Whistleblower

Reporting for unethical or unlawful behaviour

Policy

ICT Group Whistleblower's Regulation
Internal Policy
Version: 2.1

Table of contents

Document information

Reference	Description
Document	Whistleblower Policy
Authors	Legal
Reviewed by	QHSE, HR (NL, PT, SE), Legal BU
DocumentID	ICT Group Whistleblower's Regulation
Status	Approved
Date	01-01-2025
Classification	Public (R4)
Version	2.1

ICT Group B.V.
Kopenhagen 9
2993 LL Barendrecht
The Netherlands

info@ict.nl
+31 (0)88 908 2000

Forword

As ICT Group, we have the responsibility and intent to always act with integrity. We promote a culture of trust, respect and honest communication. These principles are applicable to everyone within ICT Group and are stipulated in our Code of Conduct. We are proud of our reputation and the people who work here. That's why we do not accept any violations of our Code of Conduct or any applicable legislation.
Therefore, ICT Group believes that it is important that our employees and third parties can make a report of (suspected) unethical or unlawful behaviour. To that purpose, these rules were created, in accordance with European Union law under the Whistleblower Protection.

Reading guide

This document is organized to provide clear and comprehensive guidelines applicable to everyone within ICT Group. The initial chapters consist of general rules and principles that must be adhered to by all members of ICT Group (indicated by the EU-flag).
After reviewing these general rules, readers should proceed to the appendices, located at the end of this document. The appendices contain country-specific provisions (indicated by their national flag) that are crucial for understanding the local application of these rules.

It is important to note that the country-specific provisions in the appendices take precedence over the general rules and text found in the initial chapters. Therefore, for complete compliance, please ensure that both the general rules and the country-specific provisions are thoroughly reviewed and understood.

1. Purpose

In this policy (hereafter "**Policy**") we, ICT Group, explain how concerns or issues can be reported, how reports of concerns and issues are handled and which rights and obligations apply to everyone involved. We encourage people to speak up when they have concerns or issues. The possibility to report directly to ICT Group is a key control in our decentralised organisation. We will ensure a fair and objective handling of the reports and the anonymity of the identity of anyone who files a report. As long as the filling of a report is in line with this Policy, we also guarantee that the person who reports will not face any retaliation or negative consequences only because that person filed a report.

2. Scope

This Policy is applicable to all persons of all companies who work within ICT Group, regardless of the legal basis of their working relationship, the function or position of the person, origin and place of residence. Third parties may also use this Policy to raise their concerns related to (suspected) breaches of the law or other serious issues of an ethical or moral nature (as further explained in this Policy).

All entities and business units within ICT Group must comply with this Policy.

This Policy is based on EU[1] legislation. Depending on the situation other (local) law can take precedence.

3. What can be reported?

We encourage any person and any third party to speak up when (potential or suspected) unlawful or unethical situations are encountered within or in connection with ICT Group.

This includes, for example, unlawful or unethical behaviour in relation to:

- Any of our principles as stipulated in our Code of Conduct;
- The public interest;
- Any ICT Group policy;
- Any applicable (European or local) law or regulation on;
    - Internal market, including but not limited to competition law;
    - Money laundering;
    - Public procurement;
    - Protection of environment;
    - Protection of privacy and personal data;
    - Product safety and compliance;

[1] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

- Terrorist activity, including but not limited to terrorist financing;
- Public health;
- The security of networks and information systems;
- Financial interest of the European union.

4. Who can report a (suspected) issue?

Any person who works within the ICT Group, regardless of the legal basis of their working relationship, the function or position of the person, origin and place of residence ("**Employee**"), *or* any third party can report an issue.

Anyone employee or third party who reports a (suspected) issue or concern in accordance with this Policy is a "**Reporter**".

A report can be filled anonymously (see chapter 8)

5. To whom can a (suspected) issue be reported?

An Employee can report a (suspected) issue or concern via one of the following '*channels'*:

1. At local level;
2. At group level;
3. At Human Resources;
4. To the confidential adviser.

An Employee must report in writing or report orally by telephone submit any (suspected) issue or concern (hereafter "**Report**").

