THINK.TEST.TRUST.

MTS S.r.l.

WHISTLEBLOWING PROCEDURE

pursuant to Leg. Decree n. 24/2023 and art. 6 c. 2bis of Leg. Decree n. 231/2001

Contents

1. Introduction

Following publication of Legislative Decree no. 24 dated 10 March 2023 in the Official Journal no. 63 dated 15 March 2023, Directive (EU) 2019/1937 of the European Parliament and of the Council dated 23 October 2019 on the protection of persons, operating in both the public and private sectors, who report breaches of Union law, and laying down provisions on the protection of persons who report breaches of national laws was implemented.
MTS S.r.l. (hereinafter also referred to as 'MTS' or 'Company' or 'Entity'), pursuant to the aforementioned decree, has set up a procedure for the management of whistleblowing reports, the so-called *whistleblowing procedure*, which is an integral part of the Organisation, Management and Control Model pursuant to Legislative Decree 231/2001 (hereinafter also referred to as 'MOG231') adopted by the Company.

2. Purpose of the procedure

The purpose of the procedure pursuant to Legislative Decree no. 24/2023 is to regulate the process of receiving, analysing and processing whistleblowing reports of breaches of national or European Union regulations harmful to the public interest or the integrity of MTS and of conduct that could constitute the committing of one or more offences pursuant to Legislative Decree no. 231/01 or constitute a breach of MTS' MOG231
The procedure has been set up pursuant to Legislative Decree no. 24/2023, in compliance with the provisions of article 6, paragraph 2 bis of Legislative Decree no. 231/2001, which requires the implementation within the organisational models of the activation of an internal reporting channel, the prohibition of retaliation and the application of a disciplinary system.
The procedure also regulates the procedures for checking the validity and substantiation of whistleblowing reports and the measures to be taken in the case of whistleblowing reports made solely for the purpose of slander or defamation.

3. Scope

This procedure considers as of relevance whistleblowing reports concerning illicit or irregular conduct, or offences - committed or attempted - with which the whistleblower has become acquainted in the performance of his or her duties or functions, which may consist of actions or omissions:

- relevant for the purposes of the breach of national or EU regulatory provisions;
- relevant for the purposes of the predicate offences identified in the MOG231 and for the purposes of the institution of the administrative liability of entities;
- likely to lead to breaches of the rules of conduct and/or principles of behaviour identified in the MOG231 and the Code of Ethics adopted by MTS.

In short, the whistleblowing report may concern not only breaches of national or European Union regulations, but also:

- breaches of the MOG231 adopted by MTS;
- breaches of MTS' Code of Ethics;
- the specific committing of offences under Legislative Decree no. 231/01.

The whistleblowing report may not concern:

a) disputes, claims or requests linked to an interest of a personal nature of the whistleblower or of the person who has made a report to the judicial or accounting authorities which relate exclusively to their individual employment relationships, or concerning their employment relations with hierarchically superior figures;
b) whistleblowing reports of breaches which are already mandatorily regulated by the European Union or national acts indicated in part II of the annex to Legislative Decree no. 24/2023 or by national acts constituting implementation of the European Union acts indicated in part II of the annex to Directive (EU) 2019/1937, even if not indicated in part II of the annex to the aforesaid decree;
c) whistleblowing reports of breaches of national security, as well as of tenders relating to defence or national security aspects, unless such aspects are covered by the relevant secondary legislation of the European Union.

With regard to whistleblowing reports concerning grievances of a personal nature of the whistleblower or claims/complaints falling within the field of the employment relationship, reference should be made to the Managing Director as the function delegated by the Board of Directors for matters concerning the Cooperative's personnel.

4. Entities involved

The entities as indicated in article 3 paragraphs 2 and 3 of Legislative Decree no. 24/2023 are required to apply the procedure and more specifically:

- employees of MTS, including workers whose employment contract is governed by Legislative Decree no. 81/2015, or by article 54-bis of Legislative Decree no. 50/2017, converted, with amendments, by Law no. 96/2017;
- self-employed workers, including those indicated in chapter I of Law no. 81/2017, and those involved in a collaboration agreement as referred to in article 409 of the Italian civil procedure code and article 2 of Legislative Decree no. 81/2015, who carry out their work activities within the Company;
- workers or collaborators, who carry out their work activities at entities in the public or private sector which provide goods or services or carry out works in favour of MTS;
- freelancers and consultants who provide their services to MTS;
- paid and unpaid interns who work for MTS;
- shareholders and persons with administrative, management, control, supervisory or representative functions at MTS, even if such functions are exercised on a *de facto* basis.

