WHISTLEBLOWING PROCEDURE

APPROVED BY THE BOARD OF DIRECTORS

ON 19/12/2019
UPDATE of 20/10/2020

Contents

1.	INTRODUCTION	3
2.	RECIPIENTS	3
3.	SCOPE	3
4.	REFERENCES	4
5.	DESCRIPTION OF THE PROCESS AND RESPONSIBILITIES	4
5.1	Scope and brief description of the process	4
5.2	Process activities	5
5.2.1	Sending whistleblowing	5
5.2.2	Registration and classification	6
5.2.3	Preliminary analysis of the whistleblowing	7
5.2.4	Specific investigations	7
5.2.5	Notification of results	8
5.2.6	Retaining documentation	8
5.2.7	Periodic controls	8
6.	ATTACHMENTS	9

1. INTRODUCTION

The term “whistleblowing” means any reporting of a conduct, including omissions, which does not conform to laws and regulations, applicable in any case to INWIT, and to the system of rules and procedures in effect within the company, which include the Code of Ethics and Conduct and the 231 Organisational Model.

Whistleblowing also includes complaints and objections received by the Board of Statutory Auditors.

Article 4 of the Code of Ethics and Conduct establishes the guidelines for requesting clarifications or reporting information concerning alleged violations of this Code.

The whistleblower reporting information in good faith (see section 5.2) is protected according to the terms and procedures herein, as well as the person the whistleblowing refers to, if - following analyses - there are no grounds for the whistleblowing, which was only undertaken to harm the person in question or due to the serious indiscretion, negligence or inexperience of the whistleblower (wilful misconduct or gross negligence).

In this regard, whistleblowing comes under the scope of legislation, and specifically Legislative Decree 231/01 on the administrative liability of entities (Law no. 179 of 30 November 2017 "Provisions to protect whistleblowers of crimes or irregularities that come to their knowledge during public or private employment”).
In particular, legal provisions apply to entities that have adopted a Compliance Programme and refer to specific reporting of unlawful conduct which is significant pursuant to the above Decree or violations of the Compliance Programme.
Legislation prohibits, among others, direct or indirect acts of retaliation or discrimination against the whistleblower, as an employee of the entity, for reasons related directly or indirectly to the whistleblowing.

2. RECIPIENTS

This procedure applies to:

- senior company management and members of corporate boards of INWIT;
- all INWIT employees, partners, customers, suppliers, consultants, external staff, shareholders and, more in general, any Third Party with information concerning the conduct indicated in the Introduction.

3. SCOPE

This Procedure regulates the process of receiving, analysing and processing (including filing and deletion as indicated in paragraph 5.2 below), whistleblowing, sent or transmitted by anyone, even anonymously.

Whistleblowing may, in particular, concern:

1. requests for clarification on the integrity of own or others' conduct, for the purposes of complying in full with the Code of Ethics and Conduct;
2. notices of alleged violations, requests or inducement to violate laws or regulations, provisions of the Code of Ethics, of internal procedures (e.g.: failure to observe contract clauses, slander, threats, fraud, improper use of company equipment);

3. notices of alleged violations of the 231 Organisational Model following a conduct at risk of the offences and/or unlawful activities indicated in the 231 Organisational Model being committed;
4. declarations concerning alleged findings, irregularities or reprehensible actions;
5. complaints concerning accounting, internal accounting control or auditing matters, from any party, as well as concerns reported by employees of the Company concerning questionable accounting or auditing matters.

For the matters listed below, which may be reported in whistleblowing, the following specialist channels are provided; these channels are used in the case of facts identified attributable to significant circumstances pursuant to the Organisational Model, or other cases as indicated above (points 1 - 5), for the ordinary management of the matters:

- conflicts of interest of personnel,
- security incidents concerning human resources, material and immaterial resources (such as software malfunctions, company network failures, the loss or accidental destruction of documents, ICT security incidents, theft);
- requests for information and whistleblowing concerning business travel abroad;
- conduct or events attributable to the misuse of network services, such as spam, the dissemination of viruses and malware, cyber attacks, phishing, identity theft, the publication or dissemination of offensive or subversive material (online abuse).

Whistleblowing in these categories, sent via the channels established according to this Procedure, will be forwarded to competent Functions by the Audit Function, that will monitor outcomes to identify any weaknesses in the internal control and risk management system. This whistleblowing is included in the periodic reporting indicated in section 5.2. below.

