Whistleblowing Procedure

Contents

1. INTRODUCTION

The term "*whistleblowing*" (hereinafter "*Whistleblowing*") means any report made by any person concerning conduct (of any nature, including just omissions) by TIM Staff and / or third parties that does not comply/infringes laws and regulations, the Code of Ethics and the Organizational Model 231, as well as the system of rules and procedures in force within the Group, including but not limited to: the Policy for the Respect of Human Rights, the Tax Risk Management Procedure, the TIM Anti-Corruption Management System and the Group Anti-Corruption Policy.

One of the purposes of this procedure (hereinafter "Procedure") is also to implement law no. 179 of 30 November 2017 ("*Provisions for the protection of Whistleblower reporting offences or irregularities that have come to their knowledge as part of public or private employment*") which, in order to protect employees who report alleged offences, has introduced rules for *whistleblowing* in the private sector, by modifying Legislative Decree no. 231/2001 on the "administrative" liability of entities.

The aforementioned legislation envisages in particular: i) the setting up of one or more channels (including one IT channel) for the submission of detailed reports, structured in such a manner as to ensure the confidentiality of the Whistleblower; ii) the prohibition of retaliatory or discriminatory acts, both direct and indirect, against the Whistleblower for reasons that are directly or indirectly connected to the report; iii) disciplinary sanctions for those who infringe the protection measures in favour of Whistleblowers and for those who make fraudulent or grossly negligent reports that prove to be unfounded.

TIM Group personnel involved in the management of *whistleblowing* is required, within the limits established by law, to the confidentiality of the content of the report, and of the identity of the Whistleblower, the reported party and the other parties involved. The Procedure also applies to anonymous reports, where these are adequately detailed, i.e. where they can identify facts and situations by relating them to specific contexts.

For an efficient management of *whistleblowing*, TIM has set up a *Whistleblowing* Portal (in short "Portal"), also for TIM subsidiaries (with the exception of listed companies and foreign companies, other than Telecom Italia San Marino S.p.A. and Telefonia Mobile Sammarinese S.p.A.), each of which can access the Portal to view the reports within their remit. The Portal was implemented in such a way as to prevent access to unauthorized persons, and also provides for different types of access profiles (viewing, editing, etc.) traced through the system logs.

2. RECIPIENTS

The Recipients of the Procedure are:

- the senior management and the members of the corporate bodies and the Supervisory Board of TIM and the national subsidiaries of the TIM Group, of the TIM Foundation, of Telecom Italia San Marino S.p.A. and of Telefonia Mobile Sammarinese S.p.A. (hereinafter collectively the TIM Entities);
- all employees of TIM, of TIM entities, the partners, customers, suppliers, consultants, collaborators, shareholders who have information regarding the conduct defined in the Introduction.

3. PURPOSE AND SCOPE OF APPLICATION

The process is part of the ETOM Business Process Framework in:

1. L0 Enterprise Management
2. L1 - Enterprise Risk Management

The Procedure aims to regulate the process of receiving, analysing and managing *whistleblowing* reports, sent or transmitted from any person, also anonymously (management also includes the storage and subsequent cancellation of both the reports and all the relevant documentation, as specified in the following paragraph 6.2.6).

The Procedure applies to TIM and TIM Entities, which ensure its correct and ongoing application, as well as its dissemination internally to the maximum extent possible, in compliance with the confidentiality obligations and prerogatives of autonomy and independence of each Company.

The Procedure is also a reference for TIM subsidiaries other than TIM Entities, which can implement it, subject to compliance with their specific and/or local regulations, processes and organizational structures.

The scope of the Procedure does not include the activities of the Security Function, relating to the processing and management of classified information pursuant to Prime Ministerial Decree no. 5 of 6 November 2015 ("Provisions for the administrative protection of state secrecy and classified information intended for exclusive dissemination"), as amended.

In the event of reports concerning the activities governed by the Golden Power regulations[1], subject to specific supervision and control by TIM, Sparkle and Telsy Security Organizations, the "*Golden Power Guidelines*" company policy applies, which provides for the activation of consultation mechanisms between the Audit Department and the Safety Organizations for the launch of verification activities.

