

Whistleblowing Procedure

Contents

1. INTRODUCTION	2
2. RECIPIENTS	2
3. PURPOSE AND SCOPE OF APPLICATION	3
4. REFERENCES	4
5. PROCESS DESCRIPTION AND LIABILITY	5
5.1 Purpose and process description	5
5.2 Transmission of the Report	5
5.3 Recording of the Report	6
5.4 Classification and Preliminary Analysis of the Report	6
5.5 Conducting of the investigation	8
5.6 Reporting	8
5.7 Corrective Actions: Monitoring	9
5.8 Personal data processing and retention of documentation	10
5.9 Periodic checks	10
6. GUARANTEES AND SAFEGUARDS	10
6.1 Protection of the Whistleblower	10
6.2 Protection Measures	11
7. GLOSSARY	12

1. INTRODUCTION

The purpose of this procedure (hereinafter Procedure) is to regulate the process of sending, receiving, analysing and handling Reports (so called Whistleblowing) on adequately substantiated information referring to TIM Personnel and/or Third Parties relating to violations of laws and regulations, the Code of Ethics and Conduct of the TIM Group, the Organisational Model 231, as well as the system of rules and procedures in place in the TIM Group, including - but not limited to - the Policy on "Respecting Human Rights in the Telecom Italia Group", the TIM Anti-Corruption Management System, the Telecom Italia Group Anti-Corruption Policy and the "Task Risk Management" Procedure.

The procedure is also aimed at implementing Legislative Decree No. 24 of 10 March 2023, published in the Official Journal on 15.03.2023, including the adoption of the Directive (EU) 2019/1937 on "the protection of persons who report breaches of EU law (the Whistleblower Directive)".

The provisions of the aforementioned Legislative Decree are fully applicable for anything that is not specifically stated in this Procedure.

At a glance, the aforementioned legislation provides:

- a protection system of specific categories of persons who report information, obtained in the context of their work, concerning violations of national or European Union regulations that damage the public interest or the integrity of the entity;
- protection measures, including the retaliation prohibition, to protect the Whistleblower as well as the Facilitators, colleagues and relatives of the Whistleblower and of legal entities connected to the Whistleblower;
- the establishment of reporting channels for sending Reports within the entity (one of which is an IT channel), which protect the confidentiality of the identity of the Whistleblower, the Person involved and/or in any case mentioned in the Report, of the Report content and of the relevant documentation, also through the use of encryption tools;
- in addition to the power to lodge a complaint with the judicial or accounting authorities, the possibility (if one of the conditions provided for in Article 6(1) of Legislative Decree No. 24/2023 is met) to make external Reports through the channel managed by the National Anti-Corruption Authority (hereinafter ANAC), as well as to carry out public Disclosures (if one of the conditions provided for in Article 15(1) of Legislative Decree No. 24/2023 is met), through the press or electronic means or dissemination able to reach a large number of people;
- disciplinary measures as well as fines imposed by ANAC in the cases provided for in Articles 16 and 21 of Legislative Decree No. 24/2023.

2. RECIPIENTS

The Recipients of the Procedure are:

- Top Management, members of the governing bodies and members of the Supervisory Body of TIM S.p.A. (hereinafter TIM) and its Subsidiaries,
- employees, former employees and job applicants, associates, customers of TIM and its Subsidiaries, as well as - but not limited to - partners, suppliers (including contractors/subcontractors), consultants and co-workers who work for TIM and/or its Subsidiaries,

who have information on violations as defined in this Procedure.

Physical and legal entities that are not part of the previous categories, but who are covered by the protection measures provided for by this Procedure apply, are also included in the Recipients.

The provisions of this document also apply to anonymous Reports, as long as they are adequately substantiated, as defined in this Procedure.

3. PURPOSE AND SCOPE OF APPLICATION

The purpose of the Procedure is to regulate the process of sending, receiving, analysing and handling Reports, including the retention and subsequent deletion of both the Reports and the related documents, as defined in this document.

The Procedure applies to TIM and its Subsidiaries (as defined in this Procedure), which ensure its proper and consistent application, as well as its full internal and external deployment, taking into account the prerogatives of autonomy and independence of each Company. Moreover, Fondazione TIM and other subsidiaries of TIM Group not included in the scope of application of the Procedure could refer to this document and adopt it, in accordance with specific and/or local regulations, processes and organisational structures.