5. Content of report

Whistleblowing reports must be circumstantiated and based on precise and concordant elements, and must relate to facts known and verified directly by the whistleblower and not referred to by third parties, unless the whistleblowing report is communicated to an entity other than the identified whistleblowing channel, in which case the measures shall apply

identified below in the procedure for the management of the whistleblowing report communication.
The whistleblowing report should also, if possible, contain all the information necessary to identify with certainty and unequivocally the perpetrator of the conduct to which the whistleblowing report refers.
Whistleblowing reports made anonymously will only be taken into account if they are substantiated. They will be treated in the same way as ordinary reports and processed in accordance with this procedure. The anonymous whistleblower, if subsequently identified, will benefit from the protection provided by Legislative Decree no. 24/2023 against retaliatory measures[1].
In order to ensure the whistleblower is protected as regards the confidentiality provided by Legislative Decree no. 24/2023, MTS adopts an IT platform for the management of whistleblowing reports and communications between the whistleblower and the reporting channel.

In particular, the report (hereinafter also 'whistleblowing report') must contain the following elements:

- general details of the person making the whistleblowing report;
- a clear and complete description of the facts which are the subject of the whistleblowing report and of how the whistleblower became directly acquainted with them;
- if known, the circumstances of time and place in which the fact occurred;
- if known, the personal details or other elements enabling identification of the person who determined the reported facts;
- the indication of any other entities able to provide information with regard to the reported facts;
- the indication of any documents confirming the accuracy of the reported facts;
- any other information useful to verify the existence of the reported facts.

6. Recipients of whistleblowing reports and ways of sending

The management of whistleblowing reports is entrusted by MTS to an internal whistleblowing compliance management channel (hereinafter also referred to as the "Manager") identified in the members of the Supervisory Board, who also meet the regulatory criteria set out in article 4 par. 2 of Legislative Decree 24/2023. The Manager is the recipient of whistleblowing reports in accordance with the procedures provided by the dedicated IT platform, implemented by the Company in the pages of its corporate website https://MTS.whistletech.online.
The IT platform implemented by MTS for managing whistleblowing reports ensures the confidentiality requirements set out in the legislation, allowing for both written and oral whistleblowing reports. Furthermore, at the request of the whistleblower, the IT platform allows whistleblowing reports to also be made through a direct meeting with the Manager.

[1] Art. 16 par. 4 of Leg. Decree no. 24/2023

In the case of a whistleblowing report communicated to a person other than the one indicated above, such report must be sent to the Manager within 7 days of its receipt, with simultaneous notification of such dispatch to the whistleblower.
For more complete information on the ways of sending whistleblowing reports, MTS, in addition to what is indicated in this procedure, asks that reference be made to the implemented IT platform and to the related Manual of regulation and operation of the same (Whistletech Manual) annexed to this procedure.

7. Internal reporting channel: checking, ascertaining and results of whistleblowing reports

The Manager receives the whistleblowing reports by means of the IT platform and manages them according to the following criteria:

- issue to the whistleblower of an acknowledgement of receipt of the whistleblowing report within 7 days from the date of receipt through the communication system provided by the IT platform
- formulation of an initial judgement of admissibility, excluding the whistleblowing reports that do not fall within the scope of this procedure (e.g. generic complaints, grievances)
- maintenance of exchanges with the whistleblower with, if necessary, the possibility of asking the latter to provide additional information;
- diligent management of whistleblowing reports received by proceeding:
    - to send the whistleblowing report, after making it completely anonymous and/or reproducing it in order to make it unrecognisable and/or otherwise traceable to the whistleblower, to other entities in order to acquire further information and comments. Such entities shall be required to formulate assessments and provide the requested feedback within and no later than fifteen days from receipt of the request;
    - to file the whistleblowing report, on the basis of adequate grounds, in the event of initial checks carried out revealing it to be unfounded or insufficiently circumstantiated or still irrelevant;
    - in the case of non-filing, to communicate the outcome of the assessment and/or check to the managing directors of MTS in relation to the responsibilities as defined by the powers attributed to them by the Board of Directors of the Company, for the appropriate evaluations and possible resolutions for disciplinary and sanctioning purposes, or for the appropriate interventions on the MOG231. The aforesaid persons delegated by the Board of Directors shall assess such measures in agreement with the Company's Administrative Body;
    - to review the disciplinary and sanctioning assessments activated by the MTS administrative body and any assessments of interventions on the MOG231;
- deadline of acknowledgement of the whistleblowing report within three months from the date of the acknowledgement of receipt or, in the absence of such an acknowledgement, within three months from the expiry of the seven-day period from the submission of the whistleblowing report;