A third party can report a (suspected) issue or concern via whistleblower@ict.nl.

Once a Report is received an internal audit team will be involved to investigate the report.
The Reporter shall receive an acknowledgement of receipt of the Report within seven (7) days.

The Reporting, Report and the Reporter's identity (if known) is always considered confidential. Anyone involved will not disclose the identity of the Reporter without the Reporters express permission.

5.1. At local level

A Employee may report a (suspected) issue or concern to their (direct) manager. The manager shall procure that the chairman of the executive board shall be informed immediately of the reported (suspected) issue or concern and of the date on which it was reported, and the manager shall procure that the chairman of the Executive Board receives a copy of the record.

5.2. At group level

A Employee may report a (suspected) issue or concern to the chairman of the supervisory board (‘*Raad van Commissarissen*’), in the event;

A. the (suspected) issue or concern involves or concerns, in any way, a member of the executive board; *or*
B. the reporting through the other ‘channels’ have not removed the (suspected) issue or concern within a reasonable period after reporting.

5.3. At Human Resources

A Employee may report a (suspected) issue or concern to (the local or group) Human Resources department.

5.4. To the confidential adviser

A Employee may report a (suspected) issue or concern to the confidential adviser. The confidential adviser shall procure that the chairman of the Executive Board shall be informed immediately of the reported (suspected) issue or concern and of the date on which it was reported, and the confidential adviser shall procure that the chairman of the executive board receives a copy of the record.

If a Employee chooses to report anonymously to the confidential adviser, the following procedure applies: the confidential adviser reports by e-mail the suspected irregularities internally to Human Resources, the confidential adviser shall receive an acknowledgement of receipt of the report within seven (7) days and will serve as the contact person for the anonymous Reporter.

6. Requirements on reporting

A Reporter shall always report with genuine concerns and with (motived) basis, due to the fact that false accusations can have significant impact on individuals and/or ICT Group. We expect, and therefor only protect, a Reporter who is reporting only in good faith. A Reporter is not protected in the event the Reporter willingly and consciously acted or participated in the reported breach of any of the topics stipulated in chapter 3 of this Policy.

After filling a Report, the Reporter shall keep the Report, information and/or the (suspected) issue or concern confidential. No information shall be provided to third parties, expect for competent authorities, in or outside ICT Group.

7. Investigation process

Once a Report has been filled an investigation will start. The chairman of the Executive Board decides the type of investigation.
These first steps will always, regardless of (the) Reporter, who or what is reported;

1. Verifying if the reported (suspected) issue or concern is likely to be legitimate and within the scope of this Policy.
2. Verifying if enough information is provided for an effective investigation. *and*

3. Verifying if the report is filled in correctly and in line with this Policy.

The Reporter shall receive an acknowledgement of receipt of the Report within seven (7) days.

Depending on the nature of the Report and the reported (suspected) issue or concern, an appropriate investigation team will be set up and the Report recorded in a register (equipped for this purpose). The investigation team will in principle be local, but the chairman of the Executive Board can decide to start a team on a group level. The register can only be accessed by authorized staff members and be kept in accordance with applicable laws and regulations, like GDPR, and shall be done primarily local.

The Reporting, Report and the Reporter's identity (if known) is always considered confidential. Anyone involved will not disclose the identity of the Reporter without the Reporters express permission.

Persons who are under investigation will only be notified after safeguarding relevant evidence and if such notification could not jeopardize the investigation.
The Reporter and the persons who are under investigation each have the right to be heard, by means of a physical meeting, during the investigation. They can also have a trusted person present at the hearing unless that person is directly involved or is under the investigation.

Within eight (8) weeks from filling the Report, a Reporter shall be informed in writing, of ICT Group's position with regard to the filled (suspected) issue or concern. If no position can be given within eight (8) weeks, a follow-up report will be started by ICT Group. The follow-up report shall be presented to the Reporter within three (3) months after notification. The follow-up report shall stipulate the results of the investigation (including a verdict about the (suspected issue or concern)) and/or any follow-up actions ICT Group is going to take.