Reports concerning the following are excluded from the Procedure's scope of application:

- disputes, claims or requests related to a personal interest of the Whistleblower, concerning exclusively the employment regulation or the relationship with roles hierarchically higher, unless they are connected with or refer to the violation of standards or internal rules/procedures;
- national security breaches, as well as contracts relating to defence or national security aspects, unless these aspects are covered by European Union secondary legislation;
- violations mandatorily regulated by European Union or national acts, as indicated in Art. 1(2)(b) of Legislative Decree No. 24/2023 (regarding financial services, products and markets, prevention of money laundering and terrorism financing, transport safety and environmental protection);
- facts or circumstances falling within the application of national or European Union provisions on classified information, forensic or medical secrecy and secrecy of the resolutions of judicial bodies, or falling within the application of national provisions on criminal procedure, the autonomy and independence of the judiciary, provisions on the functions and powers of the Superior Council of the Judiciary in matters of national defence and public order and security, as well as in matters of the exercise and protection of the right of workers to consult their representatives or trade unions, of protection against unlawful conduct or acts carried out as a result of such consultations, of the autonomy of the social partners and their right to enter into collective agreements, and of the suppression of anti-union conduct;
- conflict of interest disclosures, in accordance with the "Managing conflicts of interest in the TIM Group" procedure. If such circumstances are also relevant under the Organisational Model 231, they must be reported, as provided for in this Procedure;
- activities falling within the remit of the Security and Government Liaison Officer, relating to the handling and management of classified information pursuant to Prime Ministerial Decree No. 5 of 6 November 2015 ("Provisions for the administrative safeguarding of state secrecy and classified information and information for exclusive dissemination") and subsequent amendments;
- commercial complaints, for which references are services 119, 187, 191;
- requests to exercise personal data protection rights vis-à-vis the TIM Group ("privacy rights"), pursuant to Regulation (EU) No. 2016/679 (General Data Protection Regulation - GDPR) and Legislative Decree No. 196 of 30 June 2003 (Personal Data Protection Code) and Legislative Decree No. 101 of 10 August 2018, as amended and supplemented, for which refer to the contact details of the Data Protection Officer of the TIM Group and the "System of rules for the application of personal data protection regulations in the Telecom Italia Group" procedure. If such circumstances are also relevant under the Organisational Model 231, they must be reported, as provided for in this Procedure.

The aforementioned types of Reports will be forwarded to the relevant corporate department by TIM Audit Department, which will monitor their outcome to detect any weaknesses of the internal control and risk management system or impacts on sensitive 231 processes.

If the Report concerns areas governed by "Golden Power" regulations (for their definition refer to the Company Policy "Golden Power Guidelines and National Cyber Security Perimeter"), TIM Audit Department

discusses with Security Department of TIM, Sparkle and Telsy the deepening of aspects relating to the "Golden Power" regulations, as provided by the aforementioned Policy.

4. REFERENCES

EXTERNAL REGULATORY REFERENCES

- Legislative Decree No. 231 of 8 June 2001 ("Regulations on the administrative liability of legal persons, companies and associations, including those without legal personality, pursuant to Article 11 of Law No. 300 of 29 September 2000");
- Regulation (EU) No 2016/679 (General Data Protection Regulation - GDPR);
- Legislative Decree No. 196 of 30 June 2003 (Personal Data Protection Code) as amended and supplemented, including Legislative Decree No. 101 of 10 August 2018, as well as related legislative provisions;
- Directive (EU) 2019/1937 on the protection of persons who report breaches of European Union law ("Whistleblowing");
- Legislative Decree No. 24 of 10 March 2023, published in the Official Journal on 15.03.2023, transposing Directive (EU) 2019/1937;
- Decree Law No. 21 of 15 March 2012, converted into Law No. 56 of 11 May 2012 ("Regulations on special powers over company ownership structures in the Defence and National Security sectors, and as well as activities of strategic importance in the Energy, Transport and Communications sectors");
- Decree of the President of the Council of Ministers of 28 September 2017 (establishing that TIM is subject to the obligations set forth in the aforementioned Decree-Law No. 21/2012);
- Prime Ministerial Decree No. 5 of 6 November 2015 ("Provisions for the administrative safeguarding of state secrecy and classified information and information for exclusive dissemination") and subsequent amendments;
- Prime Ministerial Decree of 16 October 2017 imposing specific requirements and conditions on TIM, Telecom Italia Sparkle and Telsy, pursuant to Law No. 56 of 11 May 2012 on the exercise of the Government's special powers over private companies in certain strategic sectors ("Golden Power");
- Prime Ministerial Decree of 2 November 2017 ("Notice to TIM of the adoption of the Golden Power Law implementing decree");
- Decree-Law No. 22 of 25 March 2019 ("Provisions on special powers (Golden Power) inherent in broadband electronic communication services based on 5G technology");
- Decree-Law No. 64 of 11 July 2019 ("Golden Power - Regulations on special powers over company ownership structures");
- Provisions of the Council of Ministers of 5 September 2019 ("Prescriptions on 5G");
- Decree-Law No. 105 of 21 September 2019 converted into Law No. 133 of 18 November 2019 ("Urgent provisions on the National Security Perimeter and Cybernetics and the regulation of special powers in sectors of strategic importance");
- Prime Ministerial Decree No. 133 of 1 August 2022 ("New Procedural Regulations for the Exercise of Special Powers").

