Procedura Whistleblowing

Contenuti

1. PREMESSA

Per “whistleblowing” (di seguito “Segnalazione”) si intende qualsiasi segnalazione, proveniente da chiunque, riguardante comportamenti (di qualsivoglia natura, anche meramente omissivi) riferibili al Personale TIM e/o a Terzi non conformi/in violazione a leggi e regolamenti, al Codice Etico ed al Modello Organizzativo 231, nonché al sistema di regole e procedure vigenti nel Gruppo, tra le quali a titolo esemplificativo ma non esaustivo: la Policy per il Rispetto dei Diritti Umani, la Procedura Tax Risk Management, il Sistema di Gestione Anticorruzione di TIM e la Policy Anticorruzione di Gruppo.

La presente procedura (di seguito “Procedura”) è finalizzata anche a dare attuazione alla legge 30 novembre 2017, n. 179 (“Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato”) che, a tutela dei dipendenti che segnalano presunti illeciti, ha previsto la disciplina del c.d. whistleblowing nel settore privato, modificando il D.lgs. n. 231/2001 sulla responsabilità “amministrativa” degli enti.

La predetta normativa prevede, in particolare: i) la creazione di uno o più canali (di cui uno di tipo informatico) per la presentazione di segnalazioni circostanziate, strutturati in modo da garantire la riservatezza del Segnalante; ii) il divieto di atti ritorsivi o discriminatori, diretti e indiretti, nei confronti del Segnalante per motivi collegati direttamente o indirettamente alla segnalazione; iii) sanzioni disciplinari per chi violi le misure di tutela del Segnalante e per chi effettui con dolo o colpa grave segnalazioni che si rivelino infondate.

Il Personale del Gruppo TIM coinvolto nella gestione delle segnalazioni è tenuto, nei limiti previsti dalla legge, alla riservatezza del contenuto della segnalazione, dell’identità del Segnalante, del segnalato e degli altri soggetti coinvolti. La Procedura si applica anche alle segnalazioni anonime, ove queste siano adeguatamente circostanziate, ove cioè siano in grado di far emergere fatti e situazioni relazionandoli a contesti determinati.

Al fine di consentire un’efficiente gestione delle segnalazioni, TIM si è dotata di un Portale delle segnalazioni (in breve “Portale”), a valere anche per le società controllate da TIM (ad eccezione delle società quotate e delle società estere, diverse da Telecom Italia San Marino S.p.A. e da Telefonia Mobile Sammarinese S.p.A.), ognuna delle quali può accedere al Portale per visualizzare le segnalazioni di propria competenza. Il Portale è stato implementato in modo tale da impedire l’accesso a soggetti non abilitati, e prevede, inoltre, diverse tipologie di profili di accesso (visualizzazione, modifica, etc.) tracciati attraverso log di sistema.

2. DESTINATARI

Destinatari della Procedura sono:

- i Vertici aziendali e i componenti degli organi sociali e dell’Organismo di Vigilanza di TIM e delle società controllate nazionali del Gruppo TIM, della Fondazione TIM, di Telecom Italia San Marino S.p.A. e di Telefonia Mobile Sammarinese S.p.A. (di seguito collettivamente le Entità TIM);
- tutti i dipendenti di TIM, delle Entità TIM, i partner, i clienti, i fornitori, i consulenti, i collaboratori, i soci in possesso di notizie riguardanti le condotte definite in Premessa.

3. SCOPO E CAMPO DI APPLICAZIONE

Il processo si colloca nel Business Process Framework ETOM in:

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

La Procedura ha come scopo la disciplina del processo di ricezione, analisi e gestione delle segnalazioni, da chiunque inviate o trasmesse, anche in forma anonima (la gestione comprende anche l'archiviazione e la successiva cancellazione sia delle segnalazioni che di tutta la documentazione ad esse connessa, secondo quanto indicato nel successivo paragrafo 6.2.6).

La Procedura si applica a TIM e alle Entità TIM, che ne garantiscono la corretta e costante applicazione, nonché la massima diffusione al proprio interno, nel rispetto degli obblighi di riservatezza e delle prerogative di autonomia e indipendenza di ciascuna Società.

La Procedura costituisce inoltre un riferimento per le società controllate da TIM diverse dalle Entità TIM, che possono recepirla, previo adeguamento alle normative ai processi ed agli assetti organizzativi specifici e/o locali.

Non rientrano nel campo di applicazione della Procedura le attività di competenza della Funzione Security, relative alla trattazione e gestione delle informazioni classificate ex DPCM n. 5 del 6 novembre 2015 ("Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva") e successive modifiche.

In caso di segnalazioni riguardanti le attività disciplinate dalla normativa Golden Power[1], oggetto di specifica competenza di supervisione e controllo da parte delle Organizzazioni di Sicurezza di TIM, Sparkle e Telsy, troverà applicazione la Policy aziendale "*Linee Guida Golden Power*", che prevede l'attivazione di meccanismi di confronto tra la Direzione Audit e le Organizzazioni di Sicurezza per l'avvio delle attività di verifica.

Sono escluse dal perimetro della Procedura le segnalazioni inerenti a:
- comunicazioni relative al conflitto di interessi, ai sensi della relativa procedura;
- tematiche di security, per le quali si rimanda agli specifici canali informativi già esistenti, ovvero:
  - Reports Ermes, per la segnalazione di incidenti di security che riguardano le risorse umane, le risorse materiali e quelle immateriali (quali, ad esempio, malfunzionamenti software, guasti alla rete aziendale, smarrimento o distruzione accidentale di documenti, incidenti di sicurezza ICT, furti).

