

Protection of Whistleblowers: Guide for Employers



Protection of Whistleblowers:

Guide for Employers

This Guide was prepared by the Ministry of Justice and Public Order, in collaboration with the Office of the Law Commissioner, in February 2023 and revised in April 2024.



MINISTRY OF JUSTICE AND PUBLIC ORDER
REPUBLIC OF CYPRUS



OFFICE OF THE LAW COMMISSIONER
REPUBLIC OF CYPRUS

Table of Contents

A. Introduction	1
B. Protection of whistleblowers.....	2
1. Persons protected by the Law.....	2
2. Reports protected by the Law	3
3. Submission of reports	4
3.1. Internal report.....	5
3.2. External report.....	5
3.3. Public disclosure	6
4. Relationship between internal and external reports	6
C. Obligation to establish internal reporting channels	9
1. Which legal entities have an obligation to establish internal reporting channels?	9
2. Who can be designated as internal reporting channels?	10
D. Obligation to establish procedures for receiving internal reports and following-up	12
1. Means for submitting reports and acknowledgment of receipt of the report.	12
2. Follow-up of reports and feedback to the whistleblower	13
3. Provision of information regarding the procedures for submitting internal reports and external reports to competent authorities	14
4. Confidentiality of the identity of the whistleblower and of any other person concerned	14
5. Confidentiality of trade secrets	15
6. Processing of personal data.....	15
7. Record keeping of the reports	16

E. Obligation to take measures of protection and support for whistleblowers	18
1. Prohibition of retaliation	18
2. Obligation of the employer to provide assistance.....	20
3. Obligation to provide information to employees.....	20
4. Prohibition of waiver of rights and means of legal protection	20
F. Consequences of violating the Law	21
1. Violation against whistleblowers	21
1.1. Criminal liability of legal entities.....	21
2. Violation by whistleblowers	22

A. Introduction

On February 4, 2022, the Protection of Persons who Report Breaches of Union and National Law, Law of 2022 (Law 6(I)/2022, as amended) (“**Law**”) entered into force. The Law aims to establish an effective and strong legal framework for the protection of those employees in the public or private sector who disclose information that came into their possession or attention in the workplace and are related to specific breaches of European Union law and/or national law.

The Law encourages and enables employees to submit complaints (“reports”) of potential breaches through secure procedures, in a confidential setting. At the same time, the Law prohibits any retaliation either by their superiors or colleagues and provides for strong support measures. Consequently, the Law creates obligations for employers (public and private sector legal entities) to establish and operate a comprehensive framework for the protection of employees who report breaches.

The main obligations for employers include the obligation to establish internal reporting mechanisms (channels), the obligation to adopt measures to follow-up on the progress of the report, and the obligation to take measures for the protection of employees reporting breaches. Additionally, and in relation to specific public authorities, the Law creates an obligation to establish external reporting mechanisms (channels) and adopt measures to follow-up their progress.

This Guide is addressed to employers in the public and private sector. It explains the rights of employees who submit reports of possible breaches, the obligations of employers to establish reporting channels and provides guidance on how to implement and comply with the provisions of the Law.

B. Protection of whistleblowers

1. Persons protected by the Law

The Law aims to protect the “whistleblower” (or the “reporting person”, as referred to in the Law). That is, it protects that person who submits a “report” or makes a “public disclosure” of information obtained in the workplace (in the public or private sector) from which it appears that another natural or legal person has breached certain legal obligations.

“Report” is the submission of information/complaint by the whistleblower (either anonymously or by giving his/her name) to a competent person in relation to potential breaches.

“Public Disclosure” means the making of information on breaches available to the public, under the conditions set by the Law (see section B.3.3 below).

Whistleblowers can be:

- employees in the private, public or wider public sector;
- self-employed persons;
- company shareholders;
- persons belonging to the administrative, management or supervisory body of an undertaking;
- volunteers;
- paid or unpaid trainees;
- persons working under the supervision and direction of tenderers, subcontractors and suppliers;

- persons who obtained the information in the workplace but no longer work or provide their services to the specific employer;
- persons who obtained information on breaches during the recruitment process or other pre-contractual negotiations or before the commencement of employment.