INTERNAL REGULATORY REFERENCES

- Organisational Model 231 of TIM and its Subsidiaries;
- Code of Ethics and Conduct of the TIM Group;
- Definition and Formalisation of Group Policies, Procedures and Operation Instructions;
- "Respecting Human Rights in the Telecom Italia Group" Policy;
- Policy on the handling of gender and sexual harassment and bullying incidents;
- Management of disciplinary proceedings for non-executive staff;
- Anti-Corruption Management System of TIM and the Subsidiaries that adopt it;
- Telecom Italia Group Anti-corruption Policy;
- "Task Risk Management" Organisational Procedure;
- Procedure "Managing conflicts of interest in the TIM Group";
- "Golden Power Guidelines and National Cyber Security Perimeter".

5. PROCESS DESCRIPTION AND LIABILITY

5.1 Purpose and process description

For Reports concerning TIM, the owner for the processing is the TIM Supervisory Body, without prejudice to the responsibilities and prerogatives of the Board of Statutory Auditors on reports addressed to it, including complaints pursuant to Article 2408 of the Italian Civil Code.

For Reports concerning Subsidiaries, the process owner is the respective Supervisory Body, without prejudice to the aforementioned liabilities and prerogatives of the relevant Board of Statutory Auditors.

In order to follow up on the Reports, the Supervisory Bodies of TIM and its Subsidiaries are supported by TIM Audit Department, in compliance with the principles established by the International Standards for the Professional Practice of Internal Auditing published by the Institute of Internal Auditors (IIA) and by the TIM Group's Code of Ethics and Conduct.

TIM Audit Department, as part of supporting activities to the Supervisory Body, also carries out the deepening investigations requested by ANAC on External Reports or Public Disclosures concerning TIM and/or its Subsidiaries, by notifying the relevant Supervisory Body.

The Departments of TIM and its Subsidiaries, which can be potentially involved in external Reports or public disclosures with external Bodies, Institutions or Authorities, promptly reach out to the TIM Audit Department for further relevant investigations.

5.2 Transmission of the Report

The recipients of this Procedure who are aware of violations must send a Report through the internal reporting channels described below.

Anyone who receives a Report, in any form (verbal or written), must send it promptly (and in any case within 7 days of receipt), to the related Supervisory Body, also through the TIM Audit Department or the internal reporting channels described below, providing simultaneous notification to the Whistleblower (if known) that it has been sent. The person who received the report must also send the original Report, including any supporting documentation, as well as evidence that the Whistleblower has been informed that the Report has been forwarded. The person who received the report cannot keep a copy of the original and he/she must delete any digital copies, without taking any independent analysis and/or investigation. They must protect the confidentiality of the identity of the Whistleblower, of the Persons involved and/or otherwise mentioned in the Report, of the Report content and of the relevant documentation.

Failure to disclose a Report received as well as breach of the duty of confidentiality shall constitute a violation of the Procedure and it could result in disciplinary action.

For the purpose of diligently following up on the internal Reports received, TIM and its Subsidiaries have implemented their own IT Portal, which can be accessed from the “Whistleblowing” page on TIM's website and those of its Subsidiaries (if activated) and on their respective corporate intranet pages.

The Portal allows to transmit, also anonymously, both an own Report and a Report received from a third party, after having read the “Privacy Notice” published on the “Whistleblowing” page of TIM's website and those of its Subsidiaries (if activated) and on the respective company intranet pages.

This Procedure is also published on the aforementioned websites and intranet pages on Whistleblowing, where information on the prerequisites for sending a Report through an internal channel, as well as information on the channels, procedures and prerequisites for sending external Reports and Public Disclosures is also available. In addition, there is a Frequently Asked Questions (FAQ) section that provides answers to the most frequently asked questions to ensure the correct transmission of Reports.

Once all the details have been filled out, the Whistleblower must remind the date and the Unique Identification Code (alphanumeric ticket that uniquely identifies the Report), which is automatically created by the Portal and allows to track the processing status of the Report over time, ensuring confidentiality and anonymity.

