Grant Thornton
An instinct for growth™

External Whistleblowing Policy

March 2021

1. Introduction – what is whistleblowing, and why is it important?

Grant Thornton Greece[1] strives to achieve transparency and a high level of business ethics. Our whistleblowing scheme offers a possibility to alert the company about suspicions of misconduct in confidence. It is an important tool for reducing risks, detecting and preventing malpractices, discouraging unethical behaviour and maintaining trust in our operations by enabling us to act on possible misconduct at an early stage.

In addition, our whistleblowing scheme exposes weak or flawed processes or procedures which make Grant Thornton Greece vulnerable to loss, criticism or legal action, avoids inefficiency, reduces the risk to the environment and finally yet importantly, deters individuals from engaging in improper conduct. Whistleblowing can be done openly or anonymously.

The purpose of this Whistleblowing Policy ("the Policy") is to clarify the scope and operation of the whistleblowing scheme and the investigation process to external stakeholders. The Head of Risk Management Committee is responsible for the proper implementation of this Policy. Furthermore, the Policy intends to encourage you to feel confident in raising serious concerns at the earliest opportunity, to ensure that you will receive a response to your concerns and that you are aware of how to pursue them if you are not satisfied.

2. When to blow the whistle?

The whistleblowing scheme can be used to alert us about serious risks affecting individuals, our company, the society or the environment.

Whistleblowing can be used to report suspicions for serious irregularities or malpractices relating to any of the following:

- Infringements of laws and regulations on accounting, auditing matters, banking and financial crime or anti-bribery laws, such as misappropriation of company's or clients' assets,
- Serious improprieties concerning our company's or network's vital interests or the life or health of individuals including risks to the public, as for instance serious environmental crimes or non-compliance with health and safety rules,
- Serious forms of discrimination or harassment, such as verbal or physical disrespect of a person because of his/her origin, religion, sexual orientation, special condition or otherwise,
- Infringement of our Code of Conduct, or the laws and regulations that are applicable to our company or the profession of our staff,
- Acts that may constitute fraud and/or corruption,
- Violations of the applicable anti-money laundering legislation, such as non-compliance with customer due diligence measures or with reporting obligations

[1] "Grant Thornton Greece", "our company", "we", "us" and "our" refers to "Grant Thornton Chartered Accountants and Management Consultants Societe Anonyme" and "Grant Thornton Tax and Business Advisory Solutions Societe Anonyme".

This is not an exhaustive list but is intended to indicatively illustrate the sort of issues that may be raised under this Policy.

A person who blows the whistle does not need to have a high level of certainty or evidence; expressing an honest suspicion will be sufficient. Our company commits to protect the external stakeholders who submitted a report in good faith without abusing the whistleblowing scheme against retaliation acts. However, deliberate reporting of false or malicious information is forbidden. Abuse of the whistleblowing scheme may result in action against the perpetrator of the abuse.

In any case, the whistleblower is encouraged to share any information known to him/her (such as adequate details on the event and the person(s) involved or present and documentation that could effectively verify the validity of the event reported) in order to facilitate the investigation.

You can blow the whistle by submitting a message here

3. Named or anonymous report?

We encourage anybody who wishes to share his/her suspicions to be open with his/her identity and we guarantee that all messages received will be handled confidentially. More specifically, our company commits to maintain your identity confidential throughout the whole process, unless its disclosure is deemed required for the proper investigation of the case (e.g. within the context of any judicial or legal proceedings).

If you do not wish to submit a message in an identified manner, we offer the option of reporting your concern anonymously and we secure your anonymity throughout the whole process. Particularly, the communication channel, which allows anonymous messaging, is administrated by WhistleB, an external service provider, which abides by adequate technical and organisational measures to ensure anonymity and data security, as described in the relevant section below.

4. The investigation process

A. The whistleblowing team

Access to messages received through the communication channel is restricted to appointed individuals of our company with the authority to handle whistleblowing cases. The whistleblowing team consists of three members of our company, acting in full confidentiality and integrity. Members of said team have entered into a Confidentiality Agreement particularly with respect to the information they receive as members of the whistleblowing team. Their actions are logged and handling is confidential. When needed, individuals who can add expertise, such as external lawyers, may be included in the investigation process, subject to their written commitment to confidentiality. In addition, when needed for investigation purposes, the case may be escalated or delegated and specific persons within our company may be informed or involved in the process.

In order to secure objectivity and integrity, in case the person named in the whistleblowing report coincides with one of the whistleblowing team members, this conflict is immediately flagged and the person named in the report is removed from the recipient list (whistleblowing team) for the specific report and is not involved in the investigation of the case.

B. Receiving a message

Upon receiving a message, the whistleblowing team decides whether to accept or decline the message.

The whistleblowing team may decline a message if one or more of the following applies:

- the alleged conduct is not a reportable conduct under the Policy,
- the message has not been made in good faith or is malicious,
- there is insufficient information to allow for further investigation,
- the subject of the message has already been solved

If a message includes issues not covered by the scope of the Policy, the whistleblowing team will take appropriate actions to get the issue solved, e.g. assign the case to the adequate person or team. Cases relating to whistleblowing messages found to be unsubstantiated or in bad faith will be concluded without further acts. In any case, the whistleblowing team will send a message to the whistleblower to inform him/her about the decline and the reason for it.