8. Reporting anonymous

A report can be filled anonymously.

Filing an anonymous report is possible by leaving out your name in the online internal reporting form or via contacting the confidential advisor (see chapter 5.4. of this Policy)

9. Protection against retaliation

A Reporter shall not experience negative consequences for filing a Report in accordance with this Policy. When ICT Group believes on reasonable grounds that the Reporter acted in good faith, ICT Group shall make every reasonable effort to protect the Reporter from any negative retaliation.

If the Reporter believes they are being subject to a retaliation, the Reporter can contact the (local) Human Resource manager, Legal department, or fill another report in accordance with this Policy. ICT Group will take action against its employees who are engaged in unlawful, or not in compliance with this Policy, retaliation actions against the Reporter.

This applies to both internal and external reporting.

10. Alternatives to internal reporting

An Employee or thirty party may opt to directly report externally to a competent authority. External reporting means, the reporting not directly to ICT Group. ICT Group encourages internal reporting over external reporting.

The Reporting, Report and the Reporter's identity (if known) is always considered confidential. Anyone involved will not disclose the identity of the Reporter without the Reporters express permission.

11. Changes to the Whistleblower Policy

ICT Group reserves the right to amend this Policy at any time without prior notice. The most recent version of this Whistleblower Policy will always be published on the website and her b internal network (intranet). ICT Group will always communicate any changes or updates to this Policy to her employees via the intranet

ADDENDUM 1

Cluster Bulgaria

With the differences in the local legislation, in that regard the Bulgarian Act on Protection of Persons [2], reporting information, or publicly disclosing information about breaches and the guidelines issued by the responsible authority, we have to establish the specifics applicable for the companies registered in Bulgaria. Strypes EOO Dand Kodar EOOD, as part of ICT group, are fully committed to the ICT Group values and principles, but at the same time shall abide by the local legislation and authority requirements.
This Policy shall fully apply to the established in Bulgaria companies, part of ICT Group, whereas the differences under the local legislation described hereinafter.

I. Strypes EOOD

Differences:

5. To whom can a (suspected) issue be reported?

An Employee can report a (suspected) issue or concern via one of the following '*channels*':

1. To the Direct Manager
2. To the Confidential adviser.

Employees shall report in writing or report by telephone/ personal meeting suspected irregularities internally to the Confidential advisors at Strypes (HR Manager, IT Manager and/ or Finance Manager). They may as well contact their Direct manager and report an issue.

A third party can report a (suspected) issue or concern via WB@strypes.eu.
The written information shall be submitted by the sender by filling in an official form. Based on the nature of the report, the respective Confidential adviser will continue the communication.

5.1. To the Direct Manager

A Reporter may report a suspected issue or concern to the Direct Manager. The Direct Manager is authorized to receive the report, but afterwards obligated to inform one of the Confidential advisers, who will take over the further communication with the Reporter.

[2] Act on Protection of Persons, Reporting Information, or Publicly Disclosing Information about Breaches (Whistleblowers Protection Act)(20 Oct 2023)

5.2. To the Confidential adviser

A Reporter may report a suspected issue or concern to one of the Confidential advisors. The report (written or verbal) shall be documented by the confidential adviser by filling in the official form. The Reporter has the right to decline signing the Report with a handwritten signature.

7. Investigation process

Depending on the nature of the Report and the reported (suspected) issue or concern, an appropriate investigation team(involving respective specialists) will be set up by the lead Confidential adviser and the Report recorded in a register (equipped for this purpose). The register can only be accessed by authorized staff members and be kept in accordance with applicable laws and regulations, like GDPR.

Persons who are under investigation shall be notified and receive all the collected evidence against them. The persons against whom the report was filled have the right to be heard or to provide their written explanations and collect and evaluate the evidence (themselves). They have the right to object to the collected evidence and report within seven (7) days. The affected person may collect and provide additional evidence in the course of the investigation.