Reports can also be sent:

- orally, via voice messaging systems, to the freephone number indicated on the aforementioned websites

and intranet pages on “Whistleblowing” of TIM and its Subsidiaries (if activated). The oral channel is operationally managed by the TIM Audit Department, on behalf of the Supervisory Body of TIM and/or the relevant Subsidiaries, ensuring confidentiality as foreseen by this Procedure;

- by ordinary mail, addressed to the Supervisory Body 231 of TIM and/or its Subsidiaries, at the registered office of the reference company.

The Whistleblower can also request to submit an oral Report on his/her behalf through a direct meeting with a member of the Supervisory Body of TIM and/or of the relevant Subsidiaries, and/or a direct meeting with a member of the Audit Department involved to support the Supervisory Body as foreseen by this Procedure. In this case, after the Whistleblower consent, the interview is recorded on a device suitable for storage and listening or it is documented in minutes by the person who receives the report. The Whistleblower can verify, rectify and confirm by signing them.

Any Reports addressed to the Board of Statutory Auditors of TIM or of its Subsidiaries, including complaints pursuant to Article 2408 of the Italian Civil Code, received by the Supervisory Body of TIM and/or of its Subsidiaries and/or by TIM Audit Department, are promptly sent to the Board of Statutory Auditors of TIM or of its Subsidiaries. The Supervisory Body of TIM and/or of the relevant Subsidiary is entitled to perform independent deepening investigations, directly or with the support of the Audit Department, on relevant facts and circumstances of relevance pursuant to the Organisational Model 231.

Similarly, the Board of Statutory Auditors of TIM or its Subsidiaries shall send promptly, and in any case within 7 days of receipt, to the Supervisory Body of TIM or of its Subsidiaries, also through the Audit Department, any Reports received by the aforesaid company body but addressed to and/or within the competence of the Supervisory Body referred to in accordance with the Organisational Model 231, providing simultaneous notice of the submission to the Whistleblower.

5.3 Recording of the Report

All Reports, regardless of how they are collected, are registered in the Portal, which is a database where the key data of the Reports and their management (tracked by workflow) are summarized, and it also ensures the storage of all the attached documentation, as well as documents that are prepared or obtained during the analyses.

The access to information on the Portal is restricted to personnel of the Audit Department involved in supporting the Supervisory Body as foreseen by this Procedure, enabled with specific profiles of access to the system, traced through logs.

The members of the Supervisory Body of TIM and of the Subsidiaries can however access the Portal directly, through a special read-only profile, to view the Reports within their remit.

5.4 Classification and Preliminary Analysis of the Report

The Audit Department personnel involved in supporting the Supervisory Body as foreseen by this Procedure analyse and classify the Reports to define those are potentially included in the scope of this Procedure.

As part of these support activities, TIM Audit Department provides the Whistleblower via the Portal with:

- within 7 days of receipt of the Report, acknowledgement of the Report receipt;
- within 3 months of acknowledgement of the Report receipt or, in the absence of such notice, within 3 months of the expiry of the 7-day period after the report submission, feedback on the action taken or intended to be taken on the Report, specifying whether or not the Report falls within the scope of Legislative Decree No. 24/2023.

Reports of incidents of gender and sexual harassment and bullying are sent by the Audit Department to the Chief Human Resources & Organisation Office, in accordance with the "Handling of gender and sexual harassment and bullying incidents" Policy. At the end of the Report management process, the committee foreseen by the aforementioned Policy informs the Audit Department about the results of the checks performed and about any actions taken by the Chief Human Resources & Organisation Office, in order to provide information notice and closure proposal to the relevant Supervisory Body.

The Audit Department preliminarily assesses (also through document analysis, if any) if the conditions needed to start the next investigative phase have been met, prioritising Reports that are properly substantiated. The Audit Department communicates the results of the preliminary assessment to the Supervisory Body of TIM and, in case of Reports on Subsidiaries, also to the Supervisory Body of the related Subsidiary.

For the Reports within its remit, the Supervisory Body, taking into account the documents and the results of the preliminary analyses performed by the Audit Department, assesses:

- the start of the next investigation phase;
- if the "Reports on significant events" are timely communicated to the Control and Risk Committee and to the related Board of Statutory Auditors for their independent assessments;
- the closure of the Reports, insofar as: i) they are generic or not adequately substantiated; ii) they are clearly unfounded; iii) they refer to facts and/or circumstances that have already been investigated in the past and the preliminary assessment performed does not report new information that request further investigations; iv) they are "detailed and verifiable" and the preliminary assessment performed does not report elements that justify the start of a next investigative phase; v) they are "detailed and unverifiable" and, based on the results of the preliminary assessment performed, the analysis tools available do not allow to carry out further investigations to verify the validity of the Report.

