

Whistleblowing Reports Management Policy

Communication:

Compliance Function

Tel. +357 22 505 105

Scope:

Commercial General Insurance Ltd (Head Office and its Branches)

Effective Date:

17/12/2023

Edition:

2.0

Approval:

Board of the Directors

Date of Approval:

29/11/2023

Categorize An Official Document:

Policy

Enforcement Level:

Binding

Table of Contents

1	INTRODUCTION - PURPOSE	4
2	SCOPE	5
2.1	Material Scope (Whistleblowing Reports material)	5
2.2	Personal Scope (Persons Covered by this Policy)	6
3	DEFINITIONS	7
4	RESPONSIBILITIES / DUTIES OF W.W.R. AND the COMMITTEE	9
5	REPORTING AND MANAGEMENT PROCEDURE	11
5.1	Reporting Procedure	11
5.2	Reporting and Management Procedure	12
6	DISSATISFACTION WITH THE OUTCOME OF THE REPORT INVESTIGATION	14
7	PROTECTION OF REPORTING PERSONS	15
7.1	Conditions for the Protection of Persons submitting Reports	15
8	RECORD KEEPING AND REPORTS	16
9	CONFIDENTIALITY OBLIGATION	17
10	PROCESSING OF PERSONAL DATA	17
11	PREVENTION AND ENCOURAGEMENT MEASURES FOR REPORTING	19
12	CONSEQUENCES OF POLICY VIOLATION	20
13	INFORMATION AND AWARENESS	20
14	MONITORING OF IMPLEMENTATION	20
15	DOCUMENT HISTORY	21
	APPENDIX A	22

1 INTRODUCTION - PURPOSE

Commercial General Insurance Ltd (hereinafter referred to as "the Company" or "the Insurer") holds a strong and reliable position among Cypriot general insurance companies and its head office is located at Arch. Makarios III Avenue, 1071 Nicosia, Cyprus.

The Company was founded in 1973 by the British insurance company Commercial Union Assurance plc, present-day Aviva plc, and the Christophides Group, which had represented said company in Cyprus since 1925.

The Company remains committed to high standards of professionalism, innovation, and excellence in the insurance industry, earning trust and esteem through solvency and credibility. Its activities are guided by ethical principles and the prevailing legislative and regulatory framework, aiming to create sustainable value while adhering to the strictest standards of professional ethics, integrity, transparency, and accountability.

For this reason, the Company demonstrates zero tolerance for actions that may disturb its healthy work environment, harm its interests, and threaten its reputation and credibility. Based on this foundation, the Company requires members of the Board of Directors, management, and employees to maintain high standards of professional and personal ethics in the performance of their duties and responsibilities. Furthermore, it encourages them to promptly and in good faith report any violations of the laws of the European Union or the Republic of Cyprus when they have a sincere and reasonable belief that there are truly serious indications that any of the violations described below in the material scope of this Policy have occurred within the Company (its main offices and branches).

This Whistleblowing Management Policy (hereinafter "the Policy") aims to establish an internal reporting system for violations of EU and Cypriot law, protecting individuals who report such violations and organizing the process of submission, receipt, and monitoring of reports.

The purpose of this Policy is:

- a. To ensure the Company's compliance with Directive (EU) 2019/1937 and Law 6 (I)/2022 of the Republic of Cyprus, incorporating the Directive, regarding the Protection of Persons who Report Breaches of EU and the National Law of the Republic of Cyprus.
- b. To provide understandable, transparent, direct, and complete information regarding the protection measures and rights of individuals reporting breaches of EU and National Law under the applicable legislative framework.
- c. To encourage persons referred within the scope of this Policy to raise, through internal reports, in good faith and as soon as possible, genuine reports of breaches of EU or national law of the Republic of Cyprus, when they have a sincere and reasonable belief that serious indications exist that any of the described under the material scope of this Policy breaches have occurred within the Company (main offices and branches).
- d. To define the principles and the relevant framework within the Company, based on which authorized persons receive, process, and investigate whistleblowing reports regarding breaches described in the scope of this Policy.