The Law further protects persons who did not make a report or a public disclosure themselves, but who are associated with whistleblowers and fall into one of the following categories:

- “facilitators”, meaning persons who assist a whistleblower in the reporting process in the workplace and whose assistance is confidential;
- persons connected with the whistleblower, such as colleagues or relatives by blood or kinship up to fourth degree (i.e. parents, siblings, uncles, aunts and first cousins);
- legal persons that the whistleblower owns, works for or is otherwise connected.

To enjoy the protection of the Law, a whistleblower can submit the report by giving his or her name. In the case of an anonymous report, the Law protects persons who, while submitting the report anonymously, have subsequently been identified.

2. Reports protected by the Law

The content of the report or public disclosure must relate to breaches of either national law or European Union (EU) law.

Breaches of national rules may relate to:

- commission of a criminal offense (e.g. offences of corruption);
- breach of a lawful obligation imposed to a person by the laws or regulations of the Republic;
- breaches which put or may put in danger the safety or health of any person;
- breaches which cause or may cause damage to the environment.

A report for breaches of EU law may relate to the following EU sectors:

- public procurement;
- financial services, products and markets;
- money laundering;
- terrorist financing;
- product safety;
- transport safety;
- protection of the environment;
- protection from radiation and nuclear safety;
- food and feed safety, animal health and welfare;
- public health;
- consumer protection;
- protection of privacy and personal data and security of network and information systems;
- safeguarding the financial interests of the Union;
- competition and state aid rules;
- corporate tax or arrangements for the purpose of obtaining a tax advantage.

Finally, it is worth noting that the Law does not cover:

- reports of breaches of the procurement rules involving defense or security aspects unless they are covered by the relevant acts of the Union;
- reports of breaches of rules of certain acts issued by the EU in the sectors of financial services, products, markets and the prevention of money laundering and terrorist financing, transport security, and environmental protection, providing for special rules when reporting breaches (see Part II of the Annex to the Law).

3. Submission of reports

A whistleblower can submit the report either internally, within his or her workplace (i.e. to an “internal reporting channel”), or externally, to a national body responsible for investigating the specific act (i.e. to an “external reporting

channel”). In addition, a whistleblower may, under certain conditions set by the Law, make a public disclosure, that is to disclose information to the press, mass media or social media.

3.1. Internal report

“Internal report” means the submission of information by the whistleblower, anonymously or by giving his/her name, to a department or person(s) designated by the employer as responsible for receiving, investigating and following-up on such reports.

Employers are obligated to establish procedures for submitting internal reports, as well as follow-up procedures. They are further required to inform their employees about these procedures.

“Follow-up” means any action taken 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.

3.2. External report

“External report” means the submission of information by the whistleblower, anonymously or by giving his/her name, to a “competent authority” which receives complaints, information or is responsible for the supervision and/or the investigation of any possible breach of acts found in the complaint (for the obligations of competent authorities, see “Protection of Whistleblowers: Guide for Competent Authorities”).

3.3. Public disclosure

In addition to internal and external mechanisms for submitting reports, a whistleblower may make a “**public disclosure**”, that is to disclose information to the press, mass media or social media.

However, in the case of public disclosures, the Law sets strict conditions which must be met in order for a whistleblower to benefit from the protection of the Law.

Specifically:

- (a) prior to making a public disclosure, the whistleblower must have submitted either an internal or external report, but no action has been taken within 3 months of the submission of the report; or
- (b) the whistleblower has reasonable grounds to believe that-
 - i. the public interest or public health is threatened by an imminent or manifest danger or a risk of irreversible damage or there is another serious emergency situation, or
 - ii. in the case of external reporting, there is a risk of retaliation or there is a low prospect of the breach being effectively addressed due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed or where an authority may be in collusion with the perpetrator of the breach or involved in the breach.