- placing at disposal of clear indications on the channel, procedures, IT platform used and prerequisites for making internal whistleblowing reports, and on the channel, procedures and prerequisites for making external whistleblowing reports. In this sense, the abovementioned information shall be displayed and made easily visible in the workplace, as well as accessible to persons who, although not frequenting the workplace, have a legal relationship in one of the forms referred to in article 3, par. 3 - 4 of Legislative Decree 24/2023.

8. Protection of whistleblower

WHISTLEBLOWER IDENTITY CONFIDENTIALITY OBLIGATION

Whistleblowing reports may not be used more than what is necessary to adequately follow them up.
The identity of the whistleblower and any other information from which this identity may be inferred, directly or indirectly, may not be disclosed without the express consent of the whistleblower; this protection also applies to MTS top management, which may not investigate or request information in order to trace the identity of the whistleblower.
The obligation to keep the identity of the whistleblower strictly confidential and not to investigate or request information applies to anyone who, for whatever reason, becomes aware of the whistleblower's identity or is involved in the whistleblowing process.
In the context of disciplinary proceedings, the identity of the whistleblower may not be disclosed, where the disciplinary accusation is based on investigations which are separate and additional to the whistleblowing report, even if consequent thereto. If, on the other hand, the dispute is based, in whole or in part, on the whistleblowing report and knowledge of the identity of the whistleblower is indispensable for the defence of the accused person, the whistleblowing report may only be used for the purposes of disciplinary proceedings if the whistleblower has expressly consented to the disclosure of his or her identity.
With reference to the above-mentioned hypotheses, the whistleblower is informed of the reasons for the disclosure of the confidential data by means of a written communication. This information is provided in the context of the internal and external whistleblowing activities referred to in this procedure when disclosure of the identity of the whistleblower and of the information is also indispensable for the defence of the person concerned.
The violation of the protection of the confidentiality of the whistleblower, except in cases where disclosure of identity is permitted as outlined above, entails the start of disciplinary proceedings in accordance with the provisions of the reference legislation and of the applied Collective National Labour Agreement applicable to the entities to which it applies.
No protection is due in the event of the whistleblower incurring, with his or her whistleblowing report, criminal liability for slander (article 368 of the Italian Criminal Code) or defamation (article 595 of the Italian Criminal Code).
As part of the internal and external whistleblowing activities referred to in this procedure, the person concerned may be heard, or, at his or her request, shall be heard, also by means of a paper procedure through the acquisition of written observations and documents.

NO DISCRIMINATION WITH REGARD TO THE WHISTLEBLOWER

The entities to whom this procedure applies and who make a whistleblowing report in compliance with it and with the regulatory provisions of Legislative Decree no. 24/2023 may

not suffer any retaliation for the whistleblowing reports made. In this sense, retaliation, as defined in article 2, par. 1, point m) of the aforementioned Decree, constitutes any conduct, act or omission, even if only attempted or threatened, carried out as a result of the whistleblowing report, of the report to the judicial or accounting authorities or of public disclosure and which causes or may cause unfair harm to the whistleblower or to the person who has made a report, either directly or indirectly

The following are cases that may constitute retaliation:

a) dismissal, suspension or equivalent measures;
b) downgrading or non-promotion;
c) change of duties, change of place of work, reduction of salary, change of working hours;
d) suspension of training or any restriction as regards access to it;
e) negative merit notes or references;
f) the adoption of disciplinary measures or any other sanction, including a fine;
g) coercion, intimidation, harassment or ostracism;
h) discrimination or otherwise unfavourable treatment;
i) the non-conversion of a fixed-term employment contract into an employment contract of indefinite duration, where the employee had a legitimate expectation of such conversion;
j) the non-renewal or early termination of a fixed-term employment contract;
k) damage, including to a person's reputation, particularly on social media, or economic or financial loss, including loss of economic opportunities and loss of income;
l) improper listing on the basis of a formal or informal sector or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future;
m) the early termination or cancellation of a contract for the supply of goods or services;
n) the cancellation of a licence or permit;
o) a request to undergo psychiatric or medical examinations.