2 SCOPE

2.1 Material Scope (Whistleblowing Reports material)

This Policy applies to the protection of persons reporting or disclosing:

- a. Breaches of EU Acts, as specifically defined in Part I and II of the Annex of the Law 6(I)/2022, which you can also view [here](#), and EU Acts subsequently issued as secondary Acts in the following areas:
 - i. Public procurement,
 - ii. Financial services, products, and markets,
 - iii. Prevention of money laundering and terrorist financing,
 - iv. Financing of terrorism,
 - v. Safety and compliance of products,
 - vi. Transport safety,
 - vii. Environmental protection,
 - viii. Protection from radiation and nuclear safety,
 - ix. Food and feed safety, as well as animal health and welfare,
 - x. Public health,
 - xi. Consumer protection,
 - xii. Protection of privacy and personal data, as well as the security of network and information systems,
 - xiii. Violations affecting the financial interests of the Union under Article 325 of the Treaty on the Functioning of the European Union (TFEU), i.e., cases of fraud or any other illegal activities against the financial interests of the EU, as specifically defined in the relevant union measures,
 - xiv. Violations related to the internal market, i.e., the area of the EU in which the free movement of goods, persons, services, and capital is ensured, as referred to in paragraph 2 of Article 26 of the TFEU, including violations of EU rules on competition and state aid, as well as violations related to the internal market regarding acts that violate the rules on corporate taxation or arrangements whose purpose is to secure a tax advantage undermining the subject or purpose of the applicable corporate tax legislation.
- b. Violations of national rules of the Republic of Cyprus, mainly including, among other things:
 - i. Acts or omissions related to the commission or possible commission of a criminal offense, especially corruption offenses,
 - ii. Violation of a legal obligation imposed by the laws or regulations of the Republic,

iii. Violation that poses or may pose a risk to the safety or health of any person,

iv. Violation that causes or may cause damage to the environment.

This Policy does not apply in cases where the exceptions to the substantive scope mentioned in Article 4(3) of Law 6(l)/2022 are met, primarily for issues or contracts related to public defense or security matters, unless covered by relevant acts of the European Union.

2.2 Personal Scope (Persons Covered by this Policy)

This Policy applies to persons who report breaches that have occurred in the workplace, namely:

- Members of the Company's Board of Directors and shareholders of the Company,
- Executive Managers,
- Company employees, regardless of the type of contract that connects them to the Company (trainees/trainees, volunteers, temporary or permanent employment),
- Third-party contractors of the Company, such as suppliers, consultants, all types of collaborators, independent services suppliers, and their employees,
- Individuals associated with the Company as trainees or under an education regime (paid or unpaid),
- Individuals whose employment relationship has ended for any reason, including retirement,
- Individuals whose employment relationship has not yet begun, in cases where information about violations has been acquired during the hiring process or at another negotiation stage before the conclusion of a contract.

3 DEFINITIONS

In this Policy, the following definitions apply:

- i. **"Breaches"** means acts or omissions that are unlawful under EU or Cypriot law, DEFEAT the object or the purpose of the rules of European and national law falling within the substantive scope of this Policy.
- ii. **Committee:** The Committee which examines and follows up whistleblowing reports, the duties of which are assigned to the Company's Audit Committee, whose members are described in Appendix A of this Policy.
- iii. **"Competent Authority"** means any authority, organization, minister, deputy minister, department, council, commissioner, which under European or national law is designated to receive reports under its powers or is responsible for supervising and/or investigating reports falling within the scope of this Law, as well as any other authority, service, or organization designated as such by a decree of the Council of Ministers.
- iv. **"Direct Discrimination"** means the less favorable treatment that a person undergoes in comparison to another person in a similar situation.
- v. **"Discrimination"** means direct or indirect discrimination and includes harassment and instructions for discriminatory treatment.
- vi. **"External Report"** the oral or written communication of information on breaches to the competent authorities through external reporting channel.
- vii. **'Feedback'** means the provision to the reporting person of information on the action envisaged or taken as follow-up and on the grounds for such follow-up.
- viii. **"Follow-up"** means any action taken by the recipient of a report or any competent authority, to assess the accuracy of the allegations made in the report and, where relevant, to address the breach reported, including through actions such as an internal enquiry, an investigation, prosecution, an action for recovery of funds, or the closure of the procedure.
- ix. **"Harassment"** means unwanted behaviour by the recipient that has the purpose or effect of offending the dignity of a person, especially when it creates an intimidating, hostile, degrading, humiliating, or aggressive environment.
- x. **"Indirect Discrimination"** occurs when, in a case where, at first glance, a neutral provision, criterion, practice, act, or omission places a person in a disadvantageous position compared to other persons in a similar situation, unless this provision, criterion, practice, act, or omission can be objectively justified by a legitimate purpose, and the means for achieving that purpose are appropriate, necessary, and proportionate.
- xi. **'Information' on breaches'** means information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in the organisation in which the reporting person works or has worked or in another organisation with which the reporting person is or was in contact through his or her work, and about attempts to conceal such breaches.
- xii. **'Internal reporting'** means the oral or written communication of information on breaches within a legal entity in the private or public sector through internal reporting channel.