---

[1] D.P.C.M. 16/10/2017: i) processi di governance, con particolare riferimento a tutti i processi decisionali afferenti ad attività strategiche e alla rete; ii) controllo e supervisione di tutte le attività, svolte nei diversi ambiti aziendali, attinenti alla gestione degli asset rilevanti ai fini della Difesa e della Sicurezza Nazionale; iii) informative sullo stabilimento nel territorio nazionale delle funzioni di gestione e sicurezza delle reti e delle forniture che supportano le attività strategiche e strategiche chiave nonché i SOC, CERT, DOC, NOC, IOC e gli altri data center e/o dispositivi di sicurezza logica e informatica atti a garantire la confidenzialità e l'integrità dei dati aziendali; iv) informative su ogni decisione che possa ridurre, anche temporaneamente, o cedere capacità tecnologiche, operative, industriali nelle "attività strategiche" e nelle "attività strategiche chiave", ivi compresa la cessione di quote societarie, di diritti di proprietà o titoli legali, di capacità tecnologiche, operative o industriali, limitando di fatto, il livello di autonomia della Società.
D.P.C.M. 2/11/2017: i) informative su qualsiasi variazione e riorganizzazione degli assetti societari di TIM S.p.A. e delle Società della stessa, direttamente od indirettamente controllate; ii) informative su qualsiasi piano di cessione o alienazione di attività strategiche o delibere del Consiglio di Amministrazione rilevanti per l'eventuale impatto sulla sicurezza, la disponibilità ed il funzionamento delle reti e degli impianti nonché sulla continuità del servizio universale.
D.P.C.M. 5/09/2019: specifico Decreto Presidenziale applicato nei confronti di TIM in materia di "Servizi di Comunicazione elettronica a banda larga basati sulla tecnologia 5G. In particolare: i) processi di governance con riferimento ai processi decisionali, anche di natura tecnica, afferenti alle attività ritenute rilevanti ex art. 1-bis del Decreto-Legge 15 marzo 2012, n. 21."

- Travel Security, per la richiesta di informazioni e segnalazioni inerenti a trasferte all'estero;
- abusi on line, per la segnalazione di comportamenti o eventi riconducibili a casi di abuso nell'utilizzo dei servizi di rete offerti da TIM, quali ad esempio spam, diffusione virus e malware, attacchi informatici, phishing e furti d'identità, pubblicazione o diffusione di materiale offensivo, sovversivo, pedopornografico, salvo che tali illeciti non siano riconducibili a fattispecie rilevanti ai sensi del Modello Organizzativo 231 (nel quale caso dovranno essere trattate quali segnalazioni disciplinate dalla Procedura);
- reclami commerciali, per i quali si rimanda ai servizi 119, 187, 191, nonché al canale interno "Chi-ama Telecom Italia".

Le segnalazioni rientranti nelle suddette tipologie, inserite nel Portale, verranno inoltrate alle competenti Funzioni dalla Direzione Audit, che ne monitora comunque gli esiti per rilevare eventuali debolezze del sistema di controllo interno e di gestione dei rischi.

4. GLOSSARIO

- Personale TIM: si intendono i dipendenti, a tempo indeterminato e determinato (dirigenti, quadri, impiegati, operai) di TIM e delle Entità TIM.
- Terzi: si intendono tutti coloro che, a diverso titolo, intrattengono rapporti di lavoro, di collaborazione o d'affari con TIM e/o le Entità TIM, ivi compresi i collaboratori, gli stagisti, i somministrati, consulenti, agenti, intermediari, fornitori e business partners, in relazione alla prestazione lavorativa, di collaborazione o d'affari con TIM o le Entità TIM.
- Organismo di Vigilanza delle Entità TIM: si intende l'Organismo di Vigilanza costituito ex art. 6, punto 1, lett. B) del D. Lgs. n. 231/01, ovvero il Collegio Sindacale nelle funzioni di Organismo di Vigilanza.
- Entità TIM: si intendono le società controllate nazionali del Gruppo TIM, la Fondazione TIM, Telecom Italia San Marino S.p.A. e Telefonia Mobile Sammarinese S.p.A, alle quali si applica in via diretta la Procedura
- Segnalante: qualunque soggetto che effettua una Segnalazione.
- Segnalazione: si intende qualsiasi comunicazione riguardante comportamenti (anche meramente omissivi) riferibili al Personale TIM o a Terzi, correlati allo svolgimento dell'attività lavorativa o di collaborazione per conto di TIM o delle Entità TIM, in violazione a leggi e regolamenti e/o non conformi al Codice Etico ed al Modello Organizzativo 231, nonché al sistema di regole e procedure vigenti nel Gruppo, tra le quali, a titolo esemplificativo ma non esaustivo: la Policy per il Rispetto dei Diritti Umani, la Procedura Organizzativa Tax Risk Management, il Sistema di Gestione Anticorruzione di TIM e la Policy Anticorruzione di Gruppo.
- Segnalazione anonima: Segnalazione in cui le generalità del Segnalante non siano esplicitate, né siano individuabili in maniera univoca.
- Segnalazione effettuata con dolo o colpa grave: Segnalazione che dagli esiti della fase istruttoria si riveli priva di riscontro fattuale ed effettuata nella piena consapevolezza dell'insussistenza di una violazione o di una non conformità o dell'estraneità del segnalato alla stessa, ovvero con colpa grave nella valutazione degli elementi di fatto.
- Segnalazione circostanziata: Segnalazione in cui le asserzioni (ad esempio periodo di riferimento, luogo, valore, cause e finalità, elementi che consentano di identificare il soggetto che ha posto in essere i fatti segnalati, anomalie relative al sistema di controllo interno, documentazione a supporto, ecc.) sono caratterizzate da un grado di dettaglio sufficiente, almeno astrattamente, a far emergere fatti precisi e concordanti e situazioni, relazionandoli a contesti determinati, nonché a consentire di identificare elementi utili ai fini della verifica della fondatezza della Segnalazione stessa. Le segnalazioni circostanziate si distinguono a loro volta in:
  - segnalazioni circostanziate verificabili: qualora, considerati i contenuti della Segnalazione, sia possibile in concreto, sulla base degli strumenti di indagine a disposizione, compiere verifiche sulla fondatezza della Segnalazione in ambito aziendale;

- segnalazioni circostanziate non verificabili: qualora emerga nel corso delle verifiche preliminari che non è possibile, sulla base degli strumenti di indagine a disposizione, compiere verifiche sulla fondatezza della Segnalazione.