If the message is accepted, appropriate measures for investigation, as described below, will be taken.

C. Investigation

All messages are treated seriously and in accordance with the Policy.

- The investigation of the case is initiated as soon as possible, normally within ten days from the receipt of the message, with objectivity, integrity and taking into account the interests of all parties involved.
- No one from the whistleblowing team, or anyone taking part in the investigation process, will attempt to identify the whistleblower.
- The whistleblowing team can, when needed, submit follow-up questions via the channel for anonymous communication.
- A message will not be investigated by anyone who may be involved with or connected to the malpractice.
- The whistleblowing team decides if and how a whistleblowing message should be escalated.
- Whistleblowing messages are handled confidentially by the whistleblowing team and/or any parties involved.

After having submitted the message via the communication channel, the whistleblower will receive an ID and a password on the screen. Said credentials should be saved in a secure manner and used in order for the whistleblower to log into the communication channel, read the response or follow-up question posted by the whistleblowing team and reply to it.

Solely the whistleblowing team members will have access to the whistleblowing reports that have been submitted. In order to access the channel, each whistleblowing team member uses both a personal and a secondary password. The secondary password is encrypted, in order to secure that the messages will not be read by any third party (including WhistleB and any person within or outside our company apart from the whistleblowing team members), unless access is deemed necessary and is authorized by the whistleblowing team.

This procedure secures that the anonymous whistleblower will not be identified, unless he/she decides to reveal his/ her identity. Thus, he/she remains anonymous during the whole process, i.e. at the time of submission of the report and throughout the anonymous dialogue with the whistleblowing team.

D. Whistleblower's protection in the case of non-anonymous whistleblowing

A person expressing genuine suspicion or misgiving according to the Policy is protected against any retaliation. It does not matter if the whistleblower is mistaken, provided that he or she is acting in good faith.

The identity of the whistleblower who reports serious wrongdoings or irregularities is treated with the utmost confidentiality and is not revealed except in certain exceptional circumstances, such as if the whistleblower authorizes such a disclosure, or if the whistleblower acts in bad faith and maliciously makes a false or unsubstantiated statement, or if this is required by any subsequent legal proceedings. More specifically, in cases of alleged civil or criminal offences, the whistleblower will be informed that his/her identity may need to be disclosed to judicial authorities during judicial proceedings.

Subject to considerations of the privacy of those against whom allegations have been made or any other persons mentioned in the report, and any other issues of confidentiality, a non-anonymous whistleblower will be kept informed of the outcome of the investigation.

5. Protection of Personal Data

Throughout the whistleblowing process, the whistleblowing team is expected to receive Personal Data, either from the whistleblowing report or the follow-up communications with the whistleblower. "Personal Data" means any information relating to an identified or identifiable natural person ("Data Subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

You are highly encouraged not to include in your report special categories of Personal Data about you or the person against whom you make an allegation, unless inclusion is absolutely necessary in order to substantiate your report. Special categories of Personal Data are Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic Personal Data, biometric Personal Data for the purpose of uniquely identifying a natural person, Personal Data concerning health or Personal Data concerning a natural person's sex life or sexual orientation.

This will help to avoid the collection of excessive and unnecessary Personal Data. In any case, any unnecessary or excessive Personal Data will not be taken into account and will not be processed by the whistleblowing team.

The processing of Personal Data will be in compliance with no. 679/2016 European General Data Protection Regulation ("GDPR"), Law 4624/2019, as in force or as may be replaced and any other applicable Greek and European legislation for the protection of Personal Data ("Applicable Legislation"). The data controller within the meaning of GDPR is Grant Thornton Greece (Grant Thornton Greek legal entities), however the processing is performed solely by the whistleblowing team and/or any other person deemed necessary in accordance with the Policy.

A. Purpose and legal basis of the processing

The Personal Data of the Data Subject (e.g. the person against whom a whistleblowing report has been submitted) will be processed exclusively for the purposes of the whistleblowing scheme, i.e. for proper handling and further investigation of the whistleblowing reports.

The legal basis of the processing is (a) the compliance with the legal obligation arising out of Law 4557/2018 on the prevention and suppression of money laundering and terrorist financing, as amended and in force, and relating to the operation of a whistleblowing scheme and (b) the legitimate interest of Grant Thornton Greece relating to the prevention of and fight against any malpractices or irregularities in the performance of its business activities.