- xiii. **"Report"**: the identified provision of information, orally or in writing, regarding breaches as specified in point 2 of this Policy, to the Whistleblowing Reports Recipient in order to be handled by the Whistleblowing Reports Examination and Monitoring Committee of the Company.
- xiv. **"Reporting Person or Whistleblower"** means a natural person who reports or publicly discloses information on breaches acquired in the context of his or her work-related activities.
- xv. **"Retaliation"**: any direct or indirect act or omission which occurs in a work-related context, is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person.
- xvi. **" Person concerned "**: the natural or legal person named in the report or public disclosure as the person to whom the breach is attributed or with whom that person is associated.
- xvii. **"Substantial Grounds"** means the justified and good-faith belief of a reasonable person and/or a person with similar knowledge, education, and experience as the reporting person that the information they possess is true and constitutes a breach of European or Cypriot law falling within the scope of this Policy.
- xviii. **"TFEU"** means the Treaty on the Functioning of the European Union.
- xix. **'Work-related Context'** means current or past work activities in the public or private sector through which, irrespective of the nature of those activities, persons acquire information on breaches and within which those persons could suffer retaliation if they reported such information.
- xx. **W.R.R: Whistleblowing Reports Recipient** whose duties are assigned to the Head of Compliance Function of the Company.

4 RESPONSIBILITIES / DUTIES OF W.W.R. AND the COMMITTEE

The W.R.R and the Committee must:

- a. Perform their duties with integrity, objectivity, impartiality, transparency, and social responsibility.
- b. Respect and adhere to rules of confidentiality for matters they become aware of during their duties.
- c. Refrain themselves from managing specific cases, declaring any conflict of interest.

The W.R.R has the following responsibilities:

- a. Receives reports regarding breaches falling within the scope of this Policy.
- b. Communicates or immediately sends the report to the Committee and takes necessary actions in order for the Committee to handle the report.
- c. Confirm receipt of the report to the reporting person within seven (7) days from the date of receipt.
- d. Ensures the confidentiality protection of the identity of the reporting person and any third party mentioned in the report, preventing any unauthorized access.
- e. Archives the Report upon completion.
- f. Executes any other duties assigned to him by the Committee.

The Chairman of the Committee has the following responsibilities:

- a. Receives, alternatively, along with the W.R.R. reports regarding breaches falling within the scope of this Policy.
- b. Leads and gives instructions for all responsibilities of the Committee as stated below.

The Committee has the following responsibilities:

- a. Provides appropriate information regarding the possibility of submitting a report within the Company and communicates relevant information prominently within the Company.
- b. Receives reports from the W.R.R. regarding breaches, which fall within the scope of this Policy.
- c. Takes the necessary actions to examine and investigate each report.
- d. Ensures the confidentiality protection of the identity of the reporting person and any third party mentioned in the report, preventing any unauthorized access.
- e. Diligently monitors the report, maintains communication with the reporting person, and, if necessary, requests further information.
- f. Provides updates to the reporting person about the actions taken within a reasonable timeframe not exceeding three (3) months from the date of sending the acknowledgment of receipt to the reporting person.

- g. Provides clear and easily accessible information on the procedures for submitting a report to the relevant authority and, as appropriate, to public bodies or institutions or organizations of the European Union.
- h. Plans and coordinates training activities on ethics and integrity, participates in the development of internal policies to enhance the integrity and transparency of the Company.

5 REPORTING AND MANAGEMENT PROCEDURE

5.1 Reporting Procedure

The Company establishes easily accessible internal channels for reports, encouraging the submission of incidents falling within the scope of this Policy. It ensures that all received reports are handled confidentially.

Reports can be submitted either identified or anonymously. If submitted identified, the Company receives and manages them responsibly, ensuring the secured and confidential handling that protects the identity of the reporting person and any third party mentioned in the report. Anonymous reports, on the other hand, do not allow the reporting person to monitor the progress of the report.