- Segnalazione relativa a fatti rilevanti: Segnalazione su anomalie operative aziendali e/o illeciti e/o frodi e/o abusi:
  - per la quale, ad esito della verifica preliminare, sia stimabile per TIM S.p.A. e/o per le società da essa controllate un impatto quali-quantitativo significativo sul bilancio (in termini di tematiche di contabilità, revisione legale dei conti, controlli interni sull'informativa finanziaria)[2] e/o
  - che riguardi Presidenti, Amministratori Delegati e membri degli organi di amministrazione e/o controllo/vigilanza di TIM e delle Entità TIM e/o violazioni del Modello 231.

5. RIFERIMENTI

- D. Lgs n. 231/01 "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300"
- Regolamento (UE) n. 2016/679 sulla protezione dei dati personali (c.d. GDPR)
- D.Lgs. n. 196/03 e successive modifiche ed integrazioni, nonché le collegate disposizioni legislative
- Legge 30 novembre 2017, n. 179 "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato".
- DPCM del 16 ottobre 2017 che impone specifiche prescrizioni e condizioni nei confronti di TIM, Telecom Italia Sparkle e Telsy, ai sensi della legge 11 maggio 2012, n. 56 sull'esercizio dei poteri speciali del Governo sulle aziende private in alcuni settori strategici (c.d. Golden Power).
- DPCM 02/11/2017 - Comunicazione a TIM adozione del decreto attuativo della legge sulla Golden Power
- DPCM 16/10/2017 - Notifica a TIM del decreto attuativo della legge sulla Golden Power
- Provv. del Consiglio dei Ministri 5-09-2019 - Prescrizioni in materia di 5G
- D.L. n. 22/2019 - Disposizioni sui poteri speciali (Golden Power) inerenti ai servizi di comunicazione elettronica a banda larga basati su tecnologia 5G
- D.L. n. 64/2019 - Golden Power - Norme in materia di poteri speciali sugli assetti societari
- DPCM n. 5 del 6 novembre 2015 - Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva e successive modifiche

I riferimenti interni TIM sono:
- Modello Organizzativo 231 del Gruppo TIM (comprensivo del Codice Etico e di Condotta)
- Sviluppo dell'Identità Organizzativa - I nuovi Valori di Telecom Italia (Cod. 2015-00155)
- Sistema di Gestione Anticorruzione
- Policy Anticorruzione di Gruppo
- Procedura Organizzativa "Valutazione passività potenziali derivanti da sospette frodi con impatti fiscali" (Cod. 2016-00177)
- Definizione e Formalizzazione di Policy, Procedure ed Istruzioni Operative di Gruppo (Cod.2014-00152)
- Policy Anticorruzione del Gruppo Telecom Italia (Cod. 2012-00234)
- Procedura per la gestione dei conflitti di interessi Gruppo Telecom Italia (Cod.2013-00154)
- Rispettare i Diritti Umani nel Gruppo Telecom Italia (Cod. 2015-00193)
- Gestione del procedimento disciplinare personale non Dirigente (Cod. 2020-00017)
- Linee Guida Golden Power, emesse in data 6 aprile 2020 (Cod. 2018-00026)

[2] La significatività dell'impatto sotto l'aspetto quantitativo viene valutata dall'Organismo di Vigilanza d'intesa con il Chief Financial Office. L'impatto è significativo sotto l'aspetto qualitativo se le anomalie operative e/o frodi e/o abusi sono in grado di influenzare le decisioni economiche e di investimento dei potenziali destinatari dell'informativa finanziaria.

6. DESCRIZIONE DEL PROCESSO E RESPONSABILITA'

6.1 Scopo e descrizione breve del processo

Nell'ambito del nuovo Business Process Framework di TIM, il processo di gestione delle Segnalazioni, i cui principi, responsabilità ed attività sono descritti nei paragrafi che seguono, si inquadra nell'area L0 ENTERPRISE MANAGEMENT con il seguente riferimento: L1 Enterprise Risk Management, L2 Audit Management.

Per le Segnalazioni riguardanti TIM S.p.A., l'owner del processo di gestione è l'Organismo di Vigilanza di TIM, ferme le responsabilità e le prerogative del Collegio Sindacale sulle segnalazioni allo stesso indirizzate, ivi incluse le denunce ex art 2408 Codice Civile.

Le eventuali Segnalazioni che riguardino il Responsabile della Direzione Audit di TIM e/o le Funzioni dallo stesso dipendenti saranno trasmesse senza indugio agli altri membri dell'Organismo di Vigilanza.
Per le Segnalazioni riguardanti le Entità TIM, l'owner del processo è il rispettivo Organismo di Vigilanza, ferme le precitate responsabilità e prerogative del Collegio Sindacale.

