GUIDELINES ON WHISTLEBLOWER PROTECTION FOR COMPANIES IN GREECE

OECD
Guidelines on Whistleblower Protection for Companies in Greece
This document is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

About the OECD

The OECD is an international organisation in which governments compare and exchange policy experiences, identify good practices in light of emerging challenges, and promote decisions and recommendation to produce better policies for better lives. The OECD’s mission is to promote policies that improve economic and social well-being of people around the world.

www.oecd.org

About the Greece-OECD Project

The Greek government with the assistance of the European institutions is prioritising the fight against corruption and bribery and is committed to taking immediate action. Greece’s National Anti-Corruption Action Plan (NACAP) identifies key areas of reform and provides for a detailed action plan towards strengthening integrity, transparency and fighting corruption. The OECD, together with Greece and the European Commission, has developed support activities for implementing the NACAP. This project is scheduled for completion in January 2018 and is funded by the European Union and Greece.

www.oecd.org/corruption/greece-oecd-anti-corruption.htm
Table of Contents

Introduction......................................................................................................................... 5

I. Defining your company’s framework for protected internal reporting ........ 8
   1. Who can make a report.............................................................................................. 8
   2. What can be reported? ............................................................................................. 9
      2.1 Wrongdoing ........................................................................................................ 9
      2.2 Reasonable belief ............................................................................................ 10
   3. Setting up the reporting mechanism................................................................. 10
      3.1 Internal channels ............................................................................................ 11
      3.2 External channels ............................................................................................ 13
      3.3 Form of the report ........................................................................................... 14
      3.4 Confidentiality ................................................................................................. 14
   4. What is retaliation? ............................................................................................... 16
   5. Protection against retaliation........................................................................... 17
      5.1 Who and when to protect ............................................................................... 17
      5.2 How to protect ............................................................................................... 18
   6. What are the consequences for retaliation?...................................................... 19

II. Implementing your company’s protected internal reporting mechanism...... 20
   1. Leadership and commitment ............................................................................. 20
   2. Acting on reporting and disclosure .................................................................... 21
      2.1 Confirm the reception of the report ............................................................... 21
      2.2 Decide whether to investigate the report ....................................................... 21
      2.3 Carrying out the investigation ...................................................................... 22
      2.4 Provide follow-up to the reporting person .................................................... 23
   3. Maintain confidential, adequate and auditable documentation
      of all reports received .............................................................................................. 23
   4. Provide regular training on the whistleblowing policy ..................................... 24
   5. Communicating about your policy - Fostering a “speak-up culture” .......... 25
   6. Incentivising and rewarding whistleblowing .................................................... 27
   7. Monitoring, oversight, review and evaluation of the policy ........................... 28
Introduction

Legal or ethical misconduct can often lead to irreversible damaging consequences to a company’s business and reputation. Fraud, abuse, environmental or human rights violations can expose a private sector organisation to a vast array of liabilities, damaging its brand and leading to a loss of profits and talent. Timely detection allows for opportunities to adequately address the misconduct with remedial responses.

Internal reporting mechanisms that encourage company employees or third-party business partners to report any witnessed unethical or legal violation internally, are an effective way for a company’s leadership to take preventative or corrective action for acts that if left undetected, could be disastrous for the company. A company’s whistleblowing policies should consist of safe reporting channels as well as processes that protect those voicing their concerns from retaliation and can monitor management’s responses to ensure that concerns are efficiently and appropriately addressed.

In addition to providing the capacity to uncover misconduct that could be taking place unknown to higher management within an organisation, whistleblowing policies and mechanisms can gather information about corruption risks and patterns that can inform the organisation’s overarching anti-corruption and compliance policies. They can reveal areas that demand immediate attention, improvement or even the need for the creation of new policies that can aid in reducing the risks the company is exposed to. Finally, they can inform the refined training of staff and third party business partners based on detected patterns discovered through reports.

Whistleblower protection is vital to create a workplace guided by principles of transparency, accountability and integrity and it serves as a definitive safeguard of the public interest. For this reason,
national legislative bodies are increasingly enacting whistleblower protection legislation that requires the implementation of internal reporting mechanisms by companies. 43% of company respondents to the Survey on the Private Sector conducted by the OECD (12/2016-2/2017) stated that they did not provide internal reporting mechanisms. Furthermore, only 45% of Greek companies claimed to provide protection to employees reporting instances of non-compliance with laws on corruption, whereas 52% of companies had not provided such protection over the past two years.