The submission methods for reports are as follows:

- a. **Written Submission:** Identified, via email to AuditCommittee@cgi.com.cy
- b. **Written Submission:** Identified or anonymously, it is sent by postal letter to the Company's mail address at Arch. Makarios III Avenue 101, 1071 Nicosia, Cyprus, marked as "personal and confidential."
- c. **Oral Submission:** By phone at +357 22505105 or through a personal meeting with the W.R.R. or the Chairman of the Committee within a reasonable timeframe, upon the reporting person's request.

In case submission over the phone where the conversation is not recorded, the Company documents the oral reporting in the form of accurate minutes of the conversation written by W.R.R. and offers the reporting person the opportunity to check, rectify and agree with the content of the minutes of the conversation by signing them.

When a person requests a meeting with the W.R.R. or the Chairman of the Committee to submit a report, complete and accurate records of the meeting are kept in a durable and retrievable form, prepared by the W.R.R. and, are subject to the consent and signing of the reporting person.

If there is a refusal of the reporting person to sign the minutes as described above, a relevant reference is made by the W.R.R. in the minutes.

Reports must adhere to the principle of good faith on the part of the reporting person, who is obliged to exercise due diligence throughout the process of submitting the report and providing relevant information. According to Law 6(I)/2022, article 39(2), individuals knowingly making false reports or false public disclosures may be subject to prosecution with imprisonment for up to 3 years and/or a fine of up to €30,000.

In order for the reports to be investigated and properly assessed, they need to be clear, specific, and include all available information, such as the events that raised suspicion/concern/belief in the breach, referring names, dates, documents, and locations.

If the reporting person, after submitting the report, realizes that it was groundless/unfounded, they must inform the Company through the aforementioned methods.

5.2 Reporting and Management Procedure

Once any report is submitted, the following reporting and investigation procedure will be followed:

The W.R.R.:

- a. Confirms the receipt of the report to the reporting person immediately and, in any case, within seven (7) working days from the date of receipt.
- b. Concurrently informs the Committee about the report and manages the report in due care, impartiality, and confidentiality. The Committee is consisted of the Head of the Company's Internal Audit Function, two members of the Board of Directors and the Secretary of the Committee.

The Committee initially investigates whether the report falls within the scope of this Policy. After the initial check, the Committee. proceeds with further investigation of the report. If necessary, additional information is requested from the reporting person through the W.R.R. or an authorized member of the Committee.

In case the report is directed against a member of the Committee or if any member finds itself in a conflict of interest, that member is removed from the list of recipients for that specific report. They do not participate in the investigation of the report and are ad hoc replaced by a person appointed by the Company's Board of Directors.

The Committee. investigates the report, conducts checks, evaluates the accuracy of the claims contained therein, decides on the validity of the report under investigation, records the investigation results, and, depending on these results, proposes:

- a. Appropriate measures to address the reported breach, such as additional employee training, establishment of new internal control mechanisms, modifications to existing procedures, or legal actions (prosecution, recovery actions),
- b. Further investigation of the report, or
- c. Completion of the process and archiving the report or referral to the Company's Board of Directors for them to make the necessary decisions.

In case the report is directed against a member of the Board of Directors or if they find themselves in a conflict of interest, the decision of the Committee is forwarded to the Company's Chief Executive Officer for him to make the necessary decision.

The decisions of the Committee is justified and taken by a majority vote.

The Committee provides feedback to the reporting person about the actions taken within a reasonable timeframe, not exceeding three (3) months from the acknowledgment of receipt. or, if no acknowledgement was sent to the reporting person, three months from the expiry of the seven-day period after the report was made.

In case the report is rejected by the Committee, the process is completed. The Committee forwards the report file for archiving to the W.R.R., who notifies the reporting person in writing of the decision, including the reasons for rejection.

Reasons for rejection may include cases where:

- The actions of the person concerned do not fall within the scope of this Policy.

- The report is incomprehensible or is submitted abusively or does not contain incidents that substantiate a breach of EU or national law or do not present serious indications of such a breach.
- The report is found not to have been made in good faith.

6 DISSATISFACTION WITH THE OUTCOME OF THE REPORT INVESTIGATION

If the reporting person feels that his/her/their internal report was not effectively addressed, they may resubmit it to the Authority in charge of handling the relevant breach through an external report.

