legal provisions, the Company's internal acts, principles of social coexistence, human rights or the Company's interests;
1. **Follow-up action** – actions undertaken by the Company or a public authority in order to verify a report and, where appropriate, to counteract a breach of law;
2. **Retaliation** – any act or omission caused by a report that infringes the rights of the Whistleblower or causes harm to them, in particular:
    - refusal to establish an employment relationship,
    - termination of employment with or without notice,
    - failure to conclude an employment contract after the expiry of a probationary employment contract,
    - reduction of remuneration,
    - withholding promotion or being omitted for promotion,
    - being omitted when other work-related benefits are granted,
    - transfer to a lower position,
    - suspension from the performance of duties,
    - transfer of the Whistleblower's duties to another employee,
    - an unfavourable change in the place of work or work schedule,
    - a negative performance assessment,
    - imposition of disciplinary penalties,
    - coercion, intimidation or exclusion,
    - mobbing,
    - discrimination,
    - withholding or being omitted when referred for training,
    - unjustified referral for medical examinations,
    - actions intended to hinder finding employment in a given sector,
    - causing financial loss or loss of income,
    - causing non-material damage, including damage to the Whistleblower's reputation,
    - an unjustified threat or attempt to take any of the actions listed above.
3. **Person concerned by the report** – a natural person, legal person or organisational unit indicated in the report as responsible for the breach;
4. **Person connected with the reporting person** – a natural person who may experience retaliation, including a co-worker or a family member of the reporting person;
5. **Public disclosure** – making information on a breach of law available to the public;
6. **External report** – provision of information on a breach of law to a public authority;

7. **Commission** – an impartial internal body responsible for examining reports and conducting investigations;
8. **Internal reporting coordinator** – a person responsible for implementing and applying the Procedure, reporting directly to the Company's Management Board.

§ 3 Reports

1. A report may be made by a Whistleblower, who may be:
    - an employee or temporary employee of the Company,
    - a person applying for employment with the Company who obtained information on a breach of law during recruitment or negotiations preceding the conclusion of an agreement,
    - a person providing services to the Company under a civil law agreement,
    - a trainee, volunteer or intern,
    - a shareholder or commercial proxy,
    - an entrepreneur cooperating with the Company.
2. The report may concern breaches of law in particular in the following areas:
    - corruption,
    - public procurement,
    - financial services, products and markets,
    - anti-money laundering and counter-terrorist financing,
    - product safety and compliance,
    - 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 network and information systems,
    - financial interests of the State Treasury, local government units and the European Union,
    - the internal market of the European Union, including competition rules, State aid and corporate taxation,
    - constitutional freedoms and human rights in relations with public authorities.
3. The report shall be confidential, and the data contained therein shall be protected as personal data, unless the Whistleblower gives written consent to their disclosure or the obligation to disclose results from mandatory provisions of law. Personal data shall be processed in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council and other applicable provisions concerning the protection of personal data.
4. The Whistleblower may give written consent to the disclosure of their identity.
5. The Company shall ensure appropriate communication channels enabling reports to be made in a prompt and secure manner.
6. The report may be made:
    - in writing to the registered office address of the Company,
    - by e-mail to the dedicated e-mail address sygnalista@unibaltic.pl in an encrypted file; the password to the file should be provided to the Internal Reporting Coordinator in person or by telephone,

- in person or by telephone to the Internal Reporting Coordinator at +48 605073234.

7. Anonymous reports shall not be examined.
8. The report should include in particular:
   - a description of the breach and data enabling an investigation to be conducted and follow-up actions to be taken, including information or evidence confirming the occurrence of the breach,
   - details of the Whistleblower and other persons who are or may be connected with the report,
   - the approximate period in which the breach occurred,
   - the full name of the employee or the name of the Company department to which the report relates,
   - the preferred method of feedback contact ensuring confidentiality.
9. The report may be made using the form constituting Appendix No. 1 to the Rules.
10. A Whistleblower who has knowledge of the circumstances of the report should, where possible, secure evidence confirming the reported circumstances and provide it to the Commission or indicate where it is stored.