To protect the whistleblower, pursuant to article 17, par. 2 and 3 of the aforementioned Decree (No retaliation), in the context of judicial or administrative proceedings or, in any case, out-of-court disputes concerning the ascertainment of the prohibited conduct, acts or omissions in respect of the whistleblowers, it is presumed that such conduct or acts were put in place as a result of the whistleblowing report, public disclosure or report to the judicial or accounting authorities. The onus of proving that such conduct or acts are motivated by reasons unrelated to the whistleblowing report, public disclosure or report to the judicial or accounting authorities lies with the person who has carried them out.

Moreover, in the event of a claim for damages filed with the judicial authorities by the whistleblowers, if such persons prove that they have made a whistleblowing report, public disclosure or report to the judicial or accounting authorities pursuant to the aforementioned Decree and that they have suffered damage, it shall be presumed, unless proven otherwise, that the damage is the consequence of such whistleblowing report, public disclosure or report to the judicial or accounting authorities.

The above protections for whistleblowers do not apply if the following conditions are not met:

(a) at the time of the whistleblowing report or report to the judicial or accounting authorities or of the public disclosure, the whistleblower or reporting person

had reasonable grounds to believe that the information on the violations referred to in the whistleblowing report, publicly disclosed or reported to the judicial or accounting authorities was true and fell within the objective scope of the aforementioned Decree;

(b) the whistleblowing report or public disclosure was made on the basis of the provisions of the relevant legislation and in accordance with this procedure.

Furthermore, condition for the protection of the whistleblower is the fact that the reasons that led the person to make the whistleblowing report, the report to the judicial or accounting authorities, or the public disclosure are irrelevant for the purposes of his or her protection.

In the event of the criminal responsibility of the whistleblower being established, including by a judgement of first instance, for the offences of defamation or slander or in any case for the same offences committed with the report to the judicial or accounting authorities, i.e., his or her civil liability for the same offences, in cases of wilful misconduct or gross negligence, the protections provided for by law for the whistleblower are no longer provided and a disciplinary sanction is imposed on the whistleblower or reporting person.

The conditions for the application of the protections in favour of the whistleblower and the disciplinary measures that apply in the event of the criminal liability of the latter as set out above also apply in cases of anonymous whistleblowing or reporting to the judicial or accounting authorities or public disclosure, if the whistleblower is subsequently identified and has suffered retaliation, as well as in cases of whistleblowing reports submitted to the competent institutions, bodies and organs of the European Union, in accordance with the conditions set out in article 6 of Legislative Decree no. 24/2023.

The whistleblower may inform the ANAC (Italian National Anti-Bribery Authority) of the retaliation he/she believes he/she has suffered. In the event of retaliation committed in the employment context, the ANAC informs the National Labour Inspectorate, for measures within its field of competence.

In this regard, pursuant to article 19 of Legislative Decree no. 24/2023 and in order to acquire preliminary elements essential for ascertaining the retaliation, the ANAC may avail itself of the collaboration of the National Labour Inspectorate, to the extent of its respective competence, without prejudice to the exclusive competence of the ANAC as regards the assessment of the elements acquired and the possible application of administrative sanctions.

Measures taken in breach of the no retaliation clause are to be deemed null and void.

Whistleblowers who have been dismissed as a result of a whistleblowing report, public disclosure or report to the judicial or accounting authorities have the right to be reinstated in their jobs, pursuant to article 18 of Law no. 300/1970 (so-called Workers' Statute), or article 2 of Legislative Decree no. 23/2015, because of the specific rules applicable to the worker.

The seised judicial authority adopts all the measures, including provisional ones, necessary to ensure the protection of the subjective legal situation being asserted, including compensation for damages, reinstatement in the workplace, an order to cease the conduct which breaches the aforementioned article 17 and the declaration of nullity of the measures adopted in violation of the same article.