Reports concerning the following matters are excluded from the scope of the Procedure:

- communications relating to conflict of interest, pursuant to the relevant procedure;
- security issues, for which reference is made to the specific existing information channels, namely:
  - Ermes, for the reporting of security incidents affecting human resources, tangible and intangible assets (such as, for example, software malfunctions, corporate network failures, loss or accidental destruction of documents, ICT security incidents, thefts).
  - Travel Security, for requesting information and for reporting in relation to travel abroad;

[1] **Prime Ministerial Decree 16/10/2017**: i) governance processes, with specific reference to all decision-making processes relating to strategic activities and to the network; ii) control and supervision of all the activities, carried out in the various company areas, relating to the management of relevant assets for defence and national security purposes; iii) disclosure on the establishment in the national territory of management and security functions of the networks and of supplies that support strategic and key strategic activities as well as SOC, CERT, DOC, NOC, IOC and other data centers and / or logical and IT security devices to ensure the confidentiality and integrity of company data; iv) information on any decision that may reduce, even temporarily, or transfer technological, operational and industrial capacities in the "strategic activities" and in the "key strategic activities", including the sale of company shares, ownership rights or legal titles, of technological, operational or industrial capacity, limiting in practice the degree of autonomy of the Company.
Prime Ministerial Decree 2/11/2017: i) information on any change and reorganization of the corporate structures of TIM S.p.A. and its direct or indirect subsidiaries; ii) information on any plan for the disposal or sale of strategic activities or Board of Directors' resolutions that may have an impact on the security, availability and functioning of the networks and plants and on the continuity of the universal service.
Prime Ministerial Decree 5/09/2019: specific Prescription Decree applied to TIM on the subject of "Broadband electronic communication services based on 5G technology. Specifically: i) governance processes with regard to decision-making processes, also of a technical nature, relating to activities that are deemed relevant under art. 1-bis of Decree-Law no. 21 of 15 March 2012".

- online abuse, for reporting conduct or events attributable to cases of abuse in the use of the network services offered by TIM, such as for example spam, virus and malware spread and, cyber attacks, phishing and identity theft, publication or dissemination of offensive, subversive, child pornography material, unless these offences fall within the cases envisaged by Organizational Model 231 (in which case they must be treated as reports governed by the Procedure);
- commercial complaints, for which reference is made to the 119, 187, 191 services, as well as to the internal channel “Chi-ama Telecom Italia".

The reports that fall within the aforementioned categories, included in the Portal, will be forwarded to the relevant Functions by the Audit Department, which in any case monitors the outcome in order detect any weaknesses in the internal control and risk management system.

4. GLOSSARY

- TIM staff: refers to the employees, with permanent and fixed-term contracts (managers, middle managers, white-collars, blue-collars) of TIM and of the TIM entities.
- Third parties: means all those who, in various capacities, have work, collaboration or business relationships with TIM and / or the TIM entities, including collaborators, interns, leased staff, consultants, agents, intermediaries, suppliers and businesses partners, in relation to work, collaboration or business services with TIM or the TIM entities.
- Supervisory Board of TIM Entities: means the Supervisory Board set up pursuant to art. 6, (1)(B) of Legislative Decree no. 231/01, or the Board of Statutory Auditors acting as Supervisory Board.
- TIM Entities: means the national subsidiaries of the TIM Group, the TIM Foundation, Telecom Italia San Marino S.p.A. and Telefonia Mobile Sammarinese S.p.A, to which the Procedure applies directly.
- Whistleblower: any person making a Report.
- Reporting/report/*whistleblowing*: means any disclosure concerning conduct (including just an omission) by TIM staff or by third parties, related to the performance of work or collaboration activities for TIM or the TIM entities, which infringes laws and regulations and/or is not compliant with the Code f Ethics and the Organizational Model 231, as well as with the system of rules and procedures in force within the Group, including, by way of example but not limited to: the Policy for the Respect of Human Rights, the Tax Risk Management Organizational Procedure, the TIM Anti-Corruption Management System and the Group Anti-Corruption Policy.
- Anonymous reporting: Reporting in which the personal data of the Whistleblower are not disclosed, nor are they uniquely identifiable.
- Reporting made with wilful misconduct or gross negligence: Reporting that, based on further investigation, turns out to be devoid of factual confirmation and which has been made while being fully aware of the absence of any breach or non-compliance or of the non-involvement of the reported party, or with gross negligence in the assessment of the facts.
- Detailed reporting: Reporting in which the statements (e.g. reference period, place, value, causes and purposes, elements that consent an identification of the person who carried out the acts in questions, anomalies relating to the internal control system, supporting documentation, etc.) are characterized by a degree of detail that is sufficient, at least in theory, to identify precise and concordant facts and situations, by relating them to specific contexts, and which also consent the identification of elements that are useful to verify whether the Reporting is well-founded. Detailed Reporting in turn can be broken down into:
    - verifiable detailed reporting: if, considering the contents of the Reporting, it is possible in practice, on the basis of available investigation tools, to carry out checks on the validity of the Reporting within the company;
    - unverifiable detailed reporting: if during the preliminary checks it becomes clear that, on the basis of the available investigation tools, it is not possible to carry out checks on the validity of the Reporting.