4. REFERENCES

- Regulation 2016/679/EU (General Data Protection Regulation - GDPR)
- Law no. 179 of 30 November 2017 "Provisions to protect whistleblowers of crimes or irregularities that come to their knowledge during public or private employment"
- INWIT Compliance Programme (including the Code of Ethics and Conduct)
- Anti-Corruption Policy
- Conflict of Interest Management Procedure.

5. DESCRIPTION OF THE PROCESS AND RESPONSIBILITIES

5.1 Scope and brief description of the process

The owner of the process to manage whistleblowing is INWIT's Supervisory Board, which relies on the Head of the Audit Function for the management of whistleblowing.

The process, with the activities described in the paragraphs below, is overseen by the Audit Function in full compliance with principles of International Standards for the internal audit profession and the Code of Ethics issued by the Institute of Internal Auditors (IIA), as well as the Code of Ethics and Conduct of the company.

If the whistleblowing concerns a member of the Supervisory Board, the preliminary investigation and consequent analyses will be managed by the other members of the same Supervisory Board.

If the entire Supervisory Board or the majority of its members (3 out of 4) are involved, the preliminary investigation will be handled by the Chairmen of the Board of Directors and the Board of Statutory Auditors.

5.2 Process activities

5.2.1 Sending whistleblowing

Description of the activity

The employees of INWIT, partners, customers, suppliers, consultants, external staff, shareholders and, more in general, any third party, that acquire knowledge of a conduct described in section 3, are required to report it as indicated in this section. Employees who receive whistleblowing from other subjects (e.g. employees/third parties), must send it to the Audit Function immediately, according to the procedures indicated below, along with all supporting documentation received, without keeping a copy and without taking any independent action to analyse and/or further investigate the matter. Failure to notify whistleblowing received is a violation of this Procedure (and of the Code of Ethics and Conduct), that may result in sanctions being imposed by Human Resources Function based on the disciplinary system in effect (see Articles 46, 47 and 48 of the National Collective Bargaining Agreement for the Telecommunications industry in effect for non-executive personnel and suitable measures consistent with regulations applicable to executive personnel).

INWIT has adopted an IT solution to receive, manage and file whistleblowing, in order to guarantee full compliance with legal requirements (in particular with Law 179/17), which is available both on the intranet and Internet.

Whistleblowers can submit their concerns via a web portal to the following address, which can also be found on the company's website (www.inwit.it):

https://inwit.segnalazioni.net/

The portal can be accessed by all members of the Supervisory Board with automatic notification mechanisms if any whistleblowing is received or archived.

Whistleblowing reports may also be sent

- in writing to the attention of the 231 Supervisory Board or the Company's Head of Audit to the address:
  Infrastrutture Wireless Italiane S.p.A., Via Gaetano Negri 1 - 20123 Milano.

For specific matters dealt with by the Board of Statutory Auditors (complaints and objections pursuant to art. 2408 of the Italian Civil Code), the following procedures also are possible:

- in writing, addressed to the attention of the Board of Statutory Auditors to:
  Infrastrutture Wireless Italiane S.p.A., Via Gaetano Negri, 1 - 20123 Milano
- by email, at:
  inwit.cs@inwit.it.

If whistleblowing on matters dealt with by the Board of Statutory Auditors of INWIT is sent directly to the SB or the Audit Function, said Function will notify the receipt, ensuring immediate transmission to the Board of Statutory Auditors.

For whistleblowing relative to compliance matters, after assessment by the Supervisory Body, the Audit Function will notify the Compliance & Data Protection Function to manage aspects in its responsibility.

Whistleblowing from anyone, which is either verbal (relayed in person or by telephone), or in writing (by external or internal post, email, fax), must be promptly forwarded by the receiving party, using the IT solution. Whistleblowing which is verbal shall be stated in writing by the receiving party, giving all possible, useful details.

In the case of whistleblowing received by post, the letter and relative envelope shall be attached to the reported information. The original shall be sent immediately to the Audit Function, which will keep it in a protected environment.
The whistleblowing management system guarantees the confidentiality of whistleblowing during all stages (including information on any persons referred to), and the identity of the whistleblower, also using encrypted information, apart from cases where:

- the whistleblowing is unfounded and has been undertaken, with wilful misconduct or gross negligence, solely for the purpose of harming the person referred to and/or third parties in general;
- anonymity cannot be opposed by law (e.g. criminal investigations, inspections of control bodies, etc.);
- the whistleblowing identifies facts which, although external to the company, require reporting to the judicial authorities (e.g. terrorism, spying, attacks, etc.).