The list of Authorities is posted on the website of the Ministry of Justice of the Republic of Cyprus <https://www.mjpo.gov.cy/> and also it can be viewed [here](#). Instructions regarding the process of submitting a report to the relevant Authorities are posted also on the above website of the Ministry of Justice of the Republic of Cyprus and can be also viewed [here](#).

The breaches of Articles 101, 102, and 325 of the Treaty on the Functioning of the European Union (which concern the economic interests of the Union, related to the internal market, and rules of EU Competition Law), are handled by the National Coordinating Authority for Combating Fraud and Corruption against the Financial Interests of the European Union. The external reporting channel to which the reporting person can address, depending on the breach, is as follows:

- Superintendent of Insurance
- Law Office of the Republic of Cyprus (MO.K.A.S.)
- Treasury of the Republic of Cyprus
- Audit Office of the Republic of Cyprus
- The Department of Customs of the Ministry of Finance.
- Police
- Directorate General Growth (Ministry of Finance)
- Cyprus Agricultural Payments Organization
- Internal Audit Service
- Commission for the Protection of Competition (C.P.C.)
- Office of the Commissioner for State Aid Control
- Tax Department (Ministry of Finance)

Instructions regarding the procedure for reporting to the above Authorities, as well as the list of Authorities corresponding to the breaches received, are posted on the website of the Ministry of Justice, and the reporting person can view them [here](#) and [here](#), respectively.

7 PROTECTION OF REPORTING PERSONS

The Company protects those reporting breaches falling within the scope of this Policy and ensures the absence of retaliation.

In this context, any form of negative behavior/reprisals against anyone who has made a report is prohibited, including threats and retaliatory actions.

Especially prohibited forms of reprisals include:

- a. Suspension, lay-off, dismissal or equivalent measures.
- b. Demotion or withholding of promotion.
- c. Transfer of duties, change of location of place of work, reduction in wages, change in working hours.
- d. Withholding of training.
- e. A negative performance assessment or employment reference.
- f. Imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty.
- g. Coercion, intimidation, harassment, or ostracism.
- h. Discrimination, disadvantageous or unfair treatment.
- i. Failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment.
- j. Failure to renew, or early termination of, a temporary employment contract.
- k. Harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income.
- l. Blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry.
- m. Early termination or cancellation of a contract for goods or services.
- n. Cancellation of a license or permit.
- o. Psychiatric or medical referrals.

Any act of retaliation should be reported directly to the W.R.R.E.M.C.

7.1 Conditions for the Protection of Persons submitting Reports

- a. Whistleblowers reporting breaches falling within the scope of this Policy, acting in "good faith" at the time of the report, are protected, provided that they had reasonable grounds to believe that the information about the reported breach was true and falls within the scope of this Policy.

- b. Persons who anonymously reported and were subsequently identified and faced retaliations are protected, provided that they meet the requirements mentioned in the above paragraph 7 of this Policy.
- c. Similarly, third parties connected to the whistleblowers who may suffer retaliations in an employment context, such as colleagues or relatives of the whistleblowers, as well as personal enterprises or legal entities of interest to the whistleblowers, or with whom they are in any way connected in an employment relationship, are protected on a case-by-case basis.
- d. Reports submitted are communicated through the persons described in this Policy, who are considered necessary for conducting an investigation and are obliged to observe the rules of confidentiality. Compliance with the above also results in the protection of the identity of the reporting person.

8 RECORD KEEPING AND REPORTS

The Company maintains a file for each report received, in accordance with the confidentiality requirements of this Policy. Reports are stored confidentially, following the necessary security specifications of the Company, for a reasonable and necessary period described below, to be retrievable and to comply with the requirements imposed by this Policy, EU or national law, and in any case until the completion of any investigation or legal proceedings initiated as a result of the report against the person concerned, the reporting person, or third parties.