The purpose of this report is to assist Greek companies achieve the goal of implementing effective internal reporting mechanisms. Greece’s National Anti-Corruption Action Plan (NACAP) sets out key areas of reform and defines priorities in enhancing integrity, transparency and the fight against corruption. The OECD has committed to supporting the Greek authorities and to provide the necessary expertise to implement the reform agenda in a series of pre-identified areas. This document will be complemented by two additional outputs, namely the best-practices paper and guidelines on promoting compliance, effective internal controls and ethics in Greek companies to tackle bribery (March 2017) and guidance to Greek companies on analysing corruption risks that they face (May 2017).

These guidelines were prepared by taking into consideration international experience in other OECD countries in order to adapt them to the Greek context. They benefit from the input of Business and Industry Advisory Committee to the OECD (BIAC), Tom Devine (Government Accountability Project), Jane Ellis (International Bar Association), staff at the Securities and Exchange Commission, United States, David Lewis (Middlesex University London), Fereniki Panagopoulou-Koutnatzi (Hellenic Data Protection Authority), Constanze von Söhnen (UN Office on Drugs and Crime), Ursula Stapleton (Department of Justice and Equality, Ireland) and Marie Terracol (Transparency International). The Guidelines aim to be flexible and able to be applied by companies of various sizes and sectors. In the absence of specific whistleblower protection
legislation in Greece, these Guidelines reflect current international standards and good practices in whistleblower protection and should also be relevant and adaptable for companies operating in numerous jurisdictions.

The standards reflected in these Guidelines should enable companies to have a protected internal reporting framework that meets the highest international standards for whistleblower protection, whilst also complying with current Greek legislation. These Guidelines do not, however, constitute legal advice. Any company designing and implementing a protected internal reporting framework should seek independent legal advice to ensure that it complies with relevant legislation.

Further information about the Greek private sector was obtained through a Survey of Greek Stakeholders conducted by the OECD from December 2016 to February 2017 (companies, government stakeholders, civil society organisations, business organisations, and professional associations). The Stakeholder Survey was conducted to identify corruption risks facing the private sector, and existing incentives and mechanisms to address corruption risks. As of 2 February 2016, 516 stakeholders had replied to the Stakeholder Survey. This was followed by Consultation Meetings in Athens and Thessaloniki in February 2017 with all relevant stakeholders to further discuss the Stakeholder Survey’s findings and collect additional qualitative information about the Greek business environment.

1 These Guidelines consider that the framework for “public interest witnesses” of Law 4254/2014 and Article 45B of the Greek Code of Criminal Procedure do not amount to whistleblower protection provisions. Therefore, any reference to the notion of “whistleblower” should not be associated or understood with the said legal provisions.

2 These Guidelines have been developed with reference to model whistleblower protection policies and reporting procedures developed by the Government Accountability Project, Dutch Whistleblowers Authority and the Irish Congress of Trade Unions.
1. Defining your company’s framework for protected internal reporting

A whistleblower protection and reporting policy is intended to encourage and enable workers to report wrongdoing in confidence without fear of retaliation.

1. Who can make a report

In general, protection from retaliation should be granted to all personnel whose reporting alleges company misconduct or actions that could incur liability for the company. Protection should cover all employees, regardless of their formal status, whether they are full time, part-time, temporary or permanent; consultants; contractors; employees seconded from another organisation; freelancers; interns; volunteers; self-employed or home workers. The protection should cover those who apply for jobs, contracts or other funding and also extend to former or retired employees who may have knowledge of wrongdoing from their previous employment. Providing protection to expatriate or foreign workers is also important to ensure that wrongdoing committed abroad is also brought to the attention of the company (e.g. bribery of foreign public officials). Companies that employ relatives of the reporting person who could also be the target of retaliation could consider extending protection to relatives; this could be the case for small or family-owned companies or corporate groups. By clearly defining a broad pool of people who may report, confidence is established in the whistleblower protection system and incentives are provided to come forward to reporting alleged wrongdoing.

Whistleblowing systems should be available for external suppliers, customers and other parties with an interest in the company, including the public if the company provides goods or services for public consumption. All reports must be treated equally under the reporting system. With respect to providing protection to those who report, it is only practicable for companies able to provide comprehensive protection to a restricted category of reporting persons.
These Guidelines refer mainly to “reporting persons”, consistent with the terminology of UN and OECD reports on whistleblower protection, which adopt a neutral terminology to avoid negative connotations often associated with “whistleblowers”.

2. What can be reported?

The policy should make clear that it protects disclosures of wrongdoings:

- That occurred in the past;
- Are currently occurring; or
- Are likely to occur.

2.1 Wrongdoing

Wrongdoing should be defined broadly to include dangerous, unethical or illegal practices which take place under the responsibility of the employer or in the context of the company’s activities that create risk. For the purposes of these Guidelines, wrongdoing is defined as including, but not being limited to:

- Breaches of the organisation’s policy or Code of Conduct;
- Breaches of law or regulation;
- Risk to public health, human safety, environment, proper functioning of the organisation;
- Waste of government funds;

3 The UN Convention against Corruption Resource Guide on Good Practices in the Protection of Reporting Persons (UN, 2015); Committing to Effective Whistleblower Protection (OECD, 2016).