Violations of the non-disclosure obligation (apart from the exceptions above), are subject to disciplinary action.

It is forbidden to carry out direct or indirect acts of retaliation or discrimination against whistleblowers reporting information pursuant to this Procedure, for reasons related directly or indirectly to the whistleblowing.
The above does not apply if the whistleblowing is from employees and concerns unlawful conduct which is significant for the purposes of the Decree 231 or violations of the Compliance Programme, which may be reported to the National Directorate of Labour.
If an employee believes there has been retaliation or discrimination against him/her due to the forwarding of whistleblowing, s/he may promptly notify the Audit Function via the channels referred to in this procedure. This Function, together with the Human Resources function, will coordinate joint analysis to start disciplinary proceedings, if applicable, against the person who retaliates or acts in a discriminatory way.

For consequences related to the adoption of any direct or indirect retaliation and/or discrimination against the whistleblower/employee for reasons related, even indirectly, to the whistleblowing and regulations governing sanctions that may be imposed on persons violating measures to protect the whistleblower or on whistleblowers who, with wilful misconduct or gross negligence, report information that is unfounded, reference is made to the Compliance Programme.

5.2.2 Registration and classification

Description of the activity

All whistleblowing, regardless of how it is received/reported, will be registered on the platform, that will be the database summarising essential data on the whistleblowing and its management (traced through a workflow), also ensuring the filing of all documentation attached.
A univocal identifier will be assigned for each whistleblowing case, enabling each whistleblower to check the case progress, anonymously.
If sufficient information is not provided in the whistleblowing, the Audit Function may request the whistleblower to provide further details, according to the procedures indicated below:

- if the whistleblower has provided a contact (email, telephone, etc.), through this contact;
- if no contact is provided, through the management and messaging mechanism, using the identifier of the whistleblower.

5.2.3 Preliminary analysis of the whistleblowing
Description of the activity

All whistleblowing is subject to a preliminary analysis by the Supervisory Board in order to assess the relevance and/or responsibility for the topic at issue and to assess - if necessary - whether the Board of Statutory Auditors should be promptly informed.

Following the aforementioned analysis, to be carried out shortly after receipt of each whistleblowing, the Audit Function carries out a preliminary check to assess whether the facts reported are well-founded.

In carrying out this activity, and in particular, in analysing specific aspects processed in whistleblowing, the Audit Function may be assisted by competent Functions.

If, on completion of preliminary analysis, there are not enough details or the reported facts are unfounded, the SB will file the whistleblowing along with the relative reasons.

Apart from particularly serious cases, such as those involving the safety and also the personal integrity of the whistleblower, anonymous whistleblowing is not considered to be consistent with a fair and transparent management of interpersonal and company relations.

5.2.4 Specific investigations
Description of the activity

If the preliminary analysis identifies grounds for the whistleblowing, the Audit Function will continue the investigation on behalf of the SB. The Audit Function:

a) carries out necessary analysis of the facts reported, also through standard audit activities, with analyses being extended to the process which the reported facts refer to;

b) involves, where appropriate and guaranteeing the confidentiality and protection of those involved, the Company functions involved in the whistleblowing and the Legal & Corporate Affairs Function for any assessments on analysis procedures, pursuant to privacy legislation;

c) is assisted, as necessary, by external experts or assessors;

d) ends the investigation at any time if the whistleblowing is proved to be unfounded, without prejudice to the procedure in letter h) below;

e) interviews the person indicated in the whistleblowing, if considered appropriate by the Audit Function, as regards the outcomes of preliminary assessments, always bearing in mind that the whistleblower must remain anonymous;

f) takes specific action, if considered necessary, to safeguard the whistleblower, through formal notification to the HR Function;

g) after analysis, agrees with the Management of the Function involved in the whistleblowing on any necessary action plan to remedy the control weaknesses identified, according to the Audit Function's operating standards, also guaranteeing monitoring of the plan's adoption;

h) agrees with the SB on any initiatives to be taken and/or in-depth studies to be carried out before closing the whistleblowing case;

i) agrees with the Board of Statutory Auditors, for whistleblowing cases concerning complaints pursuant to Article 2408 of the Italian Civil Code *(complaints by shareholders)* - on any initiatives to adopt before closing the Whistleblowing case;

j) forwards the outcomes of investigations on whistleblowing relative to employees to the HR Function for assessment, and for the adoption of any disciplinary measures, which said HR Function will promptly notify to the Audit Function;

k) requests the HR Function to start disciplinary proceedings against the whistleblower and, where required by law, also the Judicial Authority (subject to prior involvement of the Legal & Corporate