In order to collect information, the Supervisory Body is entitled to:

- request the Audit Department, without prejudice to the information flows in force, to execute audits on the reported facts;
- perform in-depth investigations (also directly) in compliance with any specific applicable legislation, for instance through formal interviews with the Whistleblower, the Reported Party and/or the Persons involved in the Report and/or in any case informed of the facts. It is also entitled to request the aforesaid persons to provide informative reports and/or documents;
- engage, if needed, experts or consultants external to TIM and/or its Subsidiaries.

If the Report concerns one or more members of the Board of Directors, Board of Statutory Auditors or Supervisory Body of TIM, the Chairman of the Supervisory Body of TIM shall inform the Chairmen of the Board of Directors and Board of Statutory Auditors of TIM to manage it jointly.

If the Report involves one of the three Chairmen, he/she shall be replaced by the oldest member of the company body/Supervisory Body of TIM. If the Report involves the entire corporate body/Supervisory Body of TIM, the investigation will be handled by the Chairmen of the other two company bodies/Supervisory Bodies of TIM.

If the Report concerns the Head of the TIM Audit Department and/or the Departments he/she employs, the Chairman of the TIM Supervisory Body shall inform the Chairmen of the Board of Directors and the Board of Statutory Auditors of TIM to manage it jointly.

In the aforementioned scenarios, the results of the investigations are reported in a closing note signed jointly by the Chairmen who handled the Report.

5.5 Conducting of the investigation

The investigation phase of the Report aims to:

- perform, deepening and specific analyses to verify if there are valid grounds for the reported factual circumstances, taking into account the limits of the tools available to the Audit Department;
- assess the management and decision-making processes carried out, on the basis of the documentation and evidence collected;
- provide any suggestions on required action plans to remediate potential control weaknesses, anomalies or irregularities detected in the areas and business processes examined.

The investigation scope does not include, except within the limits of evident unreasonableness, the discretionary or technical-discretionary assessment of merit or opportunity assessments, of the decision-making and management processes performed by the corporate departments/roles involved, insofar as they are the exclusive remit of the latter.

During the investigations, the Audit Department can request additional information or clarifications from the Whistleblower. Furthermore, if it is useful for further investigation, the Audit Department can collect information from the Persons involved in the Report, who are also entitled to ask to be heard or to provide written comments or documents. In this case, the existence of the Report is communicated to the involved Person; ensuring the right of defence and the confidentiality of the identity of the Whistleblower and of the other Persons involved and/or mentioned in the Report.

The Audit Department is responsible to perform the investigation also by collecting required information from the departments concerned, involving the relevant company Departments and engaging experts or consultants external to TIM, if needed.

The investigation is performed with the support of, but not limited to: i) company data/documents useful for analysis purposes (e.g. extracts from company systems and/or other specific systems used); ii) external databases (e.g. info providers/databases on company information); iii) open sources; iv) documentary evidence collected from company departments; v) statements of involved parties or collected during interviews, if needed.

5.6 Reporting

At the end of each investigation, the results are communicated to the TIM Supervisory Body and, for Reports on Subsidiaries, also to the Supervisory Body of the relevant Subsidiary.

The results of the in-depth investigations are summarised in a report or, in the case of Reports “relating to relevant facts” and/or with complex analyses, in an investigation note which shows:

- a judgement of reasonable grounds/unfounded of the reported facts;
- the results of the activities performed, including any findings reported during previous investigations on the same or similar facts/persons detailed in the Report;
- any suggestions on the required corrective actions for the assessed business areas and processes, which are agreed with management, previously informed of the analyses results.

At the end of the investigations, the relevant Supervisory Body decides on the closure of the Report, highlighting any non-compliance with rules/procedures, without prejudice to the exclusive prerogatives and competences of the Chief Human Resources & Organisation Office as regards the exercise of disciplinary action.

Moreover, if the results of the investigation highlights:

- potential cases of criminal relevance or civil liability, the Supervisory Body can request to inform the Legal & Tax Department, which can perform its assessments;
- potential non-compliance with rules/procedures or potential disciplinary or labour law issues, the Supervisory Body can inform the Chief Human Resources & Organisation Office, which can perform its assessments and communicate the decisions taken to the Supervisory Body. In addition, TIM Chief Human Resources & Organisation Office provides the Supervisory Body with a quarterly report on the disciplinary actions taken as a result of in-depth investigations into the Reports.

Reports closed as “clearly unfounded” and not anonymous, are sent to the Chief Human Resources & Organisation Office to assess with the other competent company departments if the Report was made to impair the reputation or to damage the reported person and/or company, and to take any appropriate action against the Whistleblower, if any.