Finally, as a limitation of the whistleblower’s liability, pursuant to article 20 of Legislative Decree no. 24/2023, the whistleblower is not punishable who discloses or disseminates

information on breaches covered by the obligation of secrecy, other than that referred to in article 1, par. 3, of the aforementioned decree protected by secrecy, or relating to the protection of copyright or the protection of personal data, i.e., who discloses or disseminates information on breaches that offend the reputation of the person involved or reported, when, at the time of the disclosure or dissemination, reasonable grounds existed for believing that the disclosure or dissemination of the same information was necessary to disclose the breach and that the whistleblowing report, public disclosure or report to the judicial or accounting authorities was made pursuant to article 16 of the aforementioned Decree.
Without prejudice to the aforementioned protections provided by the reference legislation, any individual who believes he/she has been discriminated against because he/she has reported an offence shall immediately and thoroughly inform the Whistleblowing Report Manager.
The latter, having assessed what has happened, shall report it to the Board of Directors of the Company, for the adoption of all necessary and appropriate initiatives.

PERSONAL DATA PROCESSING

Any processing of personal data must be carried out in accordance with Regulation (EU) 2016/679 and Legislative Decree no. 196/2003 (the so-called Privacy Code). The disclosure of personal data by the institutions, bodies, offices or agencies of the European Union shall be carried out in accordance with Regulation (EU) 2018/1725.
Personal data that are manifestly not useful for the processing of a specific whistleblowing report shall not be collected or, if accidentally collected, shall be immediately erased.
The processing of personal data relating to the receipt and management of whistleblowing reports shall be carried out by the recipients referred to in the internal reporting channel, in their capacity as data controllers, in accordance with the principles set out in articles 5 and 25 of Regulation (EU) 2016/679, by providing appropriate information to the whistleblowers and to the persons concerned pursuant to articles 13 and 14 of Regulation (EU) 2016/679, as well as by taking appropriate measures to protect the rights and freedoms of the data subjects.
MTS defines its model for the receipt and management of internal reports, identifying appropriate technical and organisational measures to ensure a level of security appropriate to the specific risks arising from the processing carried out, based on a data protection impact assessment, and regulating the relationship with any external providers processing personal data on their behalf pursuant to article 28 of Regulation (EU) 2016/679.

STORAGE OF DOCUMENTS RELATING TO WHISTLEBLOWING REPORTS

Whistleblowing reports, both internal and external, and the relevant documentation are kept for the time necessary for their processing and in any case for no longer than five years from the date of the communication of the final outcome of the reporting procedure, in compliance with the above-mentioned obligations of confidentiality and processing of personal data.
If, in order to make the whistleblowing report, a registered telephone line or other registered voice messaging system is used, the whistleblowing report, subject to the consent of the whistleblower, shall be documented by the recipient, referred to in the internal

reporting channel, either by recording on a device suitable for storage and listening, or by transcription in full. In the case of a transcript, the whistleblower may verify, rectify or confirm the content of the transcript by signing it.
If, in order to make the whistleblowing report, an unregistered telephone line or other unregistered voice messaging system is used, the whistleblowing report shall be documented in writing by a detailed transcript of the conversation made by the Managing entity referred to in the internal reporting channel. The whistleblower may verify, rectify and confirm the contents of the transcript by signing it.
When, at the request of the whistleblower, the whistleblowing report is made orally in the course of a meeting with the Managing entity, referred to in the internal reporting channel, it shall, subject to the consent of the whistleblower, be documented by the said recipient either by recording on a device suitable for storage and listening or by the taking of minutes. In case of the taking of minutes, the whistleblower may verify, rectify and confirm the minutes of the meeting by affixing his or her signature to such minutes.

9. Changes to risk-prevention measures

If, as a result of the whistleblowing reports and communications with respect to the bodies of MTS, objective evidence emerges to reveal deficiencies in the internal control systems, the Board of Directors of the Company shall promptly adjust them or mandate the Chairperson for corrective actions to be implemented to adjust the internal control system.

10. Reference documents

- Legislative Decree 231, dated 8 June, 2001: “Regulations on the administrative liability of legal entities, companies and associations, including those without legal personality, pursuant to article 11 of Law no. 300 dated 29 September, 2000, as amended and supplemented.”
- Legislative Decree no. 24, dated 10 March, 2023: “Implementation of EU Directive 2019/1937 of the European Parliament and of the Council dated 23 October, 2019 on the protection of persons who report breaches of Union law and laying down provisions regarding the protection of persons who report breaches of national laws.”
- Model of organisation, management and control adopted by MTS.
- Code of Ethics adopted by MTS.
- Regulation of IT platform for application of whistleblowing procedure.