B. Data subjects' rights and potential restrictions

The Data Subjects will be entitled to all rights provided in the Applicable Legislation:

i. right to access Personal Data relating to themselves,

ii. right to ask for amendment of incorrect, inaccurate or incomplete Personal Data relating to themselves,

iii. right to request erasure of their Personal Data, in cases provided by the Applicable Legislation (right to be forgotten),

iv. right to ask for restriction of their Personal Data, in cases provided by the Applicable Legislation,

v. right to object to the processing of their Personal Data, in cases provided by the Applicable Legislation,

vi. right to lodge a complaint with the Greek Data Protection Authority at the following contact details:

Address: Kifissias avenue, no. 1-3,
115 23 Athens, Greece
Telephone: +30-210 6475600
Fax: +30-210 6475628
E-mail: complaints@dpa.gr

However, the exercise and/or the level of satisfaction of these rights may be subject to limitations in case of any overriding safeguarding measures required to secure the retention of evidence and the smooth investigation of the case, as well as to ensure the protection of the rights and freedoms of others involved in the whistleblowing scheme. These restrictions are applied on a case-by-case basis. For example, under no circumstances can the person accused in a whistleblower's report obtain information about the identity of the non-anonymous whistleblower on the basis of the former's right of access, except in certain exceptional circumstances, such as where the whistleblower maliciously makes a false statement.

C. Potential recipients of personal data within EEA

The Personal Data and generally the information received by the whistleblowing team will not be transferred to other persons or teams of our company, except to the extent that said transfer is considered as absolutely necessary for the purposes of further investigation of the report and solely to the required persons on a need-to-know basis.

In addition, said information and Personal Data may be transferred to the competent public authorities in case there is a legal obligation or in case of initiation of judicial or other legal proceedings within the context of the investigation of the whistleblowing case.

In case that further support for the investigation of a case is required, WhistleB or other external providers – experts within the European Economic Area ("EEA") may be involved in the process and receive Personal Data, pursuant to a data processing agreement between them and Grant Thornton Greece, in accordance with Article 28 of GDPR.

D. Transfer of personal data within our network

All Personal Data is stored within the EU. There is a general prohibition on the transfer of Personal Data outside EEA, unless specific mechanisms are used to protect the Personal Data.

The Personal Data received through the whistleblowing system may be communicated within Grant Thornton network if such communication is necessary for the investigation, depending on the nature or the seriousness of the reported misconduct. Such communication will be considered as necessary to the requirements of the investigation if for instance the report incriminates a partner of another legal entity within the group, a high level member or a management official of the company concerned. Generally, in case of an allegation against a person from another Grant Thornton member-firm, the investigation might include communication between the network, e.g. between our People and Culture team and the People and Culture team of the relevant Grant Thornton member-firm.

In this case, the information exchanged will remain confidential and will be communicated on a need-to-know basis. In any case, all Grant Thornton member-firms abide by a Cross Border Confidentiality Agreement entered into between Grant Thornton International and Grant Thornton member-firms.

In case Personal Data are transferred to a Grant Thornton member-firm outside EEA, our company ensures that said transfer will be in compliance with GDPR. In any case, all Grant Thornton member-firms abide by Inter-Firm Agreements on Personal Data protection, which include standard contractual clauses, in accordance with term 46 of GDPR.

E. Technical and organizational measures

The whistleblowing scheme is provided by an independent external partner WhistleB, Whistleblowing Centre, which abides by adequate technical and organisational measures, pursuant to Article 32 of GDPR, in order to ensure anonymity and secure Personal Data against loss, destruction, unauthorised access or any form of unlawful processing.

The anonymity of the whistleblower is guaranteed as there is no tracking of his/her IP address or other meta-data. In addition, given that the messages sent via the communication channel are encrypted and access to this channel is password-protected, the whistleblower remains anonymous in the subsequent dialogue with the whistleblowing team and the Personal Data is kept secure.

The communication channel is delivered through Microsoft Azure data centres, each designed to run 24/7/365, and each employing various measures to protect operations from power failure, physical intrusion, and network outages. They are also subject to threat management and mitigation practices, including regular penetration testing. Database and blob storage (used for logs, backups and report attachments) are replicated with failover nodes. The availability, performance and security of the whistleblowing scheme is monitored 24/7/365.

F. Deletion of personal data

Personal Data included in a whistleblowing message and investigation documentation is deleted within thirty (30) days following completion of the investigation and conclusion of the case, with the exception of when Personal Data must be maintained according to any applicable laws.

In case of initiation of any legal proceedings (against the incriminated person or the whistleblower in cases of maliciously false declaration), Personal Data will be kept until the conclusion of these proceedings, including any subsequent appeals.

Investigation documentation and whistleblowing messages that are archived will be anonymised.

6. Amendments to the Policy

The Policy may be supplemented by additional notices or guidance.

In addition, we may modify the Policy periodically to reflect amendments in the whistleblowing scheme. In such cases, you will be able to check the most updated version of the Policy, as posted on our Website.

7. Contact us

If you have any question or concern with respect to section 5 of the Policy and in general the processing or protection of your Personal Data or in case you need more information about your rights and how to exercise them, please contact the dedicated privacy team of our company at the following e-mail address: privacy@gr.gt.com or at the following postal address: 56, Zefirou str., 17564, Paleo Faliro, Athens.

In case you need any clarification with respect to the whistleblowing process, the types of misconduct that may be reported under the whistleblowing scheme or any further request, you may contact the whistleblowing team at the following dedicated e-mail address: whistleblowing@gr.gt.com