§ 4 Protection of the Whistleblower

1. The Whistleblower shall be protected as provided for in the Rules. No retaliation, attempts at retaliation or threats of retaliation may be taken against the Whistleblower.
2. The Whistleblower's data shall be confidential, unless the Whistleblower gives written consent to their disclosure or the obligation to disclose results from mandatory provisions of law.
3. Access to the Whistleblower's data shall be granted only to the Internal Reporting Coordinator and members of the Commission. Such data may not be disclosed to unauthorised persons.
4. A Whistleblower who makes a report in bad faith shall not benefit from the protection provided for in the Rules.
5. A report shall be deemed to have been made in bad faith if it concerns a breach that did not occur or contains false or misleading information, provided that the Whistleblower knew that such information was false.
6. Obstructing the making of a report, taking retaliation against the Whistleblower, breaching the confidentiality of their data or making a report in bad faith may result in liability under labour law or other applicable legal provisions.

§ 5 Commission

1. The Commission is responsible for examining reports and conducting investigations.
2. The Commission shall consist of three members appointed by decision of the Management Board, upon the request of the Internal Reporting Coordinator. The Coordinator shall submit a request for appointment of the Commission without delay after receiving a report.
3. Only an employee of the Company may be a member of the Commission.
4. The Commission shall elect a Chairperson from among its members.
5. The Commission may not include persons to whom the report relates, the direct superiors of the Whistleblower, or persons remaining in a reporting relationship with the Whistleblower.
6. Each member of the Commission, in the event of circumstances that may affect their impartiality, may apply to the Management Board for exclusion from the

proceedings. If the request is accepted, the Management Board shall appoint another person in place of the excluded member.

§ 6 Examination of reports

§ 7 External report

1. The Whistleblower may make an external report without first making an internal report.
2. The procedure for receiving and examining external reports shall be determined by the provisions of law and by the procedures applicable at the authority competent to receive the report.

§ 8 Public disclosure

§ 9 Register of reports

1. The Internal Reporting Coordinator shall maintain a Register of Reports in accordance with the template set out in Appendix No. 2 to the Rules. The Register may be kept in electronic or paper form.
2. The Internal Reporting Coordinator shall confirm receipt of the report within 7 days from the date of its receipt, unless the Whistleblower has not indicated a method of feedback contact.
3. The Register of Reports shall include in particular:
    - case number,
    - subject matter of the breach,
    - date of the internal report,
    - personal data of the Whistleblower, if disclosed,
    - data of the person to whom the report relates,
    - data of persons against whom the breach may have been committed, insofar as relevant to the matter,
    - information on follow-up actions taken,
    - date of case closure.
4. The Register of Reports shall be confidential. The controller of personal data contained in the Register shall be the Company.
5. Data contained in the Register of Reports shall be retained for a period of 3 years after the end of the calendar year in which the follow-up actions were completed or the proceedings initiated by such actions were concluded.

§ 10 Final provisions

1. In matters not regulated by these Rules, the provisions of the Act of 14 June 2024 on the protection of whistleblowers (Journal of Laws of 2024, item 928) and other relevant provisions of generally applicable Polish law shall apply.
2. The appendices to the Rules are:
    a. Appendix No. 1 – Form for reporting a breach of law by a whistleblower,
    b. Appendix No. 2 – Register of internal reports.
3. The Rules shall enter into force on 1 October 2024 and shall remain in force for an indefinite period.

Appendix No. 1 to the Rules for reporting breaches of law and protecting whistleblowers

INTERNAL FORM FOR REPORTING A BREACH OF LAW

Details of the reporting person (whistleblower)	full name	
	contact details (address, contact number, e-mail address)	
Details of the person concerned by the report	full name	
	position (if known to the reporting person)	
Description of irregularity (description of the breach of law)		
Additional remarks		
Signature of the reporting person		

Appendix No. 2 to the Rules for reporting breaches of law and protecting whistleblowers

REGISTER OF INTERNAL REPORTS							
No.	Report number	Date of report	Subject matter of the report (breach of law)	Personal data and contact address of the whistleblower	Personal data of the person concerned by the report	Information on follow-up actions taken	Date of case closure