11. Annexes to procedure

IT platform regulation – Whistletech manual

Personal data processing privacy policy within the scope of the illicit or irregular activity reporting (whistleblowing) procedure pursuant to Leg. Decree no. 24 dated 10 March 2023

This privacy policy is provided pursuant to EU Regulation 2016/679 of the European Parliament and of the Council dated 27.04.2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (so-called "General Data Protection Regulation" or "GDPR") and Legislative Decree no. 196 dated 30.06.2003, as amended and supplemented by Legislative Decree no. 101 dated 10.08.2018, ("Personal Data Code" or "Privacy Code") by the Data Controller, i.e. the entity which determines the purposes and means of personal data processing.

The Data Controller, aware of the importance of ensuring the security of information of a personal nature, provides the information necessary to inform the whistleblower (hereinafter "Data Subject") of the characteristics and methods of processing of his or her personal data acquired for the purpose of reporting potential illicit or irregular activities of which he or she has become aware by reason of his or her employment, service or supply relationship with the Data Controller.

1. Data Controller

MTS srl, with registered office in Forlì (FO), via dei Senoni, 8, taxpayer's and VAT number 11054190969, in the person of its *pro tempore* legal representative, in the capacity of Data Controller (hereinafter referred to as "Data Controller"), Dr. Francesco Ferraris

2. Purpose of processing

The processing in question concerns the personal data acquired, managed and stored in the context of whistleblowing reports of breaches of national or European Union regulatory provisions harmful to the public interest or to the integrity of a public administration or a private entity, of which the whistleblower has become aware by reason of his or her employment, service or supply relationship with the Data Controller.

All personal data acquired in the context of whistleblowing reports of potential illicit or irregular activities are processed by the Data Controller for purposes strictly related to the acquisition and management of such whistleblowing reports, in order to carry out the necessary investigative activities aimed at verifying the grounds of the facts reported and the adoption of the consequent measures.

3. Subject of processing

The following personal data may be processed, insofar as contained in the whistleblowing report and/or in acts and documents annexed thereto:

- common personal data (e.g. first name, last name, job title or position, contact details, contained in the whistleblowing reports or necessary for the functioning of the whistleblowing system, etc.);

- special personal data: no special categories of personal data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data intended to uniquely identify a natural person, data concerning a person's health or sex life or sexual orientation) are collected, unless they are indicated by the whistleblower himself/herself in the whistleblowing report and any annexes thereto;

- additional data and information relating to the reported illicit conduct: data relating to criminal convictions and offences (judicial data) may therefore be processed, pursuant to the provisions of article 10 of the GDPR.

In addition to the whistleblower, personal data may also refer to persons indicated as possibly responsible for the illicit conduct, as well as to persons in various capacities involved in the reported events, indicated in the whistleblowing report itself.

4. Legal basis

Personal data are processed in order to comply with the provisions of Legislative Decree no. 24 dated 10.03.2023*, (Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council dated 23 October 2019 on the protection of persons who report breaches of Union law and containing provisions concerning the protection of persons who report breaches of national laws).*

The legal basis justifying the processing of personal data is the fulfilment of a legal obligation to which the Data Controller is subject pursuant to article 6, par. 1, point c) GDPR for common personal data, article 9, par. 2, point c) GDPR for special personal data and article 10 GDPR for judicial personal data.

5. Nature of data provision

The provision of personal data for the above-mentioned processing purposes is necessary in order for the Data Controller to be able to take charge of the whistleblowing report and proceed with further investigations, if the legal requirements are met; failure to provide such data may therefore make it impossible to manage whistleblowing reports of potential illicit or irregular activities.

6. Secrecy of the whistleblower's identity

By default, the IT platform for receiving whistleblowing reports (digital whistleblowing) is configured so as never to reveal the identity of the whistleblower, who remains unknown to the entities receiving the whistleblowing report and/or involved in its management.

Only if, in the cases provided for by law, it is necessary to know the identity of the whistleblower (e.g. in order to ensure the reported person's right of defence in disciplinary proceedings), will the whistleblower be asked whether he/she intends to give his/her consent to reveal his/her identity. In this case, technical and organisational measures are in any case taken to ensure the utmost confidentiality of the information and its use for the exclusive pursuit of the purposes stated above.

7. Access, communication, dissemination

The personal data acquired may only be made accessible to persons expressly instructed and authorised to process such data who are employed by or under the direct authority of the Data Controller.