4 Note: The Greek government expressed concerns about the fact that the proposed approach provides a broad definition of protected disclosure. The authorities would prefer a two-stage implementation. In the first instance, they would restrict the protection to the reporting of most serious crimes such as corruption, serious financial crime, offences against the environment and the public health and then, in a second time, they would consider expanding protection to other misconduct.
• Conflicts of interest;
• Miscarriage of justice;
• Disguising or concealing any of the above; or
• Any allegations that someone impeded or discouraged anyone from assisting in an internal investigation or legal proceeding

2.2 Reasonable belief

The individual making the report should not need to be certain about the facts in the disclosure, nor make an assessment as to whether it constitutes a specific criminal offence. The relevant standard for making a report should be that, in the reasonable belief of the worker, the information tends to show one or more relevant wrongdoings related to his/her employment. Reasonable belief should be considered as a belief that a peer with similar knowledge, training and experience could agree with. It is a relative concept and applies to what is appropriate given all of the factors involved in the situation.

To avoid any consideration of the potential motive of the reporting person being taken into account—and used as a basis for retaliatory or disciplinary measures—protected disclosures have been defined broadly, without any requirement that reports be made “in good faith”. This broad definition aims to encourage wide reporting of any wrongdoing. This could have the additional advantage of bringing conduct to the attention of management that, while not specifically in the public interest (e.g. theft or fraud), would be in the interest of the company.

3. Setting up the reporting mechanism

The policy of your company should describe the procedure to follow in order to report wrongdoing and provide guidance to employees on making a disclosure, internally and externally. Protection should be provided to those who report internally within the company, as well as those who report externally to law enforcement, the media or civil society.
3.1 Internal channels

Even if not required by law, companies are encouraged to set up protected internal reporting channels and provide guidance to employees on the use of these channels, in order to encourage resolution and follow up by managers.

Your company should appoint and identify a protected disclosure manager with sufficient authority to act on the disclosures received. It is crucial that the protected disclosure manager has the total confidence of the employees and, in particular, that s/he guarantees the confidentiality of the report and the identity of the reporting person. The manager should provide direct and timely follow up on the report. The most appropriate person to designate as protected disclosure manager will depend on the structure of your company.

Ideally, the protected disclosure manager would have a separate, independent function within the company to avoid conflict of interest or any perceived threat to his/her independence. However, for smaller companies, which may not have the resources to create such a function, this could be a dual function of another company officer who is well placed to report directly to the organisational head, such as:

- A chief compliance officer;
- A human resources officer;
- A legal officer or general counsel;
- A privacy officer;
- A chief financial officer;
- A chief audit executive; or
- A member of the board.

The role of the protected disclosure manager is to maintain the day-to-day operation of the disclosure policy and reporting mechanism and to act in response to a disclosure. The protected disclosure manager’s role and contact details should be communicated to everyone within the company.

Some companies choose to outsource their protected reporting program to an “external” provider to ensure independence and confidentiality and also if they do not have the capacity to
implement an internal reporting mechanism. Nonetheless, there should be a system in place to investigate reports received through this external provider that are considered well-founded. This system should be clearly defined and communicated to employees (including the extent to which the identity of the reporting person is communicated to management and on what basis). The external provider can be a third party authorised by the employer such as:

- An external reporting platform provider;
- An external counsel or auditor; or
- A Union representative.

Clear, safe and diversified reporting channels must be available to disclose allegations of wrongdoing. The company should provide written information to the persons working for the company about the reporting procedure and make it easy to find and to understand.

For instance the reporting channel could be one or several of the following:

- In person;
- By post;
- By physical complaint box(es);
- By designated e-mail address;
- By fax;
- By online platform (intranet or internet); or
- By telephone hotline (internal or external).

In-person reporting mechanisms have the advantage of being easy and direct but could discourage individuals from coming forward for fear of discussing their concerns with direct supervisors or senior managers. Companies should therefore make several reporting channels available, including the possibility of anonymous reporting. However, confidentiality should be encouraged rather than anonymity, even though there should be no presumption that anonymous complaints are less reliable. If the company decides to set up online or telephone reporting hotlines, it should bear in mind that employees may prefer to report outside of working hours. Furthermore, companies with foreign subsidiaries or expatriate or foreign workers will need to ensure hotlines are available in
accordance with different time zones and hotlines should also be available in several languages as appropriate.