La gestione delle segnalazioni viene svolta con il supporto della Direzione Audit di TIM S.p.A. ovvero della Funzione Audit dell'Entità TIM, ove presente, nel rispetto dei principi stabiliti dagli Standard Internazionali per la pratica professionale dell'Internal Audit e dal Codice Etico emanati dall'Institute of Internal Auditors (IIA), nonché dal Codice Etico e di Condotta del Gruppo TIM.

6.2 Input/output del processo

Gli input del processo sono:
- Inserimento della Segnalazione sul Portale da parte di dipendenti, collaboratori, consulenti, prestatori di lavoro, soci e terzi.
- Obbligo per i dipendenti che ricevano la Segnalazione da Personale TIM o da terzi, di inserimento della stessa sul Portale.

Gli output del processo sono:
- Trattamento della Segnalazione e cancellazione delle segnalazioni e della relativa documentazione dopo 10 anni.

6.2.1 Invio delle segnalazioni

Descrizione attività

Il Personale TIM che venga a conoscenza di un comportamento tra quelli descritti nei precedenti paragrafi è tenuto ad effettuare una Segnalazione secondo le modalità di seguito indicate.
Le segnalazioni devono essere trasmesse mediante l'utilizzo del Portale, reso disponibile in ambiente Intranet ed Internet https://portalesegnalazioni.telecomitalia.it, presa preventiva visione dell'"Informativa Privacy" (Allegato 1), oppure inviate all'indirizzo di posta "Casella Segnalazioni, Telecom Italia S.p.A., Via Gaetano Negri, 1, 20123 Milano".
In fase di inserimento della Segnalazione tramite il Portale, il Segnalante ha a disposizione un'apposita sezione di Frequently Asked Questions (FAQ), che contiene le risposte alle domande più frequenti al fine di garantire la corretta registrazione delle segnalazioni, nonché un elenco delle tipologie di comunicazioni non rientranti nel perimetro della Procedura, al fine di assicurarne un corretto indirizzamento.

Le Segnalazioni riguardanti le Entità TIM dovranno essere inserite nel Portale oppure inviate alle caselle e-mail riportate in Allegato 3.
Eventuali segnalazioni indirizzate al Collegio Sindacale di TIM (ivi incluse le denunce ex art. 2408 c.c.) inserite nel Portale o comunque pervenute all'Organismo di Vigilanza o alla Direzione Audit saranno a cura

di quest'ultima trasmesse alla Funzione Corporate Affairs (in ambito Legal and Tax) per il successivo inoltro al Collegio Sindacale di TIM. Analogamente, la Funzione Corporate Affairs provvederà ad inserire nel Portale eventuali segnalazioni pervenute al Collegio Sindacale ma indirizzate e/o di competenza dell'Organismo di Vigilanza.
Il Personale TIM che riceva, per posta esterna o interna, e-mail o fax, una Segnalazione, ha l'obbligo di inserirla con immediatezza nel Portale, trasmettendo alla Direzione Audit l'originale, completo di eventuale documentazione di supporto. Il ricevente non può trattenerne copia e deve astenersi dall'intraprendere alcuna iniziativa autonoma di analisi e/o approfondimento. La mancata comunicazione di una Segnalazione ricevuta costituisce una violazione della Procedura e potrà comportare l'adozione delle opportune iniziative, anche di carattere disciplinare.
Nella gestione delle segnalazioni è garantita la riservatezza del contenuto e dell'identità del Segnalante, ad eccezione dei seguenti casi:

- qualora ne venga accertata, anche con sentenza di primo grado, la responsabilità' penale per i reati di calunnia o diffamazione o comunque per reati commessi con la Segnalazione, ovvero la responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave;
- a fronte di richieste dell'Autorità Giudiziaria o altri aventi diritto.

La violazione dell'obbligo di riservatezza (fatte salve le eccezioni di cui sopra) potrà comportare l'adozione delle iniziative di volta in volta applicabili ivi incluse quelle a carattere disciplinare.
E'vietato il compimento di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti dei soggetti che effettuano una Segnalazione ai sensi della Procedura, per motivi collegati, direttamente o indirettamente alla Segnalazione. Il licenziamento ritorsivo o discriminatorio del soggetto Segnalante è nullo. Sono altresì nulli il mutamento di mansioni ai sensi dell'articolo 2103 del codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del Segnalante. L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni può essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di competenza, oltre che dal Segnalante, anche dall'organizzazione sindacale indicata dal medesimo.

Qualora un dipendente ritenga di aver subito uno dei predetti comportamenti a causa dell'inoltro di una Segnalazione, potrà comunicarlo alla Direzione Audit per il tramite del Portale. Sarà cura della suddetta Direzione informare tempestivamente la Funzione Human Resources per l'analisi del caso e l'eventuale avvio di un procedimento disciplinare nei confronti dell'autore del comportamento discriminatorio o ritorsivo.
Per le conseguenze connesse all'eventuale adozione di atti ritorsivi e/o discriminatori, diretti o indiretti, compiuti nei confronti del Segnalante-dipendente per motivi collegati, anche indirettamente, alla Segnalazione e per la disciplina delle sanzioni adottabili nei confronti di chi viola le misure di tutela del Segnalante o di chi effettua con dolo o colpa grave segnalazioni che si rivelino infondate, si rinvia alla specifica disciplina contenuta al paragrafo 8 ("Sistema Disciplinare") del Modello Organizzativo 231.