Within eight (8) weeks from filling the Report, a Reporter shall be informed in writing, of Company's position with regard to the filled (suspected) issue or concern. If no position can be given within eight (8) weeks, a follow-up report will be started. The follow-up report shall be presented to the Reporter not longer than three (3) months after the receipt of the initial report confirmation.

8. Reporting anonymous

Under the terms and conditions of the Bulgarian Act anonymous reports **shall not be processed**. Incidents related to suspected violations committed more than two (2) years before reporting shall not be processed either.

II. Kodar EOOD

This Policy applies for Kodar EOOD together with the aforementioned specifics for Strypes EOOD. Under the Bulgarian legislation obligated subjects with more than 250 employees are not allowed to share resources for reporting of suspected issues, therefore Kodar EOOD established separate internal channels for reporting.

Differences:

5. To whom can a (suspected) issue be reported?

An Employee can report a (suspected) issue or concern via one of the following '*channels*':

1. To the Direct Manager
2. To the Confidential adviser.

Employees shall report in writing, by telephone or via personal meeting suspected irregularities internally to the Confidential advisor at Kodar - the Group Manager Ivaylo Ganev. They may as well contact their Direct Manager and report an (suspected) issue or concern.

A third party can report a (suspected) issue or concern, regarding Kodar or any Employee of Kodar, via wb@kodar.net
The written information shall be submitted by the sender by filling in an official form.

ADDENDUM 2

Cluster Sweden

Attitude AB and ICT Sweden AB, as part of ICT Group, are fully committed to the ICT Group values and principles.
This Policy shall fully apply to the established in Swedish companies, part of ICT Group, whereas the differences in local process described hereinafter.

Differences:

5. To whom can a (suspected) issue be reported

An Employee can report a (suspected) issue or concern via one of the following '*channels*':

1. To the Direct Manager
2. To HR

7. Investigation process

Depending on the nature of the Report and the reported (suspected) issue or concern, an appropriate investigation team(involving respective specialists) will be set up by t two independent people (one from MT) and one from the TA/HR department. They will get back to you with questions, clarifications, or information within three (3) months.

The register can only be accessed by authorized staff members and be kept in accordance with applicable laws and regulations, like GDPR. The whistleblowing functionality in the external HRM software Hailey HR is being used.

Persons who are under investigation shall be notified and receive all the collected evidence against them. The persons against whom the report was filled have the right to be heard or to provide their written explanations and collect and evaluate the evidence (themselves). They have the right to object to the collected evidence and report within seven (7) days. The affected person may collect and provide additional evidence in the course of the investigation.

ADDENDUM 3

Cluster Portugal

With the differences in the local legislation, in that regard Law no. 93/2021, of 20 December 2021, STRYPES TECHNICAL SOFTWARE, UNIPESSOAL LDA ("Strypes Portugal" or "Company"), as part of ICT group, is fully committed to the ICT Group values and principles, but at the same time shall abide by the local legislation and authority requirements.
This Policy shall fully apply to the Strypes Portugal, as part of ICT Group, with the observance of the differences under the local legislation described hereinafter.

Differences:

3. What can be reported?

Apart from the situations identified in the Policy, the following situation can be reported:

(i) An act or omission contrary to and detrimental to the financial interests of the European Union referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU), as specified in the applicable European Union measures;

(ii) The act or omission contrary to the internal market rules referred to in Article 26(2) of the TFEU, including competition and state aid rules, as well as corporate tax rules;

(iii) Violent, especially violent and highly organised crime, as well as the crimes provided for in Article 1(1) of Law no. 5/2002, of January 11, which establishes measures to combat organised and economic-financial crime.

(iv) Violent crime, under the terms of article 1 j) of the Portuguese Code of Criminal Procedure: conduct that is intentionally directed against life, physical integrity, personal freedom, sexual freedom and self-determination or public authority and is punishable by a maximum prison sentence of five (5) years or more.