3.2 External channels

Companies should provide information to their employees on how—and under what conditions—they can report to external authorities and/or the media, noting that employees should never be subject to contractual “gagging clauses” to prohibit them from reporting externally.⁵

In Greece, reports about corruption cases in the public and private sector can be made externally to the Office of Complaints of the General Secretariat against Corruption (GSAC).⁶ Furthermore, Article 40 of Greece’s Civil Procedure Code obliges all persons who become aware of a crime to report the matter to the public prosecutor or any law enforcement authority. The Greek Ombudsman is another potential reporting channel for employees of the private sector.⁷

It should be the common understanding of private and public sector organisations that reporting persons should first use internal reporting possibilities before reporting externally, unless there are certain specific situations. For instance, companies may consider defining circumstances under which an employee should make an external report, such as in cases where there is:

- No internal reporting channel in the company;
- A matter of significant and urgent public interest;
- A reasonable suspicion that the ultimate responsibility holder within the company is involved in the suspected wrongdoing;

---

⁵ See, for example “Whistleblowing and Gagging Clauses,” Briefing Paper Number CBP 7442, House of Commons Library (4 January 2016).

⁶ See Article 54 of Law 4446/2016, amending Laws 4320/2015 and 4325/2015: proposition to create an Office of Complaints under the General Secretariat against Corruption (GSAC).

⁷ Note: The Greek government would like to restrict protection to the reporting of most serious crimes in the first instance and considers that the main external reporting channel should be the prosecutor.
• A clearly identifiable threat of falsification or destruction of evidence;
• Reasonable reason to fear reprisals in connection with making an internal report;
• The internal report was not dealt with diligently or within a defined period;
• The internal report did not lead to a satisfying solution; or
• An earlier report about the same wrongdoing made in accordance with the procedure did not put an end to the wrongdoing.

3.3 Form of the report
To enable maximum reporting of wrongdoing, companies should not prescribe a specific form for making a report and should instead allow either oral or written reports through a variety of available channels. Nevertheless, companies should provide clear guidance and eventually a template to facilitate the collection of relevant information in order to facilitate the investigation.

Your policy should make clear that the reports should contain:
• A description of the wrongdoing;
• The date of the disclosure;
• The preferred contact details of the person reporting (if the person chooses to identify her/himself); and
• Any document or information that tends to show the wrongdoing.

3.4 Confidentiality
The company policy should clearly define what is meant by “confidentiality”. The reporting process should ensure confidentiality both of the content of the report and any information that could identify the person who reported (e.g. email signatures). Companies should ensure that information concerning the report is kept secure and that only the person that is in charge of dealing with the report can access it.

A failure to ensure confidentiality can entail civil and administrative consequences for the company, including under relevant data
protection legislation. In Greece, the use of internal reporting mechanisms must comply with data protection obligations set out in the Act Regarding Protection of Individuals with Regard to the Processing of Personal Data. This law transposes the EU Data Protection Directive (95/46/EU) and stipulates that the subject of a whistleblower report must be informed about the complaint and allowed to respond to the submitted allegations. Nevertheless, notifications may be delayed for as long there is risk that they would jeopardise the ability of the company to effectively investigate the allegation or gather the necessary evidence. This framework will soon be reinforced with the entry into force of the EU General Data Protection Regulation (GDPR) in May 2018.

There are strict circumstances under which confidentiality can be broken, for instance when:

- The person making the disclosure provides his/her written consent;
- It is necessary for the effective investigation of the relevant wrongdoing;
- It is necessary to prevent serious risk to the security of the State, public health, public safety or the environment;
- It is necessary to prevent a crime or to facilitate prosecution of a criminal offence; or

---


10 Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.
• The disclosure is otherwise necessary in the public interest or is required by law.

In cases where confidentiality cannot be maintained, the reporting person must be informed and s/he must provide his/her written consent for the information to be transmitted elsewhere and his/her identity disclosed. The reporting person should be advised that if consent is not given, it may not be possible to investigate the disclosure.

Anonymous concerns should be treated seriously and considered in accordance with this policy; however persons reporting could be invited to identify themselves when they make a report, in order to ensure protection from future retaliation and effective follow-up on the report.

4. What is retaliation?

Retaliation against reporting persons can take numerous forms. It can be direct or indirect, and can be carried out either by the reporting person’s management, other employees, third party business partners or clients. Retaliation can occur either before, during or after the report is made and result in the suffering of the reporting person or a change in his/her employment conditions. It is important to clearly define acts of retaliation against reporting persons in your company’s policy on protected internal reporting. The best practice standard is any discrimination that could chill the reporting. Retaliation only requires a causal link to reporting and should be defined to include (but are not limited to):

• Suspension or dismissal;
• Failure to convert a temporary employment contract into a permanent employment contract;
• Failure to renew or early termination of the temporary employment contract;
• Preventing the reporting person or his/her colleagues from investigating or discussing the matter;
• Unjustified poor performance evaluation;
• Preventing the reporting person from attending the workplace;
• Obligatory appointment of the reporting person to another position;
• Disproportionately limiting or expanding the reporting person’s duties (except at her/his own request) or working hours;
• Relocating the reporting person, changing her/his workstation, or refusing to do so (except at his/her own request);
• Preventing opportunities for promotion or demoting the reporting person;
• Withholding salary increase, reducing salary, withholding bonuses or any other allowance the reporting person is entitled to;
• Denial of opportunities and training;
• Exclusion from corporate social opportunities;
• Verbal or written harassment that intimidates the reporting person;
• Reduction in post-employment benefits.