- Reporting regarding material facts: Reporting of corporate operating anomalies and/or wrongdoings and/or frauds and/or abuses:
  - for which, as a result of a preliminary check, a material qualitative-quantitative impact on the financial statements (in terms of accounting issues, statutory audit of the accounts, internal controls on financial reporting)[2] can be estimated for TIM S.p.A. and / or for its subsidiaries and / or
  - which concerns Chairmen, Chief Executive Officers and members of the governing and / or control / supervisory bodies of TIM and of the TIM entities and / or breaches of Model 231.

5. REFERENCES

- Legislative Decree no. 231/01 which governs "the administrative liability of legal persons, companies and associations, including those without legal personality, in accordance with article 11 of law no. 300 of 29 September 2000".
- Regulation (EU) no. 2016/679 on the protection of personal data (GDPR).
- Legislative Decree no. 196/03 as amended and supplemented, and the related legislative provisions.
- Law no. 179 of 30 November 2017,"Provisions for the protection of whistleblowers reporting offences or irregularities that have come to their knowledge as part of public or private employment".
- Prime Ministerial Decree of 16 October 2017 which imposes specific prescriptions and conditions on TIM, Telecom Italia Sparkle and Telsy, pursuant to law no. 56 of 11 May 2012 on the exercise of special government powers over private companies in certain strategic sectors ("Golden Power").
- Prime Ministerial Decree 02/11/2017 - Notice to TIM of the adoption of the decree implementing the Golden Power law.
- Prime Ministerial Decree 16/10/2017 - Notification to TIM of the decree implementing the Golden Power law.
- Council of Ministers measure of 5-09-2019 - 5G requirements.
- Decree Law no. 22/2019 - Provisions on special powers (Golden Power) pertaining to broadband electronic communications services based on 5G technology.
- Decree Law no. 64/2019 - Golden Power - Rules on special powers over corporate structures.
- Prime Ministerial Decree no. 5 of 6 November 2015 - Provisions for the administrative protection of state secrecy and classified information intended for exclusive dissemination, as amended.

The TIM's internal documents are:
- The 231 Organisational Model of the TIM Group (comprehensive of the Code of Conduct and Ethics).
- Development of Organisational Identity - New Values of Telecom Italia (Code 2015-00155).
- Anti-corruption management system.
- Group Anti-corruption Policy.
- Organizational Procedure "Evaluation of contingent liabilities arising from suspected fraud with tax impacts" (Code 2016-00177).
- Definition and Formulation of Group Policies, Procedures and Operating Instructions (Code 2014-00152).
- Telecom Italia Group Anti-corruption Policy (Code 2012-00234).
- Telecom Italia Group procedure for the management of Conflict of Interest (Code 2013-00154).
- Respecting Human Rights in the Telecom Italia Group (Code 2015-00193).
- Management of disciplinary proceedings for non-executive staff (Code 2020-00017).
- Golden Power Guidelines, issued on 6 April 2020 (Cod. 2018-00026).

[2] The materiality of the impact from a quantitative standpoint is assessed by the Supervisory Board in agreement with the Chief Financial Office. The impact is qualitatively material if the operational anomalies and/or the frauds and/or the abuses are capable of affecting the economic and investment decisions of the potential recipients of the financial information.

6. DESCRIPTION OF THE PROCESS AND RESPONSIBILITIES

6.1 Purpose and brief description of the process

As part of TIM's new *Business Process Framework*, the process for the management of *Whistleblowing*, the principles, responsibilities and activities of which are described in the following paragraphs, is part of the L0 *ENTERPRISE MANAGEMENT* area with the following reference: L1 *Enterprise Risk Management*, L2 *Audit Management*.

For Reports concerning TIM S.p.A., the owner of the management process is TIM's Supervisory Board, subject to the responsibilities and prerogatives of the Board of Statutory Auditors for the reporting addressed to it, including the reports under Article 2408 of the Italian Civil Code.

Any Reporting concerning the Head of the Audit Department of TIM and/or its Functions will be sent without delay to the other members of the Supervisory Board.For Reports concerning TIM Entities, the process owner is the respective Supervisory Board, without prejudice to the aforementioned responsibilities and prerogatives of the Board of Statutory Auditors.