(v) Particularly violent crime, under the terms of Article 1(l) of the Portuguese Code of Criminal Procedure: conduct that is intentionally directed against life, physical integrity, personal freedom, sexual freedom and self-determination or public authority and is punishable by a maximum prison sentence of eight (8) years or more.

(vi) Highly organised crime, under the terms of article 1 l) of the Portuguese Code of Criminal Procedure: conduct that includes crimes of criminal association, trafficking in human organs, trafficking in persons, trafficking in arms, trafficking in narcotics or psychotropic substances, corruption, influence peddling, economic participation in business or money laundering.

(vii) Crimes provided for in Article 1(1) of Law no. 5/2002, of 11 January:

a. Drug trafficking;
b. Terrorism, terrorist organisations, international terrorism and terrorist financing;
c. Arms trafficking;
d. Influence peddling;
e. Undue receipt of an advantage;
f. Active and passive corruption, including that practised in the public and private sectors and in international trade;

g. Appropriation or misappropriation of property, for their own benefit or that of a third party, by a public official;
h. Economic participation in business;
i. Money laundering;
j. Criminal association;
k. Child pornography and pimping of minors;
l. Damage to computer programmes or other data and computer sabotage, as well as illegitimate access to a computer system;
m. Human trafficking;
n. Counterfeiting, use and acquisition of counterfeit cards or other payment devices and their preparatory acts, acquisition of cards or other payment devices obtained through computer crime, damage to computer programmes or other data and computer sabotage, as well as illegitimate access to a computer system;
o. Racketeering;
p. Smuggling;
q. Trafficking in and addiction to stolen vehicles.

(viii) The act or omission that contradicts the purpose of the rules or standards covered by paragraphs above.

(ix) In the areas of national defence and security, only an act or omission that is contrary to the procurement rules contained in the European Union acts referred to in Directive (EU) 2019/1937 of the European Parliament and of the Council or that is contrary to the purposes of these rules, shall be considered an offence for the purposes of this Policy.

6. Requirements on reporting

The Report channels should not be used to make false accusations or to resolve everyday disputes with superiors, colleagues, or third parties. Reports, complaints or concerns about personal circumstances should be submitted through Human Resources procedures.
The Reporter cannot be held disciplinarily, civilly, administratively, or criminally liable for reporting or publicly disclosing an infringement in accordance with the Policy.
The Reporter cannot be held responsible for obtaining or accessing the information that motivates the report or public disclosure, except if the obtaining or access constitutes a crime.

7. Investigation process

At any time, the Reporter may request that the result of the analysis carried out on the Report be communicated to him/her within fifteen (15) days of the conclusion of this analysis.

The identity of the Reporter, the targeted person, and any other individuals mentioned in the Report, as well as the information that may allow their identification, are of a confidential nature and have restricted access to those responsible for receiving and/or following up on the complaints made.

Information related to the identity of the aforementioned individuals may only be disclosed as a result of a legal obligation or judicial decision and must be preceded by written communication to the individuals whose identity is subject to disclosure, with an explanation of the reasons for the same, except if providing this information would compromise the underlying investigations or legal proceedings.

The obligation of confidentiality applies to all individuals who have received information about the Report.

9. Protection against retaliation

The Reporter, the Reporter's assistant and legal persons or similar entities that are owned or controlled by the Reporter, for which the Reporter works or with which the Reporter is in any way connected in a professional context, may not be subjected to retaliation acts.

The following acts, when carried out up to two (2) years after a complaint or public disclosure, are presumed to be motivated by that same complaint, until proven otherwise:

(i) Dismissal;
(ii) Changes to working conditions, such as duties, working hours, place of work or remuneration, failure to promote the Employee or failure to comply with employment duties;
(iii) Suspension of the employment contract;
(iv) Negative performance evaluation or negative reference for employment purposes;
(v) Failure to convert a fixed-term employment contract into an open-ended contract, whenever the Employee had legitimate expectations of such conversion;
(vi) Non-renewal of a fixed-term employment contract;
(vii) Inclusion on a list, based on a sector-wide agreement, which could lead to the complainant being unable to find employment in the sector or industry concerned in the future; and/or
(viii) Termination of a supply or service contract.