9 CONFIDENTIALITY OBLIGATION

1. Personal data and any information leading directly or indirectly to the identification of the reporting person, are not disclosed to anyone other than authorized personnel responsible for receiving or handling the reports, unless the reporting person consents. For this purpose, the Company takes appropriate technical and organizational measures to protect and secure the information during the monitoring of the report.
2. The identity of the reporting person and any other information may exceptionally be disclosed when required by the any Law of the Republic of Cyprus, in the context of administrative, civil, and/or criminal investigations by any competent public authority, or in the context of judicial proceedings, provided that it is necessary to serve the purposes of the EU or national law of the Republic of Cyprus or to ensure the defensive rights of the person concerned.
3. Disclosures under paragraph 2 of above are made after providing the reporting person with written information about the reasons for disclosing their identity and other confidential information unless such information undermines investigations or judicial proceedings. After being informed, the reporting person is entitled to submit written comments to the Company, which are not disclosed to anyone. Exceptionally, if the reasons presented in the comments are considered insufficient, the disclosure of the identity and other confidential information of the reporting person is not prevented. No further safeguards are provided for the identity of the reporting person and the information from which it can be implied, as provided by special provisions of EU or national law of the Republic of Cyprus.

The above provisions regarding the protection of the identity of reporting persons also apply to the protection of the identity of person concerned.

10 PROCESSING OF PERSONAL DATA

Any processing of personal data under this Policy is carried out in accordance with the Company's Privacy Policy, which is posted to its website <https://cgi.com.cy> or the following link [Privacy Policy](#) the General Data Protection Regulation (EU Regulation 2016/679 – GDPR, the Law 125(I)/2018, and its relevant amendments, with reservations of the specific provisions of Law 44(I)/2019 and its amendments, which provide special provisions regarding the processing of personal data by competent authorities for the purposes of prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal sanctions.

Any processing of personal data taking place under this Policy, is carried out in purpose of complying to the obligation of establishing internal reporting channels and taking necessary measures for their monitoring. In the context of the above processing of personal data, any information related to breaches in the context of reports is included. Transfer of information received in reports to competent supervisory and investigative authorities is permitted, and it can be used as evidence in administrative, civil, and criminal investigations and proceedings.

As the Data Controller, the Company takes appropriate technical and organizational measures to ensure that, during the submission and monitoring of reports, only the necessary and relevant personal data for the purposes of this Policy are collected. Personal data that is obviously unrelated to the handling of a specific report or is excessive is not collected, or if collected accidentally, is promptly deleted.

10.1. Retention Period of Personal Data contained in reports.

Personal data collected in the context of reports receipt are deleted within three (3) months from the date of completion of the procedure provided for in this Policy. In case that judicial or disciplinary proceedings have started against the person concerned or the reporting person, personal data shall be retained for the duration of such proceedings, including in the occasion of an appeal or objection and they shall be deleted one (1) year after the completion of the above procedures.

10.2. Exclusions from the Scope of the GDPR

Pursuant to Article 14 par. 5 and 23 of the GDPR, which provide for a derogation from the provisions of the GDPR for special cases of compliance with a legal obligation, the Company must derogate from its obligations provided for in Articles 5 par. 1 (a), 12 – 22 and 34 par. 1 of the GDPR in relation to certain categories of personal data subjects. Therefore, the Company is obliged to deviate from the General Principle of Transparency provided for in Article 5 par. 1 (a) GDPR. On this basis, the Company, due to its legal obligation for confidentiality during the receipt, monitoring, handling and retention of reports, may not provide relevant information on the processing of personal data to the person concerned and to any third party in his capacity as a subject of the data named in the report or the personal data processed in the context of monitoring measures and especially the source of the data referred in the report, as provided in par. 2 of Article 14 of the GDPR. The derogation from the above obligation shall apply for as long as necessary and if necessary for the purpose of preventing and facing attempts to obstruct reporting, block, frustrate or delay follow-up measures, in particular with regard to investigations, or attempts to identify reporting persons, as well as to protect them against retaliation. In addition, the Company may not satisfy the rights provided by Articles 15 to 22 of the GDPR, when they are exercised by data subjects and third parties named in the report or resulted from monitoring measures.

In cases where the rights of data subjects are restricted, as provided above, the Company, as controller, shall take all necessary technical and organisational measures to protect the rights and freedoms of data subjects or other individuals. When the controller refuses to satisfy the rights, without informing about the reason for the restriction, the data subject is entitled to lodge a complaint with the Commissioner for Personal Data Protection, who may investigate the fulfilment of the conditions for the restriction of rights and inform the subject accordingly, provided that such information is not harmful for the fulfilment of these purposes.