5. Protection against retaliation

5.1 Who and when to protect

It is imperative that your company demonstrates that it is committed to ethical practice by supporting and protecting employees who report from breach of confidentiality (see above, Part 3.4 Confidentiality) and retaliation. The company policy must explicitly state that any discriminatory actions taken against an employee who makes a report or any other actions that could create a chilling effect on reporting will not be tolerated and could be subject to disciplinary measures. Companies should also consider protecting any witnesses to the wrongdoing or resulting retaliation. This can avoid a broader fear of reporting because of potential consequences for colleagues. The person(s) who are the subject of the report are also entitled to protection and should benefit from the presumption of innocence.

Protection should extend to reporting persons who reasonably believe that wrongdoing has, is or will occur even if the allegations
turn out to be incorrect and should include those who assist or are associated with whistleblowers. Protection should also be extended to individuals whom employers mistakenly believe to be whistleblowers and who suffer retaliation as a result of this mistaken belief.

It is very important that the policy specify that the protection is provided even when the person is technically required to provide the information, for example in the context of reports by auditors, quality control inspectors, and normal communication of problems to a supervisor. The report does not have to be made in the context of dissent or objection to workplace wrongdoing.

5.2 How to protect

In addition to protecting the identity of the reporting person through the provision of confidential reporting channels, the employer should define the broader scope of protection. For instance, protection can be extended beyond the workspace to include training events, conferences or corporate social events.

Protection against retaliation should not be limited to a specific period. This is because retaliation can occur long after the report has been made, for example when resulting investigations or sanctions become public years later. Reporting persons can also suffer retaliation even before making a report, such as when they discover the wrongdoing and start to ask questions about it or express their opinions.

Protective measures should also apply to prevent retaliation. Companies should create a system whereby the protected internal reporting manager or a separate advisor discusses with the reporting person the risks of unfair treatment, how those risks can be reduced and what the employee can do if s/he believes that s/he is being treated unfairly. Where appropriate, the employee’s ultimate manager should also ensure that measures to prevent retaliation are taken within the workplace or unit.

Reporting persons should be able to make a formal complaint about being retaliated against or about a breach of confidentiality. Channels for making such formal complaints should be multiple, similar to the channels available for reporting. The employee
making the formal complaint should have unrestricted access to escalating her/his case to higher corporate echelons. The policy of the company should also make clear that the protection provided by the company does not cut off or otherwise affects other rights and remedies available under Greek law.

The report alleging retaliation can be made to the designated personnel who handle whistleblower complaints (e.g. protected disclosure manager, legal officer, compliance officer or other responsible staff). These reports must be thoroughly and independently investigated and assessed with strict confidentiality and consequences should follow in the case that the retaliation is verified (see below, Part 6. What are the consequences for retaliation?).

The process for handling complaints of retaliation should be communicated to all employees and should be fully transparent with declared procedures, timeframes, protections against possible conflicts of interest and anti-retaliatory policies. Employees should also be enfranchised to participate in investigation of their reports by answering rebuttals or denials, as well as to have comments on the report included as an appendix to the report resolving issues they raised.

Companies should consider providing confidential advice to employees at the outset, during and after the reporting process. This could be provided either by the protected disclosure manager, a union legal expert, or through an external legal services provider who is not the company’s own external legal representative. In cases where employees engage external advice for reporting, companies could consider reimbursing the fees for such advice.

6. **What are the consequences for retaliation?**

The company’s policy must also explicitly state the consequences for retaliation against reporting persons. This will help ensure that employees who are considering making a report feel encouraged and safe and that potential retaliators are deterred out of fear for severe consequences for their own employment conditions.
When investigating whether an act is truly retaliatory, your company should establish a presumption in favour of the reporting person. In other words, the employer and/or the person responsible for the retaliatory measures should have the burden of proving that measures taken against the reporting person were reasonable, proportionate, justified and unrelated to the disclosure. This means that if the employer takes any negative measures against the reporting person in relation to a report, the employer must justify the measures and prove they were disconnected from the report.