Any disciplinary sanction applied to the Reporter or the Reporter's assistant will be presumed abusive for up to two (2) years after the Report or public disclosure.

The ICT Group will ensure that colleagues who make a Report or who provide information to support the investigation of that Report will not suffer adverse employment consequences for providing that information.
The ICT Group take all reports of such retaliation seriously and will investigate them immediately, using personnel who are independent of the Employees who are alleged to have retaliated.
A colleague who retaliates as described in this Policy is subject to disciplinary action, which may include termination of employment.
If the Reporter reports a matter in which he/she may have committed a breach, that Report will not eliminate the possibility of internal disciplinary proceedings against the Reporter in relation to that breach, although the Company will take into account the fact that the Employee raised the matter voluntarily in any measures that may be adopted.

10. Alternatives to internal reporting

10.1. Precedence of Internal Complaints

Since there are internal channels in the Company, as a rule, the Reporter will not enjoy the protection conferred by the law when the Reporter resorts to external whistleblowing channels to report infractions, without first using the internal channels, except in the cases strictly provided for in the applicable legislation.

10.2. Prohibition on Disclosure of the Infringement

As a rule, the Reporter may not publicly disclose a breach or make it known to the media or a journalist and does not benefit from the protection afforded by the Policy, except in the cases provided for by law.

12. Data protection

12.1. Document conservation

Reports submitted under the Policy are subject to registration and retention for a minimum period of five (5) years and, regardless of this period, during the pendency of judicial or administrative proceedings relating to the complaint in question.

12.2. Data processing

The purpose of processing the information communicated under this Policy is to receive and follow up on Reports submitted.

Personal data that is clearly not relevant to the processing of the Report will not be kept and will be deleted immediately. In particular, special categories of personal data (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data to unequivocally identify a person, data relating to health or data relating to a person's sex life or sexual orientation) included in reports will be deleted.

The Company, as data controller, will ensure that the data subject has the right to access, rectify, erase and limit the processing of their personal data, as well as the right to request data portability and to object to processing, provided that the legal conditions are met.

Under the terms of the legislation applicable to the protection of personal data (including the General Data Protection Regulation and Law no. 58/2019), the Company implements the appropriate security measures to protect the information and data contained in internal reports and the corresponding records.

Before submitting a Report, the Reporter must read and declare that the Reporter has understood and accept the conditions set out in the privacy policy in force.

ADDENDUM 4

Cluster The Netherlands

With the differences in the local legislation, in that regard the Dutch Act on Protection of Persons [3], reporting information, or publicly disclosing information about breaches and the guidelines issued by the responsible authority, we have to establish the specifics applicable for the companies registered in the Netherlands. ICT Netherlands B.V., ICT Netherlands Holding B.V., ICT Group B.V., Incore Software B.V., TriOpSys B.V., INNOCY B.V.ICT Healthcare Technology Solutions B.V., as part of ICT group, are fully committed to the ICT Group values and principles, but at the same time shall abide by the local legislation and authority requirements.
This Policy shall fully apply to the established in Dutch companies, part of ICT Group, whereas the differences under the local legislation described hereinafter.

Differences:

3. What can be reported?

Instead of situations identified in the Policy, the following situation can be reported (suspected) 'abuse, in accordance with the Dutch law[4];
'*Abuse'* means;
(i) A breach or risk of a breach of Union law, *or*
(ii) An act or omission with regard to which the public interest is at stake in connection with:
   a. A breach or risk of a breach of a statutory regulation or of internal rules that impose a specific obligation and have been established by an employer on the basis of a statutory regulation; *or*
   b. A risk to public health, public safety or the environment, or an improper act or omission that jeopardises the proper functioning of the public services or an undertaking. A public interest is in any event at stake if the act or omission affects more than just personal interests and is either part of a pattern or structural in nature, or is serious or broad in scope;