In case of personal data breach, the Company does not make a communication to the data subject as provided for in Article 34 par. 1 of the GDPR obligation, if the announcement of such data breach may be harmful for the purposes of this Policy. The Company informs the Commissioner for Personal Data Protection, who may request the Company to communicate the breach to the data subject, if it finds that the conditions for exemption from notification are not met.

11 PREVENTION AND ENCOURAGEMENT MEASURES FOR REPORTING

This Policy serves as a means to ensure the integrity, internal governance, and reputation of the Company. It contributes to recognizing risks and taking appropriate corrective measures, including strengthening the Internal Control and Regulatory Compliance System, identifying incidents of fraud or other serious violations in advance, applying appropriate measures against those responsible and, when necessary, informing the relevant authorities, as appropriate.

By providing a trusted and secure environment for employees, customers, and suppliers, the Company encourages the submission of reports "in good faith" regarding illegal acts or serious offenses that fall within their perception.

The Company is open to all, and it suggests that all its employees share their questions, concerns, and suggestions with the Department or Branch Manager under which are supervised.

However, if an individual does not feel comfortable addressing the above individuals or is dissatisfied with their response, the Company encourages them to express their concerns to the Head of Compliance or a member of Management or the Internal Auditor, or the Chairman or the members of the Audit Committee. In addition, Directors of Departments, Branches and members of the Management are obliged to report any concerns, suggestions, or questions they receive from their subordinates to the Head of Compliance of the Company, who is obliged to forward them to the Company's Audit Committee.

Furthermore, the Head of Compliance Function and the Head of the Internal Audit Function of the Company, for the purpose of prevention and ensuring awareness, due care and attention, are obliged to audit the implementation of internal control procedures, Company's Policies, and compliance with the EU and current legislative and regulatory framework. They inform the Audit Committee and/or the Chief Executive Officer and/or the Board of Directors of any relevant breach or suggestions for improvement, with the aim of creating sustainable value committed to the highest standards of professional ethics, integrity, transparency and accountability.

Additionally, the Company requires from the members of the Board of Directors, members of Management and its employees to maintain high standards of professional and personal ethics while performing their duties and responsibilities.

12 CONSEQUENCES OF POLICY VIOLATION

The Company reserves the right to take any appropriate measures against any employee, contractor, or any other collaborator if it is discovered or determined in any way that:

- a. They obstructed or attempted of submission of a report in cases falling within the scope of this Policy.
- b. They subjected any person who submitted a report based on this Policy to any form of adverse treatment.
- c. They retaliated or initiated malicious proceedings against a person who submitted a report based on this Policy.
- d. They violated the obligation to maintain the confidentiality of the identity of the reporting person.

The same procedure may also be applied in cases where an employee, contractor, or any collaborator deliberately misinformed the Company on any matter under investigation within the framework of this Policy or made false claims against a colleague, contractor, or collaborator of the Company.

13 INFORMATION AND AWARENESS

In order to enhance integrity and transparency within the Company, its employees receive appropriate information and training on ethics and integrity, as well as reporting breaches, ensuring that they are fully aware of their rights and obligations under this Policy, as well as the Company's procedures for reporting and investigating.

The Company will ensure that this Policy and any revisions thereof are communicated to all relevant individuals, and its content will be included in the Employee Handbook.

Information about the Policy is electronically published in a prominent and accessible location for the administrative staff of the Company, as well as on the Company's website <https://cgi.com.cy>.

14 MONITORING OF IMPLEMENTATION

The Head of Compliance is responsible for the distribution/publication of the Policy, as well as for monitoring compliance with its requirements.

15 DOCUMENT HISTORY

Edition	Date	Editor	Amendments
0.1	18/8/2019	Head of Compliance	Approval of a Whistleblowing Policy by the Board of Directors on the basis of the adoption of best practices
0.2	17/12/2023	Head of Compliance	Updating of existing Whistleblowing Policy, on the basis of compliance with Law 6 (I)/2022 of the Cyprus D

APPENDIX A

Members of the Committee for the Examination and Follow-up of Whistleblowing Reports (Audit Committee)

The Committee is consisted of the following:

Nicos Syrimis, Chairman

George M. Kourris, Member

Dr. Christodoulos Patsalides, Member

Stella Anastasi
Head of Compliance Function, Secretary of the Committee

Contact details:

Email: AuditCommittee@cgi.com.cy

Telephone: 22505105

Address: 101 Arch. Makarios III Avenue, 1071, Nicosia
P.O.Box 21312, 1506