The management of *Whistleblowing* is carried out with the support of the Audit Department of TIM S.p.A. or the Audit Function of the TIM Entity, if present, in compliance with the principles established by the International Standards for the Internal Audit profession and by the Code of Ethics issued by the Institute of Internal Auditors (IIA), as well as by the Code of Ethics and Conduct of the TIM Group.

6.2 Process input/output

The process inputs are:

- Entering in the Portal the Report submitted by employees, collaborators, consultants, workers, partners and third parties.
- Obligation for employees who receive the Report from TIM Staff or from third parties to insert it on the Portal.

The process outputs are:

- Processing of the Report and cancellation of Reports and related documentation after 10 years.

6.2.1 Sending the Reports

Description

TIM staff who becomes aware of a conduct similar to those described in the previous paragraphs are required to Report it in the manner specified below.
The Reports must be sent through the Portal, which is available both in the Intranet and Internet environment https://portalesegnalazioni.telecomitalia.it, having previously read the "Privacy Policy" (Annex 1), or sent to the email address "*Whistleblowing* mailbox, Telecom Italia SpA, Via Gaetano Negri, 1, 20123 Milan".
When the Report is entered via the Portal, a special Frequently Asked Questions (FAQ) section is available for the Whistleblower, which contains the answers to the most frequently asked questions in order to ensure the correct registration of the Reports, as well as a list of types of communications that fall outside the scope of the Procedure, in order to ensure they are correctly addressed.

Reports regarding TIM entities must be entered in the Portal or sent to the e-mail boxes listed in Annex 3. Any Reports addressed to the Board of Statutory Auditors of TIM (including complaints under art. 2408 of the Italian Civil Code) entered in the Portal or in any case received by the Supervisory Board or by the Audit Department will be handled by the latter and sent to the Corporate Affairs Function (within the Legal and Tax area) for subsequent submission to TIM's Board of Statutory Auditors. Similarly, the Corporate Affairs

Department will enter into the Portal any Reports received by the Board of Statutory Auditors but addressed to and/or within the remit of the Supervisory Board.
TIM staff who receive a Report by external or internal mail, e-mail or fax are required to immediately enter it on the Portal, sending the original to the Audit Department along with any supporting documentation. The recipient cannot keep a copy of it and must refrain from undertaking any independent analysis and/or investigation. Failure to disclose a Report that has been received is a breach of the Procedure and may lead to the adoption of appropriate actions, including of a disciplinary nature.
In managing the Reports, the confidentiality of the content and of the whistleblower's identity is guaranteed, except in the following cases:

- if the whistleblower is found, including by judgment rendered by a first instance court, criminally liable for slander or defamation crimes or in any case for crimes committed in making the Report, or civilly liable for the same offences in cases of wilful misconduct or gross negligence;
- in response to requests from the judicial authorities or other entitled parties.

Breach of the obligation of confidentiality (without prejudice to the above exceptions) may result in adoption of the actions from time to time applicable including disciplinary actions.
It is forbidden to carry out retaliatory or discriminatory acts, whether direct or indirect, against Whistleblowers who make a Report pursuant to the Procedure, for reasons directly or indirectly connected to the Report. Any retaliatory or discriminatory dismissal of the Whistleblower is void. Likewise is null any change of duties under article 2103 of the Italian Civil Code, as well as any other retaliatory or discriminatory measure adopted against the Whistleblower. The adoption of discriminatory measures against the Whistleblower can be reported to the National Labour Inspectorate, for the relevant actions, not only by the Whistleblower but also by his/her trade union organization.

If an employee believes that he or she has suffered any of the aforementioned wrongdoings due to having submitted a Report, he or she can inform the Audit Department through the Portal. The aforementioned Department will promptly inform the Human Resources Function for the necessary investigation and potentially the commencement of disciplinary proceedings against the person responsible for the discrimination or retaliation.

For the consequences of retaliatory and/or discriminatory acts, whether direct or indirect, carried out against the employee who made the Reporting, for reasons connected, even indirectly, to the Reporting and for the regulation of sanctions that can be adopted against those who breach the whistleblower protection measures or those who acting fraudulently or with gross negligence submit a Report that is subsequently found to be groundless, reference is made to the specific rules contained in paragraph 8 ("*Disciplinary System*") of the Organizational Model 231.