6.2.2 Registrazione e classificazione

Descrizione attività

Tutte le segnalazioni, indipendentemente dalla modalità di ricezione sono registrate nel Portale, che costituisce il *database* riepilogativo dei dati essenziali delle segnalazioni e della loro gestione (tracciata tramite *workflow*) ed assicura, altresì, l'archiviazione di tutta la documentazione allegata, nonché di quella prodotta o acquisita nel corso delle attività di analisi.
Successivamente alla registrazione, la Direzione Audit analizza e classifica la Segnalazione, per limitare la trattazione alle sole segnalazioni rientranti nel perimetro della Procedura.
Per ciascuna Segnalazione, il Portale assegna un codice identificativo univoco che permette a ciascun Segnalante di verificarne lo stato di lavorazione, in modo del tutto anonimo.
Nel caso in cui una Segnalazione non risulti adeguatamente circostanziata, la Direzione Audit potrà richiedere al Segnalante ulteriori elementi di dettaglio, secondo le modalità sotto indicate:

- nel caso in cui il Segnalante abbia fornito un contatto (*e-mail*, telefono, ecc.), attraverso tale contatto;

- nel caso di mancata indicazione di un contatto, attraverso uno specifico messaggio inserito nel Portale, che il Segnalante potrà visualizzare utilizzando il codice identificativo della Segnalazione.

6.2.3 Analisi preliminare della Segnalazione
Descrizione attività

La Direzione Audit procede ad un'analisi preliminare delle segnalazioni, al fine di identificare quelle da inoltrare a specifici destinatari a cui sono indirizzate, quelle potenzialmente rilevanti ai sensi del D.lgs. n. 231/01, quelle relative a fatti contrari al Codice Etico, quelle riguardanti fatti gestionali/operativi da inviare alle strutture aziendali competenti. Inoltre, valuta, in via preliminare, anche tramite eventuali analisi documentali, la presenza dei presupposti necessari all'avvio della successiva fase di istruttoria, proponendo all'Organismo di Vigilanza l'archiviazione delle segnalazioni generiche e prive di elementi informativi.
Tutte le segnalazioni sono oggetto di informativa all'Organismo di Vigilanza che, su base documentale e anche in considerazione degli esiti delle analisi preliminari svolte dalla Direzione Audit, valuta:

i) per le segnalazioni che riguardano TIM S.p.A:
a) l'avvio della successiva fase di istruttoria; b) l'eventuale inosservanza di norme/procedure, da comunicare anche alla Direzione Human Resources, per le analisi di competenza; c) la rilevanza della Segnalazione (segnalazioni relative a fatti rilevanti), ai fini della comunicazione al Presidente, all'A.D., al Presidente del Collegio Sindacale ed al Presidente del Comitato per il Controllo ed i Rischi di TIM.

Sono archiviate dall'Organismo di Vigilanza le segnalazioni: i) generiche e/o che non costituiscono una "Segnalazione circostanziata"; ii) palesemente infondate; iii) contenenti fatti già oggetto in passato di specifiche attività di istruttoria e già chiuse, ove dalle verifiche preliminari svolte non emergano nuove informazioni tali da rendere necessarie ulteriori attività di verifica; iv) "circostanziate verificabili" per le quali, alla luce degli esiti delle verifiche preliminari condotte, non emergano elementi tali da supportare l'avvio della successiva fase di istruttoria; v) "circostanziate non verificabili" per le quali, alla luce degli esiti delle verifiche preliminari, non è possibile, sulla base degli strumenti di indagine a disposizione, compiere ulteriori verifiche sulla veridicità e/o fondatezza della Segnalazione.

Le segnalazioni archiviate in quanto palesemente infondate sono trasmesse alla Direzione Human Resources, affinché valuti, con le altre strutture aziendali competenti, se la Segnalazione sia stata effettuata al solo scopo di ledere la reputazione o di danneggiare o comunque di recare pregiudizio alla persona e/o società segnalata, ai fini dell'attivazione di ogni opportuna iniziativa nei confronti del Segnalante;

ii) per le segnalazioni riguardanti una o più Entità TIM:
la trasmissione della stessa all'Organismo di Vigilanza dell'Entità TIM per le determinazioni di competenza.

6.2.4 Approfondimenti specifici
Obiettivi e caratteristiche dell'istruttoria

L'obiettivo delle attività di istruttoria sulle segnalazioni è di procedere, nei limiti degli strumenti a disposizione della Direzione Audit, ad accertamenti, analisi e valutazioni specifiche circa la ragionevole fondatezza delle circostanze fattuali segnalate, nonché di fornire eventuali indicazioni in merito all'adozione delle necessarie azioni correttive sulle aree e sui processi aziendali interessati.

L'istruttoria ha l'obiettivo di ricostruire, sulla base della documentazione e delle informazioni ufficiali, nonché di quelle rese disponibili, i processi gestionali e decisionali seguiti. Non rientra nel perimetro di analisi dell'istruttoria, se non nei limiti della manifesta irragionevolezza, il merito delle decisioni gestionali o di opportunità, discrezionali o tecnico-discrezionali, di volta in volta operate dalle strutture/posizioni aziendali coinvolte.

Esecuzione dell'istruttoria

La Direzione Audit cura lo svolgimento dell'istruttoria anche acquisendo dalle strutture interessate gli elementi informativi necessari, coinvolgendo le competenti Funzioni aziendali ed avvalendosi, se ritenuto opportuno, di esperti o periti esterni a TIM. Restano salve le competenze in materia disciplinare della Direzione Human Resources.

In relazione alle segnalazioni riguardanti frodi con possibili impatti di carattere fiscale, la Direzione Audit, in applicazione di quanto previsto dalla Procedura Organizzativa Task Risk Management, inoltra le stesse alla Direzione Compliance Operations per il seguito di competenza e per la successiva comunicazione alla Direzione Audit dei relativi esiti.