4. Relationship between internal and external reports

In principle, whistleblowers are encouraged to use the internal mechanisms in their workplace to submit their report, thus enabling their employers to address the situation immediately.

However, it is acknowledged that this is not always possible or desirable. There are cases where a whistleblower will prefer to directly contact persons outside their workplace; and for that reason, the Law leaves the choice to the whistleblower.

That is, the whistleblower can submit his/her report internally and in case the breach is not effectively addressed, then he/she can submit a report to a “competent authority”, or directly submit it to a “competent authority”.

If, for example, a person working in a Ministry has information that his/her colleague has committed the offence of bribery, then he/she has two options. The first option is to contact the person(s) or department of the Ministry that has been designated as the person(s) responsible for receiving internal reports. The second option is to contact directly the competent authority, by submitting an external report. In this example, and since the possible breach relates to corruption, the competent authority could be the Police or the Independent Authority against Corruption.

It should be noted that if a whistleblower submits both an internal and an external report, he/she should inform the internal reporting channel accordingly, and the internal reporting procedures should be terminated.

Furthermore, in case the whistleblower submits an external report to more than one competent authorities at the same time, he/she should inform them to that effect, so that the competent authorities can coordinate with each other in handling the reported breach.

A person is considered a “whistleblower” and is protected by the provisions of the Law if:

1. he or she falls into the categories of persons referred to in section B of this Guide and has collected the information in the context of his/her work-related environment,
2. the information concerns breaches of national or EU legislation referred to in section C of this Guide,
3. he or she had reasonable grounds to believe that the information concerning breaches reported was true at the time of the report,
4. the report was submitted internally through the internal reporting channels or externally to a competent authority, or the person made a public disclosure under the conditions set by the Law,
5. the information must not have been given in violation of the rules of protection of classified information, legal or medical professional privilege, secrecy of judicial deliberations and the rules on criminal procedure, or access to and disclosure of it would not constitute a criminal offence.

C. Obligation to establish internal reporting channels

1. Which legal entities have an obligation to establish internal reporting channels?

The following entities have an obligation to establish “channels”, that is, to designate persons or departments for receiving reports:

(a) all legal entities of the public and wider-public sector (e.g. public services, semi-governmental organizations, offices of independent authorities)

For the purposes of the Law, **legal entity in the public or wider-public sector** means the public service and any independent service or authority for which provision is made in the annual public budget. This definition includes the Police, the Cyprus Fire Service, the Public Education Service, the Armed Forces of the Republic as well as any public corporate body or public law organization, including the local authorities or any other public law organization without legal personality established by law for the public interest the funds of which, are either provided for or guaranteed by the Republic. It further includes a legal entity and a state or semi-state company, that is, a legal entity under private law whose share capital is wholly or partially owned by the Republic or by a legal entity under public law or by another state or semi-state company.

Local authorities with fewer 5000 inhabitants, or fewer than twenty-five (25) employees are excluded from the obligation to establish internal reporting channels.

Local authorities may use common internal reporting channels, provided that the shared internal reporting channels are distinct from and autonomous in relation to the relevant external reporting channels.

(b) legal entities of the private sector, employing 50 or more employees (e.g. companies, industries, etc.)

It should be noted that legal entities in the private sector with 50 249 employees must establish internal reporting channels by December 17, 2023.

(c) legal entities in the private sector with less than 50 employees falling within the scope of the union acts referred to in parts I.B and II of the Annex

These are mainly legal entities that are active in the fields of financial services, products and markets, prevention of money laundering and terrorist financing. These legal entities should establish internal reporting channels regardless of the number of persons they employ.

In relation to the rest of the legal entities of the private sector that employ less than 50 employees, although they are not obliged to establish channels, the Law encourages them to do so on a voluntary basis.

2. Who can be designated as internal reporting channels?

A person(s), agency or department within the legal entity in the private and public sector may be designated as competent to receive and follow up on internal reports, i.e. complaints submitted by their employees. The person, department or agency to be designated depends on the structure of each legal entity.