6.2.2 Registration and classification

Description

All Reports, regardless of how they are received, are recorded in the Portal, which is the database that gathers the essential data of the Reports and their processing (tracked through workflow) and which also ensures the archiving of all the attached documentation, as well as of the documents produced or acquired during the investigation activities.
After registration, the Audit Department analyses and classifies the Reports, in order to limit processing to those Reports that fall within the scope of the Procedure.
For each Report, the Portal assigns a unique identification code that allows each Whistleblower to check the processing status, in a completely anonymously way.
If it is considered that a Report is not adequately detailed, the Audit Department may request further details from the Whistleblower, according to the methods specified below:

- if the Whistleblower has provided a contact (email, telephone, etc.), through such contact;
- in no contact has been provided, through a specific message entered in the Portal, which the Whistleblower may view using the Report identification code.

6.2.3 Preliminary analysis of the Report

Description

The Audit Department carries out a preliminary analysis of the Reports, in order to identify those to be forwarded to specific recipients to whom they are addressed, those potentially relevant pursuant to Legislative Decree 231/01, those relating to breaches of the Code of Ethics, those relating to management / operational events to be sent to the relevant corporate units. In addition, it assesses, on a preliminary basis, including through a documentary analysis, whether the conditions are met for starting the next preliminary investigation phase, and proposes to the Supervisory Body the archiving of generic Reports and of Reports lacking any informative element.

All Reports are disclosed to the Supervisory Board which, on a documentary basis and also considering the results of the preliminary analyses carried out by the Audit Department, evaluates:

i) for Reports concerning TIM S.p.A:
a) whether to start the subsequent investigation phase; b) whether there has been any breach of rules / procedures, to be also disclosed to Human Resources for the relevant analysis; c) the relevance of the Report (Reports relating to material facts), for the purpose of disclosing it to the Chairman, the CEO, the Chairman of the Board of Statutory Auditors and the Chairman of the Control and Risk Committee of TIM.

The following Reports are archived by the Supervisory Board: i) generic Reports and/or non-"detailed Reports"; ii) patently groundless Reports; iii) Reports containing facts already subject to specific preliminary investigations in the past and already closed, if no new information is found during the preliminary checks carried out that would warrant further investigation; iv) "Verifiable circumstances" for which, in light of the results of the preliminary checks carried out, no elements are found that would support the start of the next investigation phase; v) “Non-verifiable circumstances" for which, in light of the results of the preliminary checks, it is not possible to carry out, on the basis of available investigation tools, further checks on the truthfulness of and/or the existence of valid grounds for the Report.

The Reports filed as clearly unfounded are sent to the Human Resources Department, in order for the latter to assess, with the other corporate units concerned, whether the Report was made for the sole purpose of damaging the reputation of, or of causing damage or detriment to the reported person and/or company, for the purpose of taking any appropriate action against the Whistleblower;

ii) for Reports concerning one or more TIM Entities:
the sending of the Report to the Supervisory Board of the TIM Entity for the necessary actions.

6.2.4 Specific inquiries

Objectives and characteristics of the investigation

The objective of investigating the Reports is to carry out, within the limits of the tools available to the Audit Department, specific checks, analyses and assessments regarding the reasonable grounds of the factual circumstances reported, as well as to provide any indications regarding the adoption of the necessary corrective actions in the concerned company areas and processes.

The investigation aims to reconstruct the management and decision-making processes involved, on the basis of official documentation and information as well as on documentation and information made available. The substance of management decisions or of discretionary or technical-discretionary decisions, from time to time made by the company managers involved, falls outside the scope of analysis of the investigation, except in case of manifest unreasonableness.

Performing the investigation

The Audit Department oversees the investigation, also by acquiring the necessary information elements from the concerned units, by involving the relevant Company Functions and by relying on external experts

where deemed appropriate. The above is without prejudice to the disciplinary responsibilities of the Human Resources Department.

With regard to Reports concerning frauds with possible tax impacts, the Audit Department, in application of the provisions of the Task Risk Management Organizational Procedure, forwards the Reports to the Compliance Operations Department for follow-up and for subsequent disclosure of the related outcomes to the Audit Department.

The tools used for investigation activities include but are not limited to:
- business data / documents that may be useful for the investigation (e.g. extractions from SAP business systems and / or other specific systems used);
- external databases (e.g. info providers / databases on corporate information);
- open sources;
- documentary evidence obtained from company units;
- where appropriate, statements made by the concerned parties or obtained during interviews, that were recorded and signed.