Le attività istruttorie sono svolte ricorrendo, a titolo esemplificativo, a:

- dati/documenti aziendali utili ai fini dell'istruttoria (ad es. estrazioni da sistemi aziendali SAP e/o altri sistemi specifici utilizzati);
- banche dati esterne (ad es. info provider/banche dati su informazioni societarie);
- fonti aperte;
- evidenze documentali acquisite presso le strutture aziendali;
- ove opportuno, dichiarazioni rese dai soggetti interessati o acquisite nel corso di interviste, verbalizzate e sottoscritte.

Al fine di acquisire elementi informativi, l'Organismo di Vigilanza ha facoltà (i) di richiedere alla Direzione Audit di TIM, fermi restando i vigenti flussi informativi, l'attivazione di audit c.d. "spot" sui fatti segnalati; (ii) di svolgere approfondimenti anche direttamente, tramite, ad esempio, formale convocazione e audizioni del Segnalante, del segnalato e/o di altri soggetti citati nella Segnalazione come informati dei fatti, nonché richiedere ai predetti soggetti la produzione di relazioni informative e/o documenti.

A conclusione dell'istruttoria, la Direzione Audit predispone una relazione che riporta:

- le attività svolte, i relativi esiti, nonché gli esiti di eventuali precedenti istruttorie svolte sui medesimi fatti o su fatti analoghi a quelli oggetto della Segnalazione;
- un giudizio di ragionevole fondatezza o meno dei fatti segnalati con eventuali indicazioni in merito all'adozione, da parte del competente management - che viene informato sugli esiti dell'istruttoria - delle necessarie azioni correttive sulle aree e sui processi aziendali interessati dalla Segnalazione.

Qualora, all'esito dell'istruttoria, emerga che i fatti oggetto di accertamento possano assumere rilevanza sotto il profilo disciplinare o, in ogni caso, in cui vi siano profili giuslavoristici, la relazione conclusiva contenente gli esiti delle attività è inviata anche al Responsabile della Direzione Human Resources, per le valutazioni di competenza. Analogamente, qualora dall'istruttoria emergano possibili fattispecie di rilevanza penale o di responsabilità civile, le risultanze della stessa sono trasmesse alla Direzione Legal & Tax per le valutazioni di competenza.

Le attività istruttorie relative a fatti segnalati sui quali sia nota l'esistenza di indagini in corso da parte di pubbliche autorità (ad esempio: autorità giudiziarie, ordinarie e speciali, organi amministrativi ed authority indipendenti, investiti di funzioni di vigilanza e controllo) sono sottoposte alla preliminare valutazione delle competenti Funzioni aziendali, affinché verifichino la compatibilità dell'istruttoria interna con le attività d'indagine/ispettive. Il Presidente e l'A.D. di TIM sono informati in merito agli esiti degli orientamenti assunti dalla competente Funzione aziendale.

Al termine dell'istruttoria, l'Organismo di Vigilanza delibera la chiusura della pratica evidenziando l'eventuale inosservanza di norme/procedure, ferme, quanto all'esercizio dell'azione disciplinare, le esclusive prerogative della Società, che provvederà a dare all'Organismo di Vigilanza comunicazione delle determinazioni assunte.

Nel caso in cui la Segnalazione riguardi uno o più componenti del Consiglio di Amministrazione, del Collegio Sindacale o dell'Organismo di Vigilanza di TIM, l'istruttoria sarà gestita congiuntamente dai rispettivi Presidenti. Nel caso in cui fosse chiamato in causa uno dei tre Presidenti, questo sarà sostituito dal componente dell'organo o dell'Organismo di Vigilanza anagraficamente più anziano. Nel caso in cui fosse invece coinvolto l'intero organo o l'intero Organismo di Vigilanza, l'istruttoria sarà gestita dai Presidenti degli altri due organi/Organismo di Vigilanza. In tali casi le risultanze dell'istruttoria saranno comunicate al Consiglio di Amministrazione, al Collegio Sindacale e all'Organismo di Vigilanza per quanto di rispettiva competenza.

Monitoraggio Azioni Correttive

Se dalle fasi dell'istruttoria dovesse emergere la necessità di azioni correttive, sarà responsabilità del management delle aree/processi oggetto di verifica definire un piano delle azioni correttive per la rimozione delle criticità rilevate. L'Organismo di Vigilanza ne monitora, con il supporto della Direzione Audit, lo stato di attuazione, fornendone informativa nella reportistica periodica di cui al successivo paragrafo.
Al competente management verrà richiesto un aggiornamento almeno trimestrale (a seconda della tipologia/entità delle azioni correttive) dello stato di attuazione delle azioni correttive.

6.2.5 Comunicazione dei risultati

Descrizione attività

Gli esiti di ciascuna istruttoria svolta sono contenuti in un report predisposto dalla Direzione Audit e trasmesso all'Organismo di Vigilanza oltre che alle strutture aziendali interessate affinché assumano le eventuali iniziative di competenza.
Nei casi rilevanti (cfr. definizione nel Glossario), l'Organismo di Vigilanza valuta l'invio della predetta istruttoria ai Vertici aziendali ed agli Organi di Controllo. Negli stessi casi, valuta, altresì, la trasmissione del report alle strutture aziendali interessate.
La Direzione Audit fornisce, altresì, all'Organismo di Vigilanza un report mensile di avanzamento di tutte le segnalazioni pervenute e rientranti nel perimetro della Procedura, con l'evidenza degli esiti delle istruttorie svolte.

Analogamente, su base trimestrale, la Funzione Human Resources fornisce all'Organismo di Vigilanza ed al Collegio Sindacale un'informativa sui provvedimenti disciplinari assunti a seguito dell'istruttoria svolta sulle segnalazioni.