Personal data may also be processed by third parties who carry out activities on behalf of the Data Controller (and to workers or collaborators, expressly instructed and authorised to process data, who work in the employ or under the direct authority of the same third parties), who can prove that they have adopted technical and organisational measures such as to ensure data security. Such third parties, expressly designated as Data Processors, are provided with adequate operating instructions. The company supplying the digital whistleblowing IT platform has been designated as Data Processor in respect of activities connected with the operational management and maintenance of the system itself.

The processed personal data may be communicated to other specified parties in the cases provided for by applicable legislation, such as, where applicable, the Judicial Authority and ANAC, which will process them as autonomous data controllers within the scope of their institutional functions

The processed data may not be disclosed to unspecified parties.

8. Processing methods and data retention period

Personal data will be processed using electronic and manual devices, in such a way as to safeguard their integrity and confidentiality, as well as their availability only to persons authorised to investigate and manage the whistleblowing report.

The personal data relating to the whistleblowing report and any attachments will be retained on the digital whistleblowing IT platform for at most 3 (three) months from receipt of the whistleblowing report, unless the investigation continues. The investigation

file, the documentation relating to the investigation and the personal data contained therein, shall be kept for the time necessary for their definition and, in any case, for no longer than 5 (five) years from the date of the communication of the final outcome of the whistleblowing procedure, without prejudice to different requirements due to the establishment of possible legal proceedings.

9. Data transfer

The personal data are stored in Italy or, in any case, within the European Union and the European Economic Area.

Any transfer to third countries, not belonging to the European Union or the European Economic Area, may only take place to those countries able to ensure an adequate level of protection of personal data, by means of methods that comply with the regulations on the protection of personal data.

10. Data subjects' rights

Pursuant to art. 15 et seq. GDPR, the data subject, where applicable, has the right to:

- obtain from the Data Controller confirmation as to whether or not personal data concerning him/her are being processed and, if so, access to the personal data and other related information, including by receiving a copy thereof (right to access)
- obtain from the Data Controller the rectification of inaccurate personal data and/or the supplementing of incomplete personal data concerning him/her (right to rectification);
- in the cases provided for, to obtain from the Data Controller the erasure of personal data (right to erasure);
- in the cases provided for, to obtain from the Data Controller the restriction of the processing of all or part of the personal data processed by the Data Controller (right to restriction of processing);
- in the cases provided for, to object, in whole or in part, to the processing of personal data (right to object);
- in the cases provided for, not to be subjected to a decision based solely on automated processing.

If the Data subject considers that the processing of the personal data is in breach of data protection legislation, he/she has the right to lodge a complaint with the competent supervisory authority (Data Protection Authority) or, in the cases provided for, to take the matter to the judicial authority.

11. Exercising rights

The Data subject may exercise his or her rights at any time by using the computer platform activated by the company.

_ _ _ _ _ _ _ _ _

Additional information for the reported person and persons involved in various ways in the reported events.

The acquisition and management of the whistleblowing reports received gives rise to the processing of personal data, including those belonging to particular categories of data and relating to criminal convictions and offences, possibly contained in a whistleblowing report and in acts and documents annexed thereto, referring to the person reported or possibly to those involved in various ways in the reported matter.

For the sake of transparency vis-à-vis these persons, please note that

- the right to be informed about the processing of one's personal data pursuant to articles 12, 13 and 14 GDPR is restricted in light of the obligations of secrecy and confidentiality imposed by the whistleblowing legislation, as well as due to the risk of making it impossible or seriously prejudicing the achievement of the purposes of the processing related to the whistleblowing reports of illicit or irregular activities;
- the rights set out in article 15 et seq. of the GDPR cannot be exercised inasmuch as the exercising of those rights could prejudice the protection of the confidentiality of the identity of the whistleblower. In this case, therefore, the reported person is precluded from exercising his or her rights by addressing the Data Controller in the prescribed manner. This is without prejudice to the possibility for the reported person to exercise his or her rights in the specific ways provided for in articles 2-*undecies* and 160 of the Privacy Code.

For further information to the reported person or, if applicable, to those involved in the reported matter, please refer to the other paragraphs regarding the personal data processing privacy policy within the scope of the illicit or irregular activity reporting (whistleblowing) procedure.

_ _ _ _ _ _ _ _ _

Should it become necessary, the Data Controller may have to update this policy. The Data Subject is therefore invited to periodically visit this page to check that nothing has changed.

_ _ _ _ _ _ _ _ _

_ _ _ _ _ _ _ _ _

The Data Controller

MTS srl.