In order to obtain informative elements, the Supervisory Board has the right (i) to request that TIM Audit Department, without prejudice to current information flows, activate a "Spot" audit on the reported facts; (ii) to carry out further analyses, also directly, through, for example, formal summons and hearings of the Whistleblower, of the reported party and / or of other parties mentioned in the report as being aware of the facts, as well as by requesting the aforementioned persons to produce information reports and/or documents.

At the end of the investigation, the Audit Department prepares a report on:
- the activities carried out, their results, as well as the results of any previous investigations carried out on the same facts or on events similar to those covered by the Report;
- an opinion of whether the reported facts are reasonably well-founded, along with any indications regarding the adoption by the relevant management - who is informed of the investigation results - of the necessary corrective actions on the company areas and processes affected by the Report.

If, at the outcome of the investigation, it is found that the facts under investigation may be relevant from a disciplinary point of view or, in any case, they involve employment law issues, the final report containing the results of the activities is also sent to the Head of the Human Resources Department, for the relevant ass essments. Similarly, if the investigation shows that the events may potentially involve criminal or civil offences, the results of the investigation are sent to the Legal & Tax Department for the relevant assessments.

The investigations of reported facts for which it is known that investigations by public authorities are ongoing (for example: judicial, ordinary and special authorities, administrative bodies and independent authorities, vested with supervisory and control functions) are subject to the preliminary assessment of the relevant corporate functions, in order to ascertain whether the internal investigation is compatible with said public investigation / inspection activities. The Chairman and the CEO of TIM are informed of the results of the guidelines adopted by the relevant corporate function.

At the end of the investigation, the Supervisory Board resolves the closure of the case, noting any breach of rules / procedures, without prejudice, as regards the exercise of disciplinary action, to the exclusive prerogatives of the Company, which will inform the Supervisory Board of the decisions made.

If the Report concerns one or more members of the Board of Directors, the Board of Statutory Auditors or the Supervisory Board of TIM, the investigation will be handled jointly by the respective Chairmen. If one of the three Chairmen is called into question, he/she will be replaced by the oldest member of the body or of

the Supervisory Board. In the entire body or the entire Supervisory Board is involved, the investigation will be managed by the Chairmen of the other two bodies / Supervisory Board. In such cases, the results of the investigation will be notified to the Board of Directors, the Board of Statutory Auditors and the Supervisory Board for the matters within their remit.

Monitoring of Corrective Actions

If the investigation shows the need for corrective actions, the management of the investigated areas / processes will be responsible for developing a plan of corrective actions designed to resolve the critical issues detected. The Supervisory Board monitors the implementation status of the Plan with the support of the Audit Department, and provides information in this regard in the periodic reporting referred to in the following paragraph.
The management will be required to update the implementation status of the corrective actions at least quarterly (depending on the type / extent of the corrective actions).

6.2.5 Disclosure of results

Description

The results of each investigation carried out are contained in a report prepared by the Audit Department and sent to the Supervisory Board as well as to the corporate units concerned so that they can take any relevant action.
In material cases (see definition in the Glossary), the Supervisory Board assesses whether the aforementioned investigation is to be sent to the Company's top management and Control Bodies. In the same cases, it also assesses whether the report is to be sent to the company units concerned.
In addition, the Audit Department provides the Supervisory Board with a monthly progress report on all the Reports received and which fall within the scope of the Procedure, along with the results of the investigations carried out.

Similarly, on a quarterly basis, the Human Resources Function provides the Supervisory Board and the Board of Statutory Auditors with information on the disciplinary measures taken following the investigation of the Reports.

In order to allow the Board of Statutory Auditors a timely information about the issues subject to Reports, the Audit Department also sends, on a monthly basis, to the Chairman of the Board of Statutory Auditors a report on the results of the investigations carried out during the reporting period.
At least, every six months, a summary disclosure of the number and type of Reports received and of the main actions undertaken is prepared for the Chairman, the CEO, the Chairman of the Board of Statutory Auditors and for the Chairman of the Control and Risk Committee.

In addition, the members of TIM Supervisory Board and of the individual Supervisory Boards of the TIM Entities can access the Portal directly through a specific profile in view-mode only, in order to view the Reports that fall within their respective remit.

6.2.6 Record keeping

Description

The information and any other personal data are processed - also as part of the Portal - in compliance with EU Regulation 2016/679 (General Data Protection Regulation - hereinafter GDPR) (Annex 2).
In order to ensure the management and traceability of the Reports and the consequent activities, the Head of the Audit Department oversees the preparation and updating of all the information regarding the Reports and ensures - using the Portal and its functions - the storage of all related supporting documentation for a period of ten years, starting from the date of receipt of the Report. The originals of the Reports received in paper form are kept in a special protected environment.