Affairs Function), if it is proved that the whistleblowing was only undertaken to harm the person reported or due to the serious recklessnes, negligence or inexperience of the whistleblower.

5.2.5 Notification of results

Description of the activity

According to the specific content, the Audit Function notifies the results of the checks carried out to the Supervisory Board or, for whistleblowing pursuant to art. 2408 of the Italian Civil Code, to the Board of Statutory Auditors.

The Audit Function notifies the results of the checks carried out to the Senior Management and to the Head of the company functions involved in the investigation process.

Moreover, the SB, through the Audit Function, sends the Board of Stautory Auditors a periodic (monthly) report on all whistleblowing received in the reporting period, without prejudice to the timely notification of investigation results for specific whistleblowing cases of special relevance.

Lastly, as part of the report, usually prepared every six months for the Board of Directors, also sent to the Control and Risk Committee, on the activities carried out, the SB gives information summarising the whistleblowing received, without prejudice to the specific reporting of analysis results by the Audit Function to the CRC if audit action is started regarding a whistleblowing case.

5.2.6 Retaining documentation

Description of the activity

To guarantee the management and traceability of whistleblowing and relative activities, the Head of the Audit Function prepares and updates all information on whistleblowing and files all related supporting documentation for a period of ten years, from the date when the whistleblowing is received. The originals of whistleblowing received as hard copies are filed in a specific, protected environment.

5.2.7 Periodic controls

Description of the activity

The SB carries out controls on completeness, every six months, to ensure all whistleblowing received has been processed (including whistleblowing sent to dedicated Functions) and included in the periodic reporting, as indicated in this Procedure.

6. ATTACHMENTS

Attachment 1

SAFEGUARDING THE PROCESSING OF PERSONAL DATA

The information and any other personal data obtained are processed in compliance with Regulation (EU) 2016/679 (General Data Protection Regulation – hereinafter GDPR). In particular, the Company guarantees that the processing of data takes place in compliance with the rights and fundamental freedoms, as well as the dignity of data subjects, with particular reference to the confidentiality and security of data, ensuring compliance, among other, with the provisions below.
Pursuant to the GDPR, the personal data that comes to the knowledge of the Company for the purposes of this procedure shall:

- be limited to the data that are strictly and objectively necessary to verify the grounds of the whistleblowing, and for its relative management;
- be processed lawfully and fairly.

In addition:

- all functions/organisational positions of the Company concerned by any direct receipt of whistleblowing will ensure the utmost confidentiality of the whistleblowers and reported persons. Pursuant to Article 4 of the Code of Ethics and Conduct, there will be no negative consequence for whistleblowers acting in good faith and the confidentiality of their identity will be ensured, according to specific internal procedures, save for legal obligations;
- the privacy notice indicated in Attachment 2, which is an integral and substantial part of the "Whistleblowing" procedure shall be made available to data subjects;
- third parties, not having direct or indirect business dealings with the company, shall be notified that their personal data are processed regarding whistleblowing received by the Company only if there is no risk that in disclosing this information, the capacity to effectively verify the grounds of the whistleblowing is compromised;
- the person referred to in the whistleblowing is not given information on the identity of the whistleblower, save for cases where it is established that the whistleblower has made a false declaration;
- Similarly to Article 54-bis, paragraph 2 of Legislative Decree no. 165 of 30 March 2001 (Consolidated Act on Public Employment) and Article 6 of Legislative Decree no. 231 of 8 June 2001, as amended by Law no. 179 of 30.11.2017, during any disciplinary proceedings brought against the reported person, the identity of the whistleblower may not be revealed, without his/her consent, provided that the claim the disciplinary proceedings refer to is based on separate grounds in addition to the whistleblowing. If the claim against the whistleblowing is founded, entirely or in part, the identity may be revealed if such knowledge is absolutely essential for the defence of the reported person.