Policies should state that acts of retaliation and reprisal constitute corporate wrongdoing that can lead to the company taking disciplinary action up to and including dismissal of the retaliator. These disciplinary measures should be applicable to all company employees, including third party business partners such as suppliers and clients whose contracts can be terminated, suspended or sanctioned if it can be proven that they have engaged in retaliatory behaviour against reporting persons.

II. Implementing your company’s protected internal reporting mechanism

This section is intended to guide your company in implementing the key components of its own framework for protected internal reporting.

1. Leadership and commitment

A company’s approach to business ethics stems from and is fostered by top-level management (i.e. CEO, Board of Directors etc.) through the establishment of policies and procedures that govern the company’s attitude towards ethical concerns and promote open communication. Similarly, the commitment of senior management is imperative to the development and implementation of an effective whistleblower policy within a company that motivates employees to report violations internally.

Internal reporting must be welcomed as a necessary process for maintaining transparency and accountability within the company. Regular communication about the reporting procedure by the board
or CEO as well as managers within the company, will set the expectation that all staff is responsible for the reporting of violations. Those relaying the message to the majority of employees must be well-informed of the company’s protected internal reporting framework. Every opportunity and channel to communicate the company’s commitment to ethical conduct should be utilised (i.e. company newsletters, top-level speeches to employees, company intranet, memos, social media etc.).

The commitment of top-level management must not be restricted to articulating the company’s ethical stance and encouragement of reporting; management must also be actively involved in the implementation of the reporting mechanisms, with oversight of their use and results, as appropriate. All reports received internally must be taken seriously and addressed promptly.

2. Acting on reporting and disclosure

2.1 Confirm the reception of the report

When a report is received, the protected disclosure manager must reach out to the person who made the report, without undue delay, to acknowledge in writing that the report has been received.

2.2 Decide whether to investigate the report

The protected disclosure manager should inform within a reasonable period of time, ideally no more than two weeks after the report is received, whether the company chooses to follow through with the report.

2.2.1 Grounds for not investigating a report

The protected disclosure manager should state in writing the reasons for declining to investigate the report. The reasons could include:

- Alleged acts that fall outside the definition of wrongdoing;
- The report has insufficient information to substantiate the allegation;
- The report calls for intrusive inquiries into a person’s sexual, health, religious or political beliefs;
• The matter of the report has already been resolved.

2.2.2 Grounds for investigating a report

The protected disclosure manager should provide indications on how the matter will be dealt with, including an approximate date by which the person should expect a follow up, within a reasonable period.

In order to protect any individuals accused of wrongdoing, an initial inquiry should be conducted to decide whether the report should be followed by an informal or formal investigation and what form it should take. At this stage, the person to whom the report relates should be informed in writing.

The following actions should be considered in response to matters raised in the report:

• Be investigated by management assisting the protected disclosure manager, or internal audit;
• Be referred to the external auditor;
• Be referred to external enforcement agency or regulator, depending on its seriousness;
• Form the subject of an independent (third party) inquiry; or
• Be dealt with under in accordance with the company’s disciplinary procedures.

2.3 Carrying out the investigation

The protected disclosure manager should inform the reporting person in writing whether the decision has been taken to investigate the report and, where appropriate, the identities of the persons carrying out the investigation. This communication could invite the reporting person to a meeting or a call to further develop her/his concerns. The content of the interview should be recorded in writing and a copy provided to the reporting person.

All personnel involved in the investigation of the reporting person’s allegations should be contractually bound by a confidentiality agreement to handle the entire case confidentially throughout all stages without disclosing information about the case or the identity of the reporting person, the person to whom the report relates or
other involved parties. The confidentiality agreement should set forth the consequences of its breach.

The person who is the subject of a report should be notified and s/he should be informed that s/he can seek independent legal advice to ensure her/his rights are protected. The reporting person should also have the right to answer initial denials of his/her allegations.

### 2.4 Provide follow-up to the reporting person

Once it has been decided to investigate the report, it is vital that the protected disclosure manager maintains regular contact with the reporting person during the investigation. The regularity and content of the contact will depend on the nature of the matters raised and the clarity of the information provided.

Once the investigation is concluded, the protected reporting manager should inform the reporting person of the outcomes, including how the concerns raised in the disclosure were dealt with and what action was taken to rectify the wrongdoing. The person who reported the alleged wrongdoing should be allowed to raise any concerns about the outcomes. It is important that those concerns be included in record of final report.

Should the reporting person consider that the issue has not been resolved satisfactorily, s/he should then be able to report externally.

To ensure effective protection of reporting persons, the protected disclosure manager ought to follow up with the individual after a certain amount of time (e.g. one year) to ensure the person has not been retaliated against.