Examples of “internal channels”:

- chief compliance officer,
- human resources officer,
- integrity officer,
- legal or privacy officer,
- chief financial officer,
- chief audit executive.
- members of the board.

Public corporate bodies with internal audit units established based on decisions of the Council of Ministers or pursuant to the provisions of any law, may designate such internal audit units as internal reporting channels.

For instance, legal entities in the public sector that have established internal audit units by virtue of the Decisions of the Council of Ministers with no. 75.841 dated 10.7.2013 and no. 76025 dated 6.11.2013, may use such units as internal reporting channels.

Moreover, third parties (i.e. persons who do not belong to the legal entity's workforce) can also be authorized to receive internal reports.

Examples of "third parties":

- external reporting platform providers,
- external counsels,
- auditors,
- trade union representatives,
- employees' representatives.

In any case, internal channels must offer appropriate guarantees of respect for independence, confidentiality, data protection and secrecy of the identity of every whistleblower, person concerned, and third person referred to in the report, and must prevent access thereto by non-authorized staff members.

D. Obligation to establish procedures for receiving internal reports and following-up

Legal entities of the public and private sector that have an obligation to establish internal reporting channels must design and establish specific procedures for receiving and following-up on reports.

The Law does not provide for the establishment of specific procedures for submitting, receiving and following-up on the internal reports, however it sets some minimum requirements:

1. Means for submitting reports and acknowledgment of receipt of the report

Internal channels shall enable reporting in writing or orally, or both.

Oral reports may be submitted via:

- telephone,
- physical meeting, upon request by the reporting whistleblower,
- recorded voice messaging system, subject to the consent of the whistleblower (see also section D.7).

Written reports may be submitted via:

- electronic mail,
- filling in of special form,
- fax.

After receiving the report, and within seven days, an acknowledgement of receipt must be transmitted to the whistleblower.

2. Follow-up of reports and feedback to the whistleblower

Legal entities in the private and public sector have a further obligation to establish procedures for diligent “**follow-up**”.

The term “**follow-up**” refers to the assessment of the accuracy of the allegations made in the report and, where relevant, the adoption of measures to address the breach reported. The follow-up may be carried out by the same person or department as the one that receives the reports or by another impartial person or department designated for this purpose.

Examples of follow-up action:

- internal enquiry and provision to the whistleblower of information on the action envisaged or taken to address the breach,
- referral to a competent authority for further assessment,
- investigation,
- prosecution,
- action for recovery of funds,
- the closure of the procedure due to insufficient evidence.

The whistleblower must receive “**feedback**”, within 3 months from the acknowledgment of receipt of the report, on the progress of the investigation of the report.

“**Feedback**” refers to the provision of information to the whistleblower on the action envisaged or taken as follow-up and on the grounds for such follow-up.

3. Provision of information regarding the procedures for submitting internal reports and external reports to competent authorities

Employers are obliged to inform their employees of the procedures in place for submitting internal reports. That is, they must provide information regarding the person(s), service or department responsible for receiving the reports, as well as the available means for submitting a report for possible breaches of national or EU law.

Moreover, the employers must provide clear and easily accessible information regarding the procedures for submitting external reports to competent authorities (see “Protection of Whistleblowers: Guide for Competent Authorities) or, where relevant, to institutions, bodies, offices, or agencies of the Union.

4. Confidentiality of the identity of the whistleblower and of any other person concerned

The channels receiving internal reports must ensure the protection of the confidentiality of the identity of the whistleblower and of the person concerned or of any other information from which the identity of the whistleblower may be directly or indirectly deduced. Disclosing any information that might identify the whistleblower or the person concerned to staff members other than those responsible for receiving or handling the report is prohibited.

Exceptionally, the identity of the whistleblower may be disclosed provided that:

- (a) the whistleblower explicitly consents to that,
- (b) the disclosure is a necessary and proportionate obligation imposed by EU or national law, in the context of investigations by national authorities or judicial proceedings, inter alia, with a view to safeguarding the rights of defense of the person concerned.