The Audit Department provides TIM Supervisory Body with a monthly summary report of all the Reports received during the period and details of those included in the Procedure’s scope. highlighting the progress and the results of the completed investigations, which could be closed.

After reporting to the TIM Supervisory Body, the Audit Department periodically provides the TIM Control and Risk Committee and the TIM Board of Statutory Auditors with a summary of the Reports received and the results of the investigations completed.

The Supervisory Body can request the disclosure of the details of the investigations performed or the investigation closing notes, also at the request of the aforementioned company bodies.

After the reporting to the Supervisory Body, the TIM Audit Department also communicates any issues reported from its investigations concerning suspected frauds with potential impacts on:

- tax matters, to the Compliance Department (Compliance Operations, within the scope of its remit), and to the Legal & Tax Department (Tax Office – Reporting and Fiscal Monitoring), to start the investigation process with the involvement of the relevant Tax Office Department, as foreseen by the TIM "Tax risk management" Procedure;
- anti-corruption matters, to the Compliance Department to prevent corruption at TIM and/or the relevant Subsidiary, identified pursuant to the Anti-Corruption Management System, in accordance with the ISO 37001 Standard, for the activities included its remit.

In addition, the Audit Department provides:

- on a half-yearly basis, the Compliance Department with an overview of the number and type of Reports received concerning potential corruption violation, to prevent corruption at TIM and at the relevant Subsidiaries;
- on a half-yearly basis, the TIM Chief Regulatory Affairs Department with an overview of the number and type of Reports received concerning suspicious conduct or potential violations of competition law and TIM Group Antitrust Code of Conduct;
- annually, the TIM Sustainability Department with information needed to prepare the TIM Group Sustainability Report, with special reference to Reports included in the scope of the "Respecting Human Rights in the Telecom Italia Group" Policy.

5.7 Corrective Actions: Monitoring

If the analyses performed on the business areas and processes lead to recommendations to define appropriate remediation actions, management in charge of the areas/processes in scope is responsible to define them to address the critical detected issues. Management is also responsible to ensure their implementation in line with the defined deadlines and to update the Audit Department, which monitors the implementation status of the actions.

The relevant Supervisory Body monitors the progress of corrective actions based on information periodically provided by the Audit Department.

5.8 Personal data processing and retention of documentation

All personal data processing, including the one performed in the Portal, is carried out in compliance with the confidentiality obligations pursuant to Article 12 of Legislative Decree No. 24/2023 and in accordance with the personal data protection regulations referred to in Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR), Legislative Decree No. 196 of 30 June 2003 and Legislative Decree No. 51 of 18 May 2018.

Personal data protection is ensured not only for the Whistleblower (for non-anonymous reports), but also for the Facilitator as well as the Person involved or mentioned in the report.

Potential involved parties are provided with the notice on the personal data processing published on the dedicated portal.

In compliance with Art. 13(6) of Legislative Decree No. 24/2023, a Privacy Impact Assessment (PIA) was performed in line with the Art. 35 of Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR), to define the technical and organisational measures needed to reduce the risks which could impact the rights of data subjects, including the security measures needed to prevent unauthorised or unlawful processing.

In order to ensure the management and traceability of Reports and activities, the Audit Department prepares and updates all information concerning the Reports and ensures, with the support of the Portal, that all the related supporting documentation is stored for the time strictly necessary for their definition, and in any case for no more than 5 years from the notification date of the final outcome of the Report to the Supervisory Body

Personal data that are clearly not useful for processing a specific report, are not collected or are promptly deleted, if accidentally collected.

The original reports received in paper form are archived in a secure environment.

5.9 Periodic checks

On a six-monthly basis, a completeness check is performed by members of the Audit Department, other than those involved in supporting the Supervisory Body as foreseen by this Procedure, to verify that all the Reports received have been processed, duly forwarded to the relevant addressees and reported in accordance with this Procedure.

6. GUARANTEES AND SAFEGUARDS

6.1 Protecting the identity of the Whistleblower

Reports may not be used for any purpose other than the actions needed to adequately follow them up.

Without prejudice to legal obligations, the Whistleblower's identity and any other information from which that identity could be directly or indirectly inferred, cannot be disclosed without his/her express consent, to persons other than those responsible for receiving or following up on the Reports, clearly authorised to process these data pursuant to Articles 29 and 32(4) of Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR) and Article 2-*quaterdecies* of Legislative Decree No. 196 of 30 June 2003 (Personal Data Protection Code).