Attachment 2

PRIVACY NOTICE

Pursuant to the Regulation (EU) 2016/679 (General Data Protection Regulation – hereinafter GDPR)) information is given to you, below, by Inwit S.p.A., hereinafter Inwit, on the processing of your personal data carried out in relation to the management of whistleblowing regulated by the "Whistleblowing Procedure" issued by the Audit Function of Inwit.

1) Purposes for which the processing of data is necessary and relative legal basis

The personal data of data subjects are processed for purposes related to the adoption of the above procedure and to meet obligations of law, regulations or EU legislation. Giving data is mandatory to achieve the above purposes. Failure to provide all or some of the data or providing inaccurate date could make it impossible to manage the whistleblowing received.

2) Retention of personal data

Inwit retains its data for the time indicated in the"Whistleblowing Procedure" which establishes that whistleblowing and relative documentation is deleted after 10 years and, in any case, is retained for no longer than is necessary for the purposes for which the personal data are obtained or subsequently processed.

3) Procedure and logics of processing

Data are processed manually (for example on hard copies) and/or by automated means (for example using electronic procedures and media), with logics related to the above purposes and, in any case, in such a way as to guarantee the security and confidentiality of the data. The whistleblowing management system guarantees the confidentiality of the whistleblowing during all stages (including information on any persons referred to), and the identity of the whistleblower, also using encrypted information, apart from cases where:

- the whistleblowing is unfounded and was only undertaken to harm the person reported or due to the serious indiscretion, negligence or inexperience of the whistleblower;
- anonymity cannot be opposed by law (e.g. criminal investigations, inspections of control bodies, etc.);
- the whistleblowing identifies facts which, although external to the company, require reporting to the judicial authorities (e.g. terrorism, spying, attacks, etc.).

Violations of the non-disclosure obligation (apart from the exceptions above), are subject to disciplinary action.

4) The Controller, Data Protection Officer and categories of persons authorised to process data at INWIT

The Controller is INWIT S.p.A., with head office in via Gaetano Negri, n. 1 - 20123 Milano. INWIT S.p.A. has appointed its own Data Protection Officer The contact information for the Data Protection Officer is as follows:

- Postal Address: INWIT DPO, c/o Infrastrutture Wireless Italiane S.p.A., Via Gaetano Negri 1 - 20123 Milan.
- Email Address: dpo.inwit@telecomitalia.it

Personal data are processed by the Processor and Employees of the Audit Function of INWIT S.p.A. These employees have been authorised to process personal data and in this regard have received adequate operating instructions.

5) Categories of third parties to whom the data could be notified in a capacity as Controllers or to whom data could come to their knowledge in a capacity as Processors

Besides the above employees of INWIT, some of your personal data might be processed by third parties, to whom INWIT assigns some activities (or a part of said) to achieve the purposes indicated in point 1). These third parties might also have establishments abroad, in EU or non-EU countries; in the latter case, data are transferred based on the existence an adequacy decision by the European Commission as to the level of protection of data in the non-EU country, or based on appropriate or suitable safeguards as indicated in Articles 46 or 47 of the GDPR (e.g. signing standard data protection clauses adopted by the European Commission), or further conditions enabling transfer, as indicated in Article 49 of the GDPR. These entities operate as independent Controllers or will be designated as Processors and are basically included in the following categories:

a) Members of Corporate Boards
b) Consultants (Organisation, Litigation, Legal Practices, etc.)
c) Companies appointed to oversee personnel administration and management, the storage of employees' personnel data, and the development and/or operation of dedicated IT systems
d) Companies in charge of the management of the company's archives, including the personal data of former employees
e) Audit companies
f) Public institutions and/or authorities, judicial authorities, the police force, investigation agencies.

6) Right to access personal data and other rights

You are entitled to access data concerning you, at any time - save for indications in attachment 1 of the applicable procedure - and may exercise other rights established by legislation on the protection of personal data (e.g. request the origin of data, the rectification of inaccurate or incomplete data, a restriction on processing, the cancellation or portability of data, the right to be forgotten, as well as object to the use of data for lawful reasons), sending an email to dpo.inwit@telecomitalia.it. Lastly, you have the right to file a complaint with the Data Protection Authority.