### 3. Maintain confidential, adequate and auditable documentation of all reports received

All reports received should be maintained in a relevant record together with documents collected for investigations, in compliance with relevant laws and regulations (including accounting and auditing requirements and data protection and privacy legislation).
The confidential report register should provide, for each report received:

- All the communications with the reporting person and the person to whom the report relates;
- Documents and interview transcripts collected for investigations;
- Documentation of the outcomes of the investigations; and
- Any further observations of the reporting person after being informed of the outcomes.

4. **Provide regular training on the whistleblowing policy**

In order to encourage internal reporting, companies should consider the following elements when designing and implementing a protected internal reporting framework. Companies should regularly disseminate information and train management and staff on what the protected internal reporting mechanism offers:

- What is wrongdoing and how to identify it;
- What is the basis for a “reasonable belief” that wrongdoing is occurring;
- The internal and external reporting channels;
- The contact details of the protected disclosure manager;
- How to file a report;
- How reports are dealt with;
- Any relevant follow-up procedures;
- How the company identifies next steps for reports that are well-founded;
- Conduct that is considered to be retaliatory;
- Protections against and remedies for retaliation; and
- Consequences for retaliation against reporting persons.

Companies should also make clear that no employee will suffer retaliation, discrimination or disciplinary action for reporting suspected wrongdoings as defined in section 2.1.
5. Communicating about your policy - Fostering a “speak-up culture”

Whistleblower protection is most effective when it functions in a corporate environment that fosters an open-door culture that encourages employees to stand up against wrongdoing and speak about their concerns without fear of retaliation.

Encouraging employees to speak up, however, can prove very challenging, particularly in certain parts of the world where negative associations with whistleblowing and anonymous accusations can be traced back to historical incidents. This is also the case in Greece, where unfavourable attitudes towards whistleblowers seem to persist, with the term being closely linked to notions of “snitching” and “betrayal for personal gain”.

Overcoming these notions is essential in order to construct an organisational culture that encourages ethical conduct and a “speak-up culture”. This can be more complex for larger companies operating across various geographical locations than smaller companies, but the approach remains the same for both.

The approach to positive organisational change is twofold: to break down the negative connotations associated with whistleblowing and instead create a culture of open-dialogue and reporting. The first approach is to focus on the deficit; the company must be responsive to all reported and unreported wrongdoing, plan remedies and analyse root causes, demonstrating an urgent response approach to all identified unethical corporate behaviour. Secondly, an appreciative, positive focus must follow; one that seeks to draw on the human strength of employees so that the organisation can become even better and more ethical. Both approaches must be implemented to address the problems created by the minority and help the majority prevent future problems.

---

Furthermore, the term “whistleblower” must be normalised within the company culture. It should be closely associated with notions of speaking up in the company’s interest about wrongdoing, injustice and risk. It should be treated as an act of loyalty and concern for the greater benefit and interests of all employees by alerting those who are able to take steps to mitigate or remediate problems that may prove to be detrimental to the well-being of all employees and/or the greater public interest.

From a practical perspective, the communication strategy stemming from higher leadership must be designed to encourage employees to make ethical decisions. This messaging must be incorporated in periodic communication throughout the company to all employees, incorporating key words such as “integrity”, “compliance”, “reporting of unethical behaviour”, that in the long run can help comprise the core of the corporate culture. Discussing the internal mechanisms available to employees who wish to report and the strict upholding of company policies regarding employee retaliation is vital to ensuring that employees feel secure and supported.

The company could consider communicating through the different medium to make sure that every potential reporter is aware of the whistleblowing channels:

- Newsletters
- Email correspondence
- Trainings
- Publishing regularly on the internet/intranet page

The role of the protected disclosure manager should be brought to the attention of all staff. Where possible, the protected disclosure manager should have an opportunity to meet and introduce her/himself to employees. The company should also inform employees of the advice function of the manager (or other independent advisor) for those who are considering making a report and throughout the reporting and investigation process. Where reporting persons are willing, and there is no risk of subsequent retaliation, they could be publicly rewarded or praised within the company for reporting wrongdoing, along with providing general information about the action taken to address the report and any resulting retaliation. This is a way of communicating the
effectiveness of the protected internal reporting framework. On the other hand, the issue of communicating about the framework raises important issues of protecting the identity and the identifying information of the reporting persons as well as those who are the subject of the report, particularly in small companies. Any public or internal corporate reporting should be carefully considered and balanced with the risks of retaliation or violation of data protection rights.

Ethical dilemmas should be discussed regularly in staff meetings in a safe space or in the context of training activities. Managers should be tasked with teaching employees about complying with the company’s anti-corruption policies and the overarching company values. To ensure that managers are effective in this task, the company could disseminate periodic feedback surveys to employees questioning whether they are aware of the protected internal reporting framework.