In particular, the Whistleblower's identity and any other information from which that identity could be directly or indirectly inferred, can be disclosed only with the Whistleblowers express consent in case of:

- disciplinary proceedings, if the dispute is fully or partially based on the Report and the Whistleblower's identity is crucial for the accused's defence;
- proceedings started due to internal or external Reports, if the disclosure of the Whistleblower's identity or of any other information from which that identity could be directly or indirectly inferred is also crucial for the defence of the Person concerned.

For this purpose, the reasons for the confidential data disclosure are communicated in advance by written notice to the Whistleblower. .

TIM Group personnel involved in handling the Reports must protect the confidentiality of the identity of the Whistleblower, of the Persons involved and/or otherwise mentioned in the Report, of the content of the Report and of the relevant documentation.

Confidentiality is also guaranteed if the Whistleblowers send the report before the start of employment or after the termination, or during the probation period, if such information was obtained in the working environment or during the selection or pre-contractual phase.

Confidentiality is also guaranteed on the identity of the Persons involved and/or mentioned in the Report, as well as for the identity and support provided by the Facilitators, with the same guarantees provided for the Whistleblower.

A violation of the confidentiality obligation, except as above, could result in administrative fines by ANAC against the person concerned, as well as disciplinary actions by the Chief Human Resources & Organisation Office, in line with the paragraph 8 of the Organisational Model 231 ("Disciplinary System").

6.2 Protection Measures

Retaliation against the Whistleblower is forbidden, understood as any conduct, act or omission, even if only attempted or threatened, carried out as a result of the internal or external Report/Public Disclosure/complaint, which directly or indirectly causes or may cause the Whistleblower unfair damage.

Protection is also granted to the anonymous Whistleblower, who believes he or she has been identified and suffered retaliation .

The protection measures apply within the limits and conditions provided for in Chapter III of Legislative Decree No. 24/2023 and are also extended to:

- categories of Whistleblowers that are not within the scope of objective and/or subjective application provided for by Legislative Decree No. 24/2023;
- Facilitators, people in the same work environment as the Whistleblower who are linked to the latter by a stable emotional or family relationship up to the fourth degree, the Whistleblower's colleagues who operate in the same work environment and have a regular and current relationship with the Whistleblower;
- entities owned by or for which the Whistleblower works, as well as entities operating in the same work environment as the Whistleblower.

Those who believe they have suffered retaliation because of the Report may notify ANAC.

Any retaliatory acts taken as a result of the Report are null and void, and people who have been dismissed as a result of the Report entitled to be reinstated in their jobs, in accordance with the rules applicable to the worker.

Without prejudice to the exclusive competence of ANAC regarding the application of the administrative fines referred to in Article 21 of Legislative Decree No. 24/2023, reference is made to the specific rules in paragraph 8 of the Organisational Model 231 ("Disciplinary System") for any disciplinary consequences within the remit of the Chief Human Resources & Organisation Office.

7. GLOSSARY

For the purposes of this Procedure, the following are understood to mean:

- **Work environment:** past or present work or professional activities carried out by TIM Personnel or Third Parties within the scope of the legal relations they have established with TIM S.p.A. (hereinafter TIM) and/or with Subsidiaries;
- **Public disclosure:** making information about violations publicly available through print or electronic media or otherwise through means of dissemination capable of reaching many people. Pursuant to Article 15(1) of Legislative Decree No. 24/2023, the Whistleblower may make a public disclosure if one of the following conditions is met (i) he/she has already made a Report, either internally or externally, or has made an external Report directly and has not received feedback within the set time limits as to the measures envisaged or taken to follow up on the Reports; (ii) he/she has well-founded reasons to believe that the breach may constitute an imminent or obvious danger to the public interest (iii) he/she has well-founded reasons to believe that the external Report may entail a retaliation risk or may not be effectively followed up due to the specific circumstances of the case, such as where evidence may be concealed or destroyed, or where there is a well-founded fear that the recipient of the Report may be in collusion with the perpetrator of the breach or actually involved in the breach;
- **Facilitator:** the natural person who assists the Whistleblower with the Whistleblowing process and who works in the same work environment and whose assistance must be kept confidential;
- **TIM Group:** TIM and/or its subsidiaries;
- **Information on violations:** adequately substantiated information, including well-founded suspicions, concerning violations resulting from conduct, acts or omissions that have been committed or are likely to be committed, as well as elements concerning conduct, including omissions, aimed at concealing such violations. This also includes information on violations obtained in the context of a legal relationship that has not yet commenced or has meanwhile ended, if such information was obtained in the work environment, including the probation period, or during the selection or pre-contractual phase;
- **Organisational Model 231:** the organisation, management and control model adopted by TIM and its Subsidiaries pursuant to Legislative Decree no. 231/2001;
- **Supervisory Body:** the TIM Body, or the Board of Statutory Auditors of the Subsidiaries in the capacity of the Supervisory Body, appointed pursuant to Article 6(1)(b) of Legislative Decree no. 231/2001, with autonomous initiative and control powers, responsible for supervising the operation of and compliance with the Organisational Model 231 and ensuring that it is updated;
- **Person involved:** the natural or legal person mentioned in the Report made through the internal or external channel, complaint or Public Disclosure, as the person to whom the violation is attributable or in any case referable;
- **TIM personnel:** those who are linked to TIM or its Subsidiary Companies by an employment relationship or the provision of occasional services, as well as Top Management and members of the company bodies and of TIM Supervisory Body and its Subsidiary Companies (even where they perform such functions on a purely de facto basis);
- **Whistleblower:** the person who makes a Report via the internal or external Report channel, complaint or Public Disclosure;
- **Report:** written or oral communication of information referable to TIM Personnel and/or Third Parties concerning violations of laws and regulations, of the Code of Ethics and Conduct of the TIM Group, of the Organisational Model 231, as well as of the system of rules and procedures in force within the TIM Group, including - but not limited to - the Policy on "Respecting Human Rights in the Telecom Italia Group", the "Task Risk Management" Procedure, the TIM Anti-Corruption Management System, and the Telecom Italia Group Anti-Corruption Policy;
- **Anonymous reports:** A Report in which the identity of the Whistleblower is neither made explicit nor is

