

MINISTRY OF JUSTICE AND PUBLIC ORDER

OFFICE OF THE LAW COMMISSIONER

Protection of Whistleblowers: Guide for Competent Authorities



MINISTRY OF JUSTICE AND PUBLIC ORDER
REPUBLIC OF CYPRUS



OFFICE OF THE LAW COMMISSIONER
REPUBLIC OF CYPRUS

Protection of Whistleblowers: Guide for Competent Authorities

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	5
C. Competent authorities	8
D. Establishment of external reporting channels	10
E. Establishment of procedures for receiving and following-up on external reports	12
1. Means for submitting reports and acknowledging receipt of reports	12
2. Follow-up on reports	13
2.1. Repetitive reports/breaches of minor importance/lack of competence ..	14
3. Obligation for electronic publication of information for the receipt and follow-up on external reports	15
4. Confidentiality of the identity of whistleblowers	16
5. Confidentiality of trade secrets	16
6. Processing of personal data	16
7. Record keeping of the reports	17
F. Obligation to take measures of protection and support for whistleblowers	19

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 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 called “competent authorities”, the Law creates an **obligation to establish external mechanisms (channels) for the submission of reports and measures to follow-up on the progress of such external reports**. This Guide is addressed to those public bodies which fall within the definition of “competent authorities” and elaborates on their obligations relating to the establishment of external reporting channels and follow-up procedures.

B. Protection of whistleblowers

1. Persons protected by the Law

The Law aims to protect “whistleblowers” (or “reporting persons”, as referred to in the Law). That is, it protects persons who submit “reports” or make “public disclosures” 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 point 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 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 offence (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 areas of financial services, products, markets, and prevention of money laundering and terrorist financing, transport safety, 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.

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.

In relation to the obligation of legal entities of the public and private sector to establish internal reporting channels, see “Protection of Whistleblowers: Guide for Employers”.

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.

3.3. Public disclosure

In addition to internal and external 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 the public disclosure, the whistleblower must have submitted either an internal or external report, but no action has been taken within 3 months from 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.

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; and
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. Competent authorities

“Competent authorities” with an obligation of establishing external reporting channels are those national authorities (e.g. services, authorities, bodies, ministries, deputy ministries, councils, commissioners, etc.) which, based on EU or national law, already receive complaints in the context of exercising their competences, or which are designated to receive and follow-up on reports for breaches falling within the scope of application of the Law.

The Law does not define a sole competent authority for receiving external reports, since the Law covers a wide range of areas of EU and national law for which a person may submit reports (public procurement, product safety and compliance, protection of the environment, public health, consumer protection, protection of privacy and personal data, criminal offences, corruption offences, etc.) (see articles 4 and 31 of the Law and the relevant annex therein).

Therefore, existing entities that already receive complaints, information or have the responsibility to supervise and/or investigate breaches regarding acts covered by the Law, are considered as “competent authorities”.

For instance, if the report relates to:

- corruption offences, the competent authority may be the Police, or the Office of the Attorney-General, or the Independent Authority against Corruption, as they have competence to receive complaints in relation to corruption offences,
- personal data breaches, the competent authority may be the Commissioner for Personal Data Protection.

In addition to these, the Council of Ministers has the power to designate additional competent authorities. In particular, in the absence of an authority responsible for receiving reports for certain types of breaches that fall within the scope of the Law, the Council of Ministers can issue decrees designating national authorities as competent authorities for the purposes of receiving and following-up on specific types of reports.

For the public's convenience in submitting external reports, the Ministry of Justice and Public Order maintains a list of all competent authorities on its website.

D. Establishment of external reporting channels

The Law provides that competent authorities must establish external reporting channels for the receipt of and follow-up on “external reports”, i.e. reports submitted by whistleblowers to authorities outside their workplace.

Persons or agencies or departments within the national authorities explained in section C may be designated as competent to receive external reports. The person, agency or department to be appointed depends on the structure of the competent authority.

The competent authorities must establish independent and autonomous external reporting channels, for receiving and handling reports in full confidentiality. According to the Law, an external channel shall be considered independent and autonomous, when:

- (a) it is operated in a manner that ensures the integrity and confidentiality of the information received; and
- (b) prohibits access thereto by non-authorised staff members of the competent authority.

At the same time, arrangements must be made internally so that even if a report is received by a non-authorized person, that person will immediately forward the report to the appropriate persons and will not disclose any information or the identity of the whistleblower and the person concerned under any circumstances.

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.

Staff members of the competent authorities designated as responsible for handling reports shall receive specialized training for the purposes of handling reports, and in particular for:

- (a) providing information on the procedures for reporting;

(b) receiving and following up on reports;

(c) maintaining contact with the whistleblower for the purpose of providing feedback and requesting further information where necessary.

It should be noted that all legal entities of the public sector that are “competent authority”, pursuant to the provisions of the Law, must establish channels and procedures for the receipt of and follow-up on internal reports, as well as for the receipt of and follow-up on external reports. That is, they should function as **recipients of internal reports**, i.e. reports from their employees regarding potential breaches at an internal level, but also as **recipients of external reports**, i.e. reports from persons employed at a different organization regarding potential breaches within their workplace.

The Law, however, does not preclude the possibility of internal and external channels being common. Each competent authority shall determine whether internal and external report will be received by the same person(s)/department.