6.2.7 Periodic checks

Description

Every six months, a check on the completeness of the reports is carried out by an Audit Department function other than the one that manages the reports in operational terms, in order to ensure that all the reports received have been processed (including those to be sent to the relevant functions) and included in the monthly reports sent to the Board of Statutory Auditors as per this Procedure.

7. ANNEXES

Annex 1

PRIVACY POLICY

Pursuant to Regulation 2016/679/EU (General Regulation on Data Protection - hereinafter GDPR), Telecom Italia S.p.A., hereinafter TIM, provides you with the following Privacy Statement on the processing of your data in relation to the management of Reports governed by the "*Whistleblowing* Procedure" issued by the Audit Department of TIM.

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

The personal data of the data subjects are processed for the purposes related to the application of the aforementioned procedure and to fulfil the obligations established by law, regulations or community legislation. The provision of data is necessary to achieve the purposes referred to above. Failure to provide, or partial or incorrect provision of data could result in the inability to manage the Reports received.

2) Retention of personal data

TIM will retain your data for the period set out in the "*Whistleblowing* Procedure" which provides for cancellation of the Reports and the associated documentation after 10 years and, in any case, not for longer than the achievement of the purposes for which they were collected or subsequently processed.

3) Processing methods and logic

The data will be handled manually (for example as paper copies) and/or using automated tools (for example, using electronic procedures and supports), in accordance with principles that are congruous with the above-mentioned purposes and, in any case, with a view to ensuring the safety and confidentiality of the data. At each stage, the *whistleblowing* management system ensures the confidentiality of the content of the report (including information on any reported person) and of the Whistleblower's identity, including through the use of encrypted communications, except in cases where:

- the report is found to be unfounded and carried out for the sole purpose of harming the reported person or due to serious recklessness, negligence or inexperience on the part of the Whistleblower;
- anonymity is not legally enforceable (e.g. criminal investigations, inspections of control bodies, etc.);
- the report reveals facts that, albeit unrelated to the company affairs, are such that reporting to the Judicial Authority is necessary (for example, terrorist offences, espionage, attacks, etc.).

Breach of the obligation of confidentiality (without prejudice to the above exceptions) may give rise to disciplinary sanctions.

4) Data Controller, Data Protection Officer and categories of persons authorised to process data in TIM

The Data Controller of the personal data is TIM S.p.A., with registered office at Via Gaetano Negri, no. 1 - 20123 Milan. TIM and the Telecom Italia Group companies have appointed a sole Data Protection Officer for the TIM Group, domiciled at TIM, Via Gaetano Negri, no. 1 - 20123 Milan, who can be contacted by email at the following address: dpo.gruppotim@telecomitalia.it. The processing of personal data is carried out by the Data Processor and by employees of the Audit Department of TIM S.p.A. These employees have been authorised to process personal data and have received adequate operating instructions in this regard.

5) Categories of third-party subjects to whom the data might be disclosed in their capacity of Data Controllers or who might become familiar with them in their capacity of Data Processors

In addition to TIM employees, certain personal data may be processed by third parties, including Telecom Italia Group companies, to whom TIM entrusts certain activities (or part of them) for the purposes referred to in point 1). These third-party subjects might also be based abroad, in EU or non-EU countries; in the latter case, the transfer of the data is carried out if the European Commission has ruled on the adequacy of the level of data protection in the non-EU country or on the basis of appropriate and opportune guarantees provided by Articles 46 or 47 of the GDPR (e.g. signing of the "standard clauses" of data protection adopted by the European Commission) or of the additional preconditions for the legitimacy of the transfer provided by Article 49 of the GDPR. These subjects will operate as independent Data Controllers or will be designated as Data Processors and mainly come under the following categories:

a) Members of corporate bodies.
b) Consultants (Organization, Litigation, Legal Studies, etc.).
c) Companies in charge of payrolls administration and HR management, retention of employee. personal data, development and / or operation of the information systems dedicated to such matters.
d) Companies appointed to manage company archives, including the personal data of former employees.
e) Auditing companies.
f) Institutions and/or public authorities, judicial authorities, police bodies, investigative agencies.