Al fine di consentire una tempestiva informativa del Collegio Sindacale sulle tematiche oggetto di segnalazioni, la Direzione Audit trasmette, inoltre, con cadenza mensile, al Presidente del Collegio Sindacale un Report sugli esiti delle istruttorie svolte nel periodo di riferimento.
Infine, con cadenza semestrale, la Direzione Audit predispone per il Presidente, per l'A.D., per il Presidente del Collegio Sindacale e per il Presidente del Comitato per il Controllo ed i Rischi un'informativa di riepilogo del numero e della tipologia delle segnalazioni pervenute e delle principali iniziative assunte.

E' altresì prevista la possibilità per i componenti dell'Organismo di Vigilanza di TIM e dei singoli Organismi di Vigilanza delle Entità TIM di accedere direttamente al Portale, tramite un apposito profilo in sola visualizzazione, per prendere visione delle segnalazioni di rispettiva competenza.

6.2.6 Conservazione della documentazione

Descrizione attività

Le informazioni ed ogni altro dato personale acquisiti sono trattati – anche nel contesto del Portale - nel rispetto del Regolamento 2016/679/UE (Regolamento Generale sulla Protezione dei Dati – di seguito GDPR) (Allegato 2).

Al fine di garantire la gestione e la tracciabilità delle segnalazioni e delle attività conseguenti, il Responsabile della Direzione Audit cura la predisposizione e l'aggiornamento di tutte le informazioni

riguardanti le segnalazioni ed assicura - avvalendosi del Portale e delle sue funzionalità - l'archiviazione di tutta la correlata documentazione di supporto per un periodo di dieci anni, decorrenti dalla data di ricezione della Segnalazione. Gli originali delle segnalazioni pervenute in forma cartacea sono conservati in apposito ambiente protetto.

6.2.7 Controlli periodici

Descrizione attività

Con periodicità semestrale, viene svolto un controllo di completezza, a cura di una Funzione della Direzione Audit diversa rispetto a quella che gestisce operativamente le segnalazioni, al fine di accertare che tutte le segnalazioni pervenute siano state trattate, debitamente inoltrate ai destinatari di competenza e fatte oggetto di reportistica secondo quanto previsto dalla Procedura.

8. ALLEGATI

Allegato 1

INFORMATIVA PRIVACY

Ai sensi del Regolamento 2016/679/UE (Regolamento Generale sulla Protezione dei Dati – di seguito GDPR) Telecom Italia S.p.A., nel seguito TIM, Le fornisce, qui di seguito, l'informativa sui trattamenti dei Suoi dati personali effettuati in relazione alla gestione delle segnalazioni disciplinate dalla "Procedura whistleblowing" emessa dalla Direzione Audit di TIM.

1) Finalità per le quali il trattamento dei dati è necessario e relativa base giuridica

I dati personali degli interessati sono trattati per le finalità connesse all'applicazione della procedura sopra citata e per adempiere gli obblighi previsti dalla legge, dai regolamenti o dalla normativa comunitaria. Il conferimento dei dati è obbligatorio per il conseguimento delle finalità di cui sopra. Il mancato, parziale o inesatto conferimento potrebbe avere come conseguenza l'impossibilità di gestire le segnalazioni ricevute.

2) Conservazione dei dati personali

TIM conserva i Suoi dati per il tempo previsto dalla "Procedura Whistleblowing" che stabilisce la cancellazione delle segnalazioni e della relativa documentazione dopo 10 anni e, comunque, per un periodo di tempo non superiore al conseguimento delle finalità per le quali sono raccolti o successivamente trattati.

3) Modalità e logica del trattamento

I trattamenti dei dati sono effettuati manualmente (ad esempio, su supporto cartaceo) e/o attraverso strumenti automatizzati (ad esempio, utilizzando procedure e supporti elettronici), con logiche correlate alle finalità sopraindicate e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati. Il sistema di gestione delle segnalazioni garantisce, in ogni fase, la riservatezza del contenuto della segnalazione (incluse le informazioni su eventuali segnalati) e dell'identità del Segnalante, anche tramite l'uso di comunicazioni crittografate, ad eccezione dei casi in cui:

- la Segnalazione risulti infondata ed effettuata al solo scopo di nuocere al segnalato o per grave imprudenza, negligenza o imperizia del Segnalante;
- l'anonimato non sia opponibile per legge (es. indagini penali, ispezioni di organi di controllo, etc.);
- nella Segnalazione vengano rivelati fatti tali che, seppur estranei alla sfera aziendale, rendano dovuta la Segnalazione all'Autorità Giudiziaria (ad es. reati di terrorismo, spionaggio, attentati, etc.).

La violazione dell'obbligo di riservatezza (fatte salve le eccezioni di cui sopra) è fonte di responsabilità disciplinare.

4) Titolare, Data Protection Officer e categorie di persone autorizzate al trattamento dei dati in TIM

Il Titolare del trattamento dei Suoi dati personali è TIM S.p.A., con sede in via Gaetano Negri, n. 1 – 20123 Milano. TIM e le Società del Gruppo Telecom Italia hanno nominato un unico Data Protection Officer, domiciliato presso TIM, via Gaetano Negri, n. 1 – 20123 Milano, e contattabile inviando una e-mail al seguente indirizzo: dpo.gruppotim@telecomitalia.it. I dati personali sono trattati dal Responsabile e dai dipendenti della Direzione Audit di TIM S.p.A. Detti dipendenti sono stati autorizzati al trattamento dei dati personali ed hanno ricevuto, al riguardo, adeguate istruzioni operative.