Before proceeding to the disclosure of the identity of the whistleblower, and provided that such disclosure does not jeopardize the related investigations or judicial proceedings, the internal reporting channels must inform the whistleblower accordingly and must send him/her an explanation in writing of the reasons for the disclosure of the confidential data concerned.

5. Confidentiality of trade secrets

If the internal reporting channels receive information on breaches that includes trade secrets, then they shall not use or disclose those trade secrets for purposes going beyond what is necessary for proper follow-up on the report.

6. Processing of personal data

Any processing of personal data (i.e. any information which relates to an identified or identifiable natural person, such as name, identity, telephone number) during the receipt or follow-up of reports is carried out in accordance with the provisions of Regulation EU 2016/679, the Protection of Natural Persons Against the Processing of Personal Data Law and of the Protection of Natural Persons Against the Processing of Personal Data by Competent Authorities for the purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties and on the Free Movement of such Data Law. At the same time, any exchange or transmission of information by EU institutions, bodies, offices, or agencies shall be undertaken in accordance with Regulation EU 2018/1725.

Personal data, which are manifestly not relevant for the handling of a specific report shall not be collected and, where they are accidentally collected, shall be deleted without undue delay.

7. Record keeping of the reports

Employers shall keep records of every report received, in compliance with the confidentiality requirements (see section D.4 and D.5).

Where a **recorded telephone line or another recorded voice messaging system** is used for reporting (subject to obtaining the consent of the whistleblower), the internal reporting channels may document the oral reporting:

- (a) by making a recording of the conversation in a durable and retrievable form;
- or
- (b) through keeping a complete and accurate transcript of the conversation.

Where an **unrecorded telephone line or another unrecorded voice messaging system** is used for reporting, the internal reporting channels may document the oral reporting in the form of an accurate transcript of the conversation.

Finally, where the report was submitted by means of a **physical meeting**, and subject to the consent of the whistleblower, the internal reporting channels ensure that complete and accurate minutes of the meeting are kept in a durable and retrievable form. The content of the conversation during the meeting is documented:

- (a) by making a recording of the conversation in a durable and retrievable form;
- or
- (b) through accurate minutes of the meeting.

In all three cases described above, the whistleblower must be offered with the opportunity to check and rectify the minutes of the meeting by signing them.

Personal data collected in the context of receiving and following-up on the reports shall be deleted within three (3) months from the date of closure of the procedure.

However, where judicial or disciplinary proceedings have commenced against the person concerned or the whistleblower (including appeal or objection proceedings), the personal data shall be maintained for the whole duration of the

said proceedings and shall be deleted after the expiration of one (1) year from the date of their closure.

E. Obligation to take measures of protection and support for whistleblowers

1. Prohibition of retaliation

Natural and legal persons of the private and public sector are prohibited from engaging in any form of retaliation, or threats of retaliation against whistleblowers. Retaliation may take the following forms:

- suspension, lay-off, dismissal or equivalent measures;
- demotion or withholding of promotion;
- transfer of duties, change of location of place of work;
- reduction in wages, change in working hours;
- withholding of training;
- a negative performance assessment or a negative employment reference;
- imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;
- coercion, intimidation, harassment or ostracism;
- discrimination, disadvantageous or unfair treatment;
- failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he/ she would be offered permanent employment;
- failure to renew, or early termination of, a temporary employment contract;
- harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
- 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;
- early termination or cancellation of a contract for goods or services;
- cancellation of a license or permit;
- psychiatric or medical referrals;

- unilateral detrimental change of working conditions, that is any act or omission or the behavior, in general, of an employer or any other person, who is competent or responsible for the determination or the change of the working conditions, which causes direct or indirect, material or moral, damage to the worker or offends, in any way, his/her personality or his/her dignity.

It is noted that, in the event that retaliation of any kind was imposed against the whistleblower, then he/she can ask his/her employer to restore the situation to the state it was in before the retaliation. The employer can refuse to take actions for reinstatement only in the event that this is objectively impossible or becomes disproportionately burdensome (as for example in the event that the company does not operate due to a suspension of its operations or in the event of a change in economic conditions), **but not** when these events occurred as a result of the employer's actions (such as when, due to the dismissal of the whistleblower, a new employee was immediately hired to fill the vacated position of the whistleblower, so that the latter was considered redundant).