unambiguously identifiable;

- **Substantiated report:** Report in which the information/assertions contain a sufficient level of detail, at least in the abstract, to reveal circumstances and facts that are specific and concordant and related to specific contexts, as well as to make it possible to identify elements useful for the purpose of verifying the merits of the report itself (for example, elements that make it possible to identify the person who has committed the reported facts, the context, the place and time when the reported circumstances took place, the value, causes and purpose of the conduct, anomalies relating to the internal control system, supporting documentation, etc.). Within the scope of substantiated Reports, a distinction is made between information/assertions that are: i) “verifiable”, if on the basis of the Report's contents it is actually possible to check their veracity within the company, within the limits of the activities and with the analysis tools available to the Audit Department; ii) “not verifiable”, if on the basis of the analysis tools available, it is not possible to check the veracity of the Report. Checks on circumstances and evaluations that can be traced back to intentional and/or subjective elements are affected by the limitations inherent in audit work and the tools available;
- **External Report:** written or oral communication of information on violations made by the Whistleblower through the external reporting channel activated by the National Anti-Corruption Authority (ANAC). Pursuant to Article 6(1) of Legislative Decree No. 24/2023, the Whistleblower may make an external Report if one of the following conditions is met i) there is no mandatory activation of the internal reporting channel in his/her work environment, or this channel, even if mandatory, is not active or, even if activated, it is not compliant; ii) he/she has already made an internal Report and it has not been followed up; iii) he/she has well-founded reasons to believe that, if he/she made an internal Report, it would not be effectively followed up on or would lead to retaliatory conduct; iv) he/she has well-founded reasons to believe that the violation may represent an imminent or obvious danger to the public interest;
- **Internal reporting:** written or oral communication of information on violations made by the Whistleblower through the internal channel;
- **Reports of relevant facts:** i) Reports concerning top management and members of the company bodies and of TIM Supervisory Body and/or its Subsidiaries; ii) Reports in respect of which, even on the basis of preliminary analyses, serious breaches of the Organisational Model 231 are likely to occur, such as to expose the company to the risk of criminal-administrative liability under Legislative Decree No. 231/2021; iii) Reports of corporate operational anomalies and/or offences and/or frauds and/or abuses for which, at the end of the preliminary analysis, a significant quali-quantitative impact on the financial statements can be estimated for TIM and/or its Subsidiaries (in terms of accounting issues, statutory audits, internal controls on financial reporting). The impact is qualitatively “significant” if operational anomalies and/or frauds and/or abuses can influence the economic and investment decisions of potential recipients of financial reporting. The quantitative significance of the impact is assessed by the Supervisory Body in agreement with the Chief Financial Office of the relevant company;
- **Subsidiaries:** the subsidiaries of the TIM Group, excluding listed and foreign companies, to which this Procedure applies directly;
- **Third parties:** natural or legal persons, other than TIM Personnel, who have, for various reasons, employment, collaboration or business relations with TIM and/or its Subsidiaries, including - but not limited to - customers, partners, suppliers (including contractors/subcontractors) self-employed workers or those with collaborative relationships, freelancers, consultants, agents and intermediaries, volunteers and trainees (whether paid or unpaid), or anyone who has a legitimate interest in the TIM Group's business activities.