5) Categorie di soggetti terzi ai quali i dati potrebbero essere comunicati in qualità di Titolari o che potrebbero venirne a conoscenza in qualità di Responsabili

Oltre che dai dipendenti di TIM, alcuni trattamenti dei Suoi dati personali potranno essere effettuati da soggetti terzi, ivi incluse le Società del Gruppo Telecom Italia, ai quali TIM affida talune attività (o parte di esse) per perseguire le finalità di cui al punto 1). Tali soggetti terzi potrebbero essere stabiliti anche all'estero, in Paesi Ue o extra Ue; in quest'ultimo caso, il trasferimento dei dati è effettuato in virtù dell'esistenza di una decisione della Commissione europea circa l'adeguatezza del livello di protezione dei dati del Paese extra UE oppure sulla base delle appropriate e opportune garanzie previste dagli artt. 46 o 47 del GDPR (es. sottoscrizione delle "clausole tipo" di protezione dei dati adottate dalla Commissione europea) o degli ulteriori presupposti di legittimità al trasferimento previsti dall'art. 49 del GDPR. Tali soggetti opereranno in qualità di Titolari autonomi o saranno designati Responsabili del trattamento e sono essenzialmente ricompresi nelle seguenti categorie:

a) Membri Organi sociali
b) Consulenti (Organizzazione, Contenzioso, Studi Legali, ecc.)
c) Società incaricate dell'amministrazione e gestione del personale, della conservazione dei dati personali dei dipendenti, dello sviluppo e/o esercizio dei sistemi informativi a ciò dedicati
d) Società incaricate per la gestione degli archivi aziendali, ivi inclusi i dati personali dei dipendenti cessati dal servizio
e) Società di Revisione/auditing
f) Istituzioni e/o Autorità Pubbliche, Autorità Giudiziaria, Organi di Polizia, Agenzie investigative.

6) Diritto di accesso ai dati personali ed altri diritti

Lei ha diritto di accedere in ogni momento ai dati che la riguardano – fatto salvo quanto riportato nell'allegato 2 della vigente procedura - e di esercitare gli altri diritti previsti dalla normativa sulla protezione dei dati personali (es. chiedere l'origine dei dati, la rettifica dei dati inesatti o incompleti, la limitazione del trattamento, la cancellazione o l'oblio, la portabilità dei dati, nonché opporsi al loro utilizzo per motivi legittimi), inviando una e-mail al seguente indirizzo whistleblowing@telecomitalia.it. Infine, Lei ha diritto di proporre un reclamo al Garante per la protezione dei dati personali.

Allegato 2

TRATTAMENTO DEI DATI PERSONALI

Le informazioni ed ogni altro dato personale acquisiti sono trattati – anche nel contesto del Portale segnalazioni - nel rispetto del Regolamento 2016/679/UE (Regolamento Generale sulla Protezione dei Dati – di seguito GDPR). In particolare, le Società del Gruppo TIM interessate (le "Società") garantiscono che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità degli interessati, con particolare riferimento alla riservatezza ed alla sicurezza dei dati, assicurando l'osservanza, tra l'altro delle disposizioni di seguito riportate.

Ai sensi del GDPR, i dati personali di cui le Società vengono a conoscenza ai fini della presente procedura devono essere:

- limitati a quelli strettamente e obiettivamente necessari per verificare la fondatezza della segnalazione e per la relativa gestione;
- trattati lecitamente e secondo correttezza.

Inoltre, è fatto obbligo che:

- tutte le funzioni/posizioni organizzative del Gruppo TIM e delle relative Società controllate interessate dalla eventuale diretta ricezione delle segnalazioni, assicurino l'assoluta riservatezza delle persone segnalanti e segnalate. Nel merito si ribadisce che, ai sensi dell'art. 4 del Codice Etico e di Condotta di Telecom Italia, nessuna conseguenza negativa deriva in capo a chi abbia in buona fede effettuato una Segnalazione ed è assicurata la riservatezza dell'identità dei segnalanti secondo apposite procedure interne, fatti salvi gli obblighi di legge;
- sia resa disponibile agli interessati, anche tramite il Portale segnalazioni, l'informativa privacy di cui all'Allegato 1, che costituisce parte integrante e sostanziale della "Procedura whistleblowing";
- sia comunicato ai soggetti terzi, non in rapporti d'affari diretti o indiretti con l'azienda, che i loro dati personali sono trattati in relazione ad una Segnalazione pervenuta alla Società, solo qualora non sussista il rischio che, comunicando tale informazione, si comprometta la capacità di verificare efficacemente la fondatezza della segnalazione;
- non siano fornite indicazioni al segnalato sull'identità del Segnalante, fatto salvo il caso in cui venga accertato che quest'ultimo abbia dichiarato il falso in malafede;
- in analogia con quanto previsto dall' art. 54-bis, comma 2, del decreto legislativo 30 marzo 2001, n. 165 (T.U. sul Pubblico Impiego) e dall'articolo 6 del decreto legislativo 8 giugno 2001, n.231, come modificati dalla legge 179 del 30.11.2017, nell'ambito del procedimento disciplinare, eventualmente promosso nei confronti del soggetto denunciato, l'identità del Segnalante non può essere rivelata, senza il suo consenso, sempre che la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione, l'identità può essere rivelata ove la sua conoscenza sia assolutamente indispensabile per la difesa del soggetto denunciato.
  Per quanto non espressamente previsto nel presente allegato, con particolare riferimento ad eventuali trasferimenti di dati all'estero, si rinvia al "Sistema delle regole per l'applicazione della normativa privacy nel Gruppo Telecom Italia", emesso dalla Funzione Privacy (codice 2009-00048), consultabile anche sul sito Intranet della Funzione stessa.

Allegato 3

Caselle e-mail dei Collegi Sindacali/OdV 231 delle società del Gruppo TIM

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