6) Right of access to personal data and other rights

You have the right to access your data at any time - subject to the provisions in Annex 2 of this procedure - and to exercise your other rights under the data protection legislation (e.g. ask for the source of the data, correction of inaccurate or incomplete data, restriction of processing, erasure of data (right to be forgotten), portability of data, as well as the right to object to their use for legitimate reasons), by sending an e-mail to the following address ***whistleblowing@telecomitalia.it.*** Finally, you have the right to lodge a complaint with the Privacy Authority.

Annex 2

PROCESSING OF PERSONAL DATA

The information and any other personal data are processed - also as part of the Whistleblowing Portal - in compliance with EU Regulation 2016/679 (General Data Protection Regulation - hereinafter GDPR). More specifically, the TIM Group companies concerned (the "Companies") ensure that personal data processing is carried out in compliance with the fundamental rights and freedoms, and respecting the dignity of the data subjects, with specific regard to the confidentiality and security of data, ensuring compliance, inter alia, with the provisions set out below.
Pursuant to the GDPR, the personal data of which the Companies become aware for the purposes of this procedure must be:

- limited to those strictly and objectively necessary to verify the grounds of and to manage the report;
- processed lawfully and fairly.

Furthermore, it is mandatory that:

- all the organizational functions / positions of the TIM Group and its subsidiaries affected by the direct receipt of the reports, ensure the strict confidentiality of the whistleblowers and of the reported persons. In this regard, it is reiterated that, pursuant to art. 4 of the Telecom Italia Code of Ethics and Conduct, those who have made a report in good faith will not suffer any adverse consequence and the confidentiality of the whistleblowers' identity is ensured according to specific internal procedures, subject to legal obligations;
- the privacy statement referred to in Annex 1 be made available to the data subjects, including through the *Whistleblowing* Portal, which constitutes an integral and substantial part of the "*Whistleblowing* Procedure";
- third parties, who do not have direct or indirect business relationships with the company, be informed that their personal data are processed in relation to a report received by the Company, only if there is no risk that such disclosure may compromise the ability to effectively verify the grounds of the report;
- no indications are provided to the reported person on the Whistleblower's identity, except if it is ascertained that the latter has made a false statement in bad faith;
- in analogy with the provisions of art. 54-bis, paragraph 2, of legislative decree no. 165 of 30 March 2001, (Consolidated Law on Public Employment) and of article 6 of legislative decree no. 231 of 8th June 2001, as amended by law 179 of 30.11.2017, in the context of disciplinary proceedings that may be brought against the reported subject, the Whistleblower's identity cannot be revealed, without his or her consent, as long as the disciplinary charge is based on separate and additional findings with respect to the report. If the charge is based, in whole or in part, on the report, the identity can be revealed where such knowledge is essential for the defence of the reported party.
  For all matters not expressly provided for in this annex, with specific reference to any data transferred abroad, reference is made to the "System of rules for Privacy law application within the Telecom Italia Group", issued by the Privacy Function (code 2009-00048), which can also be consulted on the Intranet site of said Function.

Annex 3

E-mail boxes of the Boards of Statutory Auditors/SB 231 of the TIM Group companies

TIM Ventures Board of Statutory Auditors	timventures.cs@telecomitalia.it
TIM Retail Board of Statutory Auditors	4gr.cs@telecomitalia.it
TI Sparkle Board of Statutory Auditors	tisparkle.cs@telecomitalia.it
Olivetti Board of Statutory Auditors	olivetti.cs@telecomitalia.it
Telecontact Center Board of Statutory Auditors	tcc.cs@telecomitalia.it
Telenergia Board of Statutory Auditors	telenergia.cs@telecomitalia.it
Telsy Board of Statutory Auditors	telsy.cs@telecomitalia.it
TI Trust Technology Board of Statutory Auditors	titt.cs@telecomitalia.it
H. R. Services Board of Statutory Auditors	hrs.cs@telecomitalia.it
TN Fiber Board of Statutory Auditors	tnfiber.cs@telecomitalia.it
TIESSE Board of Statutory Auditors	tiesse.cs@telecomitalia.it
Fondazione TI Board of Statutory Auditors	foundation.cs@telecomitalia.it
Telecom Italia San Marino Board of Statutory Auditors	tism.cs@telecomitalia.it
Telefonia Mobile Sammarinese Board of Statutory Auditors	tms.cs@telecomitalia.it
Flash Fiber Board of Statutory Auditors	flashfiber.cs@telecomitalia.it
TIMVISION S.r.l. Board of Statutory Auditors	timvision.cs@telecomitalia.it
Noovle S.r.l. Board of Statutory Auditors	noovle.cs@telecomitalia.it