6. Incentivising and rewarding whistleblowing

Greek companies should actively promote their anti-corruption programmes by adopting appropriate incentives for compliance at all levels of the company in general and for whistleblowing more particularly. Employees may fear retaliation if they report wrongdoings, therefore providing incentives may encourage them to come forward.

Nearly all of the companies operating in Greece (approximately 86%) that responded to the OECD Private Stakeholder Survey claimed that they do not offer or do not know if they offer incentives to their employees in order to encourage compliance.

12 OECD Good Practice Guidance on Internal Controls, Ethics and Compliance, A. 9; “Within a company, some organisations have also sought to incentivise “compliant” behaviour within their human resources strategy, for example, by tying performance-based bonuses and remuneration to compliance, and promotion of the company’s business integrity programme. The challenges for this exercise were discussed by the 2011 OECD paper on Board Practices: Incentives and Governing Risks (Box 14).” (available at: http://www.oecd.org/daf/ca/49081438.pdf).
with their code or programme. A common theme that emerged from the Survey and the consultation meetings was that the act of whistleblowing is tantamount to spying or snitching. It is not uncommon for the individual who reports a violation to be ostracised or blacklisted, sometimes even when s/he supposedly submitted an anonymous complaint. Therefore, in light of these issues, an approach seeking to strengthen compliance in general and provide support to whistleblowers must not only include a structural component but also a behavioural and cultural component.

Within a company, an explicit commitment to whistleblower protection and a reporting system can incentivise reporting of wrongdoing. Financial rewards can also incentivise reporting and companies have been known to provide bonuses or promotions in recognition of staff who report wrongdoing. Non-financial recognition that provides institutional vindication and recognition are an option that deserves to be explored. For instance, an effective way to demonstrate commitment and to exercise leadership changing corporate culture is to institute positive reinforcement through annual Ethical Conduct Awards for those whose disclosures have made the most difference helping the company. Any awards system must, of course, take into account overarching requirements or requests for confidentiality of the whistleblower.

7. Monitoring, oversight, review and evaluation of the policy

Ongoing monitoring and review of the protected internal reporting framework is vital to guarantee that it operates effectively. A designated group of individuals within the company should be identified to review and analyse how investigations into reported wrongdoing were conducted and their outcomes.

The internal audit division of a company is most often designated to monitor and review the existing whistleblowing mechanisms due to its extensive working knowledge of all parts of the company. The internal audit function usually receives information and collaborates closely with the compliance or legal departments. In cases where the internal audit division is also responsible for the administration of the internal reporting mechanism, it is advised that an external party is tasked with the monitoring and reviewing process. The Board or company should oversee the reporting framework and its evaluation and be provided with a detailed review by the administrators of the reporting mechanisms who can demonstrate how reports are addressed in various situations.

Evaluating the whistleblower mechanism can also reveal gaps that need to be remediated. Companies are constantly evolving, regulatory and legal requirements change both in the country where the company is located and where it conducts business abroad, and personnel is reassigned, therefore it is important that the reporting mechanisms in place adapt to these changes. External parties can also conduct independent and objective monitoring and evaluation.

Effective monitoring of the internal controls and existing whistleblowing mechanisms should take into consideration whether awareness raising and training activities are in place for all employees (including senior managers and executives) and third party business partners. Furthermore, it is important that the influence of the tone at the top is examined so as to ensure that it reinforces the company’s zero-tolerance stance on unethical behaviour.

For companies with a multinational presence, legal whistleblower protections vary from country to country and according to allegation. It is therefore important companies tailor the protected internal reporting frameworks accordingly.

Several indicators can be used to measure the overall effectiveness of a company’s whistleblowing program, including the timeliness and appropriateness of investigations; whether wrongdoing comes
to an end; measures taken within the organisation to change its policies and procedures when necessary. On a practical level, some companies evaluate the effectiveness of their protected internal reporting mechanisms by generating random “fake” reports to test and analyse responses to reports of wrongdoing. It is important that even senior level management is unaware of the test, to ensure the efficiency of the entire system.

In terms of the common cultural challenges of viewing whistleblowers as snitches, a company must review whether or not it makes a significant effort to reduce the stigma associated with reporting wrongdoing and reinforce the idea that reports that help detect or prevent unethical behaviour within a company are beneficial for all employees and stakeholders. This can further be strengthened by ensuring that it is safe, tolerable and expected to make a report and that the fear of those who do come forth is mitigated by preventing and protecting against retaliation.

Finally, the review must also consider whether all reports are received and processed within a timely manner by specialised individuals who are fully informed of whistleblower procedures and rights, ensuring that whistleblower confidentiality is maintained and steps are taken to prevent, detect and punish retaliation. Prior reporting persons and employee representatives should be involved in each step of this review process.

14 St-Martin, Frederic, Measuring the Effectiveness of Canadian Whistleblowing Law (October 30, 2014).