Failure to take corrective measures by the employer is considered an aggravating factor in the imposition of the penalty, in the event of a violation of the Law (see point F, below).

In the event that the employer fails to protect the whistleblower from retaliatory conduct or harm, the whistleblower may request from a competent court (Industrial Disputes Tribunal or District Court or Administrative Court, as the case may be), to remove any retaliation and may claim compensation.

In such case, a rebuttable presumption is created that the harm is the result of retaliation because of the submission of the report. Therefore, it is up to the employer to prove that the measure that caused the harm did not constitute retaliatory action but was based on duly justified reasons unrelated to the submission of the report. At the same time, the competent court may issue temporary/interim protection measures, pending the lengthy court proceedings, in order to prevent or terminate retaliation.

2. Obligation of the employer to provide assistance

All employers shall protect their employees against any act by their superior or by any other employee which constitutes retaliation due to reporting and take any appropriate and prompt measures to prevent the acts. All employers, immediately after specific retaliation comes to their attention due to the submission of a report, shall take any available measure for the removal of retaliation, as well as for the removal of its consequences.

Where an employer does not take the measures to prevent the above behavior, may be jointly liable for the civil wrong with the person who committed the said acts, thus the employer may have the same liability as if they have retaliated or threatened to retaliate against a whistleblower themselves.

3. Obligation to provide information to employees

Employers must provide comprehensive and independent information and advice, which is easily accessible to the public and free of charge, on procedures and remedies available, on protection against retaliation, and on the rights of the person concerned. For this purpose, the employers shall prepare informative material in which the necessary information, advice and remedies available on protection are included.

4. Prohibition of waiver of rights and means of legal protection

The employers cannot force their employees to waive or limit their rights and means of legal protection provided for by the Law by any agreement, policy, form or condition of employment. Any such condition is void *ab initio*.

F. Consequences of violating the Law

1. Violation against whistleblowers

Actions against whistleblowers may result in the initiation of legal proceedings by whistleblowers seeking compensation for any harm they may have suffered. At the same time, and depending on the seriousness of the violation, certain actions can even lead to the establishment of a criminal offense.

Specifically, as the Law provides, a person who obstructs the submission of a report or engages in retaliation against a whistleblower or initiates malicious proceedings against such a person or reveals the identity of a whistleblower, is guilty of a criminal offense and, in case of conviction, is subject to imprisonment not exceeding three (3) years or a fine not exceeding thirty thousand euros (€30,000) or both.

1.1. Criminal liability of legal entities

A legal entity may also have criminal liability and may be prosecuted for any offence provided for by the Law which is committed on behalf of the said legal entity by any person who acts either individually or as a member of a body of this legal entity or exercises managerial power within this legal entity. Such managerial power may be based either on a power of representation or on a decision-making power for account of the legal entity or on a power to exercise control within the legal entity.

Moreover, legal entities may be criminally liable in case where the lack of supervision has made possible the commission of any of the offences described above, by persons under their authority.

In both cases, the legal entity shall be liable to a fine not exceeding thirty thousand euros (€30.000).

2. Violation by whistleblowers

As already explained in the previous sections of this Guide, the Law creates a strong legal framework for the protection of persons who submit reports in accordance with the prescribed procedures and conditions.

In order to avoid any abuse of the Law, but also to protect the rights of persons who may suffer harm due to malicious or non-existent reports, the Law provides for severe penalties while at the same time guaranteeing the right of these persons to compensation, in case they have suffered damage from false or misleading reports or false or misleading public disclosures.

Moreover, the Law provides that a person who knowingly makes false reports or false public disclosures is guilty of a criminal offense and, upon conviction, is liable to imprisonment for a term not exceeding three (3) years or to a fine not exceeding thirty thousand euros (€30,000) or both penalties.