5. To whom can a (suspected) issue be reported?

Additional to chapter 5;
An Employee can report any (suspected) abuse (hereafter "**Report**") via;
(i) In writing;
(ii) Orally by telephone or other audio messaging system; *or*

[3] Act on Protection of Persons, Reporting Information, or Publicly Disclosing Information about Breaches (Whistleblowers Protection Act)(20 Oct 2023)
[4] Act on Protection of Persons, Reporting Information, or Publicly Disclosing Information about Breaches (Whistleblowers Protection Act)(20 Oct 2023)

(iii) Upon request within a reasonable period in a face-to-face conversation at a location;

If a Report is made using a telephone line or other audio messaging system, or if a Reporter makes a Report in a face-to-face conversation at an agreed location, ICT Group shall register the Report by:

a. Recording the conversation in a permanent and retrievable form, *or*
b. Drafting a complete and accurate written account of the conversation.

For recording on the conversation prior consent of the Reporter is required.
When drafting a account of the conversation, the Reporter will be giving the opportunity to check and correct the report. An drafted account of the conversation will always require a signature of the Reporter.

9. Protection against retaliation

Additional to chapter 9;

The position of the Reporter who reported a suspected irregularity in accordance with these rules shall not be affected in any way as a result of the Report. If it should become clear that the Reporting has not been used in good faith (for example, in case of a personal grudge against another Employee), this will constitute misconduct. This protection also applies to natural and legal persons assisting the Employee as well as family members and colleagues who have a working relationship with the reporter. Furthermore, the protection applies to internal investigators, i.e. those who follow up on an internal report and receive an internal report.

All forms of retaliation are prohibited. The threat of or an attempt to retaliation is also prohibited. More specifically, the following are prohibited:

- dismissal or suspension
- a fine as referred to in article 650 of Book 7 of the Civil Code;
- demotion;
- withholding promotion;
- a negative assessment;
- a written reprimand;
- transfer to another location;
- discrimination;
- intimidation, bullying or exclusion;
- defamation;
- early termination of a contract for the provision of goods or services; and
- revocation of a permit.

10. Alternatives to internal reporting

Additional to chapter 10;

Employees and third parties are also able to report directly externally to the Dutch Whistleblowers Authority or another competent authority. The following authorities that are responsible for

receiving and following up on reports, in so far as they are competent in accordance with Dutch law[5], are:
(1°) the Netherlands Authority for Consumers and Markets;
(2°) the Dutch Authority for the Financial Markets;
(3°) the Data Protection Authority;
(4°) De Nederlandsche Bank N.V.;
(5°) the Authority;
(6°) the Health and Youth Care Inspectorate;
(7°) the Dutch Healthcare Authority;
(8°) the Authority for Nuclear Safety and Radiation Protection; and
(9°) organisations and administrative authorities, or units thereof, designated by an order in council or a ministerial order which have tasks or powers in one of the areas referred to in Article 2, paragraph 1 of the directive[6].

Employees and third parties are not obligated to report internally first, but this remains the preference and will be encouraged as much as possible.

12. Whistleblower subsidy scheme

As of February 1, 2024, the Legal Aid Council ('Raad voor Rechtbijstand') has implemented a Whistleblower Subsidy Scheme. The scheme enables free legal assistance and/or mediation for whistleblowers. This also applies to involved third parties and people assisting a whistleblower.

[5] Act on Protection of Persons, Reporting Information, or Publicly Disclosing Information about Breaches (Whistleblowers Protection Act)(20 Oct 2023)
[6] Act on Protection of Persons, Reporting Information, or Publicly Disclosing Information about Breaches (Whistleblowers Protection Act)(20 Oct 2023)

Disclaimer

ICT GROUP
Creating a smarter world

ICT Group B.V.
Kopenhagen 9
2993 LL Barendrecht
The Netherlands

P +31 (0)88 908 2000
E info@ict.eu
W www.ict.eu