E. Establishment of procedures for receiving and following-up on external reports

Competent authorities, in addition to designating external reporting channels, must also design and establish specific procedures on how they will receive and manage the information communicated to them through external reporting. In fact, the Law provides that competent authorities must review the established procedures at least once every three (3) years and, taking account their experience as well as that of other competent authorities, adapt them accordingly.

The competent authorities are under an obligation to inform the Ministry of Justice and Public Order within the first month of each year of the number of external reports they received during the previous year.

Although the Law does not provide for the creation of a specific procedure for submitting, receiving and following-up on external reports, it sets some minimum requirements that must be met.

1. Means for submitting reports and acknowledging receipt of reports

The external reporting channels shall enable reporting in writing or orally, or both. In any case, the competent authorities shall ensure that the designed procedures enable the durable storage of information so as to allow further investigations to be carried out (see section E.7).

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 E.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, unless the whistleblower explicitly requested otherwise or the competent authority reasonably believes that acknowledging receipt of the report would jeopardize the protection of the whistleblower's identity.

2. Follow-up on reports

After receiving external reports, the authorized staff members of the competent authority must diligently “follow-up” on the report, assessing the accuracy of the allegations and the possibility of taking measures to address the breach reported.

Examples of follow-up action:

- assessment of the accuracy of the allegations made in the report;
- investigation, prosecution or action for recovery of funds, or other appropriate remedial action;
- referral to another competent authority for further assessment;
- closure of the procedure based on lack of sufficient evidence;
- communication with the whistleblower requesting clarification of the information reported or provision of additional information.

The whistleblower must receive feedback on the action envisaged or taken as follow-up within a reasonable timeframe not exceeding three (3) months, or six (6) months in duly justified cases.

In the event of high inflows of reports, the Law provides that the competent authorities may examine reports of serious breaches or breaches of essential provisions falling within the scope of the Law as a matter of priority without prejudice to the above timeframe.

Upon completion of the investigation, the competent authorities must communicate to the whistleblower the final outcome of the investigations carried out on the basis of the report and in due course transmit the information contained in the report to the competent institutions, bodies, offices and agencies of the EU, as appropriate, for further investigation.

2.1. Repetitive reports/breaches of minor importance/lack of competence

In certain cases, and after having duly assessed the matter, the competent authority may decide:

- (a) that the reported breach is of minor importance and does not require further follow-up other than closure of the procedure,
- (b) to close procedures regarding repetitive reports which do not contain any meaningful new information on breaches compared to a past report in respect of which the relevant procedures were concluded, unless new legal or factual circumstances justify a different follow-up,
- (c) where the whistleblower reports to a channel which does not have the competence to address the breach reported, the said channel shall transmit the report to the competent authority, within reasonable time, in a secure manner, and the reporting person shall be informed, without delay, of such a transmission.

3. Obligation for electronic publication of information for the receipt and follow-up on external reports

Competent authorities must publish on their websites in a separate, easily identifiable and accessible section, the following information:

- (a) their contact details, in particular the electronic and postal addresses and phone numbers, as well as a statement regarding the recording or non-recording of phone conversations;
- (b) the procedures applicable to the reporting of breaches, including the manner in which the competent authority may request the whistleblower to clarify the information reported or to provide additional information, the timeframe for providing feedback and the type and content of such feedback;
- (c) the nature of the follow-up to be given to reports;
- (d) the confidentiality regime applicable to reports, and in particular the information in relation to the processing of personal data in accordance with the Law, and in accordance with the relevant EU directives and regulations (see article 14(d) of the Law),
- (e) the conditions for qualifying for protection under the Law as a whistleblower,
- (f) the remedies and procedures for protection against retaliation and the availability of confidential advice for persons contemplating reporting;
- (g) a statement clearly explaining the conditions under which whistleblowers reporting to the competent authority are protected from incurring liability for a breach of confidentiality pursuant to the Law; and
- (h) contact details of the information center established for the purpose of assisting whistleblowers.

4. Confidentiality of the identity of whistleblowers

The competent authorities must ensure the confidentiality of the identity of the whistleblower and of the person concerned or of any other information from which their identity may be directly or indirectly deduced. Disclosing any information about the identity of the whistleblower or of the person concerned to persons 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 competent authorities 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 competent authorities 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 of or follow-up on 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

Competent authorities are required to keep records of every report received, in compliance with the confidentiality requirements (see section E.4 and E.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 competent authorities 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 competent authorities 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 competent authorities 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 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 procedures), 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.

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

The Law provides for measures of protection for whistleblowers, such as the prohibition of retaliation (e.g. prohibition of suspension, lay-off, dismissal, demotion or withholding of promotion, etc.) and the protection in judicial proceedings (see “Protection of Whistleblowers: Guide for Employees”, section G). Moreover, the Law creates an obligation for the provision of support measures to whistleblowers by their employers (see “Protection of Whistleblowers: Guide for Employers”, section E).

Competent authorities 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 competent authorities shall prepare informative material in which the necessary information, advice and remedies available on protection are included.

The competent authorities must further offer effective assistance to whistleblowers before any relevant authority involved in their protection against retaliation. In the case of whistleblowers pursuing their rights by instituting legal proceedings, courts may order the waiver of retaliation, the re-employment of the whistleblower and may award compensation for the damage suffered by the whistleblower.

The competent authorities can assist the whistleblower in this process by providing evidence or other documents that may be requested of them, in order to confirm before the courts or other authorities that an external report was made and therefore that the employee may enjoy the protection offered by the Law.