

Procedura Whistleblowing

Indice

1. PREMESSA	2
2. DESTINATARI	2
3. SCOPO E CAMPO DI APPLICAZIONE	3
4. RIFERIMENTI	4
5. DESCRIZIONE DEL PROCESSO E RESPONSABILITÀ	5
5.1 Scopo e descrizione del processo	5
5.2 La trasmissione della Segnalazione	5
5.3 La registrazione della Segnalazione	6
5.4 Classificazione e analisi preliminare della Segnalazione	6
5.5 L'esecuzione dell'istruttoria	8
5.6 Reporting	8
5.7 Azioni correttive: il monitoraggio	10
5.8 Trattamento dei dati personali e conservazione della documentazione	10
5.9 Controlli periodici	10
6. GARANZIE E TUTELE	10
6.1 La tutela del Segnalante	10
6.2 Misure di protezione	11
7. GLOSSARIO	12

1. PREMESSA

La presente procedura (di seguito Procedura) ha lo scopo di disciplinare il processo di trasmissione, ricezione, analisi e gestione delle Segnalazioni (cd. *Whistleblowing*) su informazioni, adeguatamente circostanziate, riferibili al Personale TIM e/o Terzi relative a violazioni di leggi e regolamenti, del Codice Etico e di Condotta del Gruppo TIM, del Modello Organizzativo 231, nonché del sistema di regole e procedure vigenti nel Gruppo TIM, tra le quali - a titolo non esaustivo - la Policy “Rispettare i Diritti Umani nel Gruppo Telecom Italia”, il Sistema di Gestione Anticorruzione di TIM, la Policy Anticorruzione del Gruppo Telecom Italia e la Procedura “Tax Risk Management”.

La procedura è anche finalizzata a dare attuazione al Decreto Legislativo 10 marzo 2023 n. 24, pubblicato in G.U. in data 15.03.2023, recante il recepimento della Direttiva (UE) 2019/1937 riguardante “la protezione delle persone che segnalano violazioni del diritto dell’Unione (cd. disciplina *Whistleblowing*)”.

Per quanto non espressamente indicato dalla presente Procedura resta integralmente applicabile quanto previsto dal suddetto Decreto Legislativo.

La predetta normativa prevede, in sintesi:

- un regime di tutela verso specifiche categorie di soggetti che segnalano informazioni, acquisite nel contesto lavorativo, relative a violazioni di disposizioni normative nazionali o dell’Unione Europea che ledono l’interesse pubblico o l’integrità dell’ente;
- misure di protezione, tra cui il divieto di ritorsioni, a tutela del Segnalante nonché dei Facilitatori, dei colleghi e dei parenti del segnalante e dei soggetti giuridici collegati al Segnalante;
- l’istituzione di canali di segnalazione interni all’ente (di cui uno di tipo informatico) per la trasmissione di Segnalazioni che garantiscano, anche tramite il ricorso a strumenti di crittografia, la tutela della riservatezza dell’identità del Segnalante, della Persona coinvolta e/o comunque menzionata nella Segnalazione, del contenuto della Segnalazione e della relativa documentazione;
- oltre alla facoltà di sporgere denuncia all’autorità giudiziaria o contabile, la possibilità (qualora ricorra una delle condizioni previste all’art. 6, comma 1, del d.lgs. n. 24/2023) di effettuare Segnalazioni esterne tramite il canale gestito dall’Autorità Nazionale Anticorruzione (di seguito ANAC), nonché di effettuare Divulgazioni pubbliche (al ricorrere di una delle condizioni previste all’art. 15, comma 1, del d.lgs. n. 24/2023), tramite la stampa o mezzi elettronici o di diffusione in grado di raggiungere un numero elevato di persone;
- provvedimenti disciplinari nonché sanzioni amministrative pecuniarie irrogate da ANAC nei casi previsti dagli artt. 16 e 21 del d.lgs. n. 24/2023.

2. DESTINATARI

Destinatari della Procedura sono:

- i Vertici aziendali e i componenti degli organi sociali e dell’Organismo di Vigilanza di TIM S.p.a. (di seguito TIM) e delle Società Controllate,
- i dipendenti, gli ex dipendenti e i candidati a posizioni lavorative, i soci, i clienti di TIM e delle Società Controllate, nonché - a titolo non esaustivo - i partner, i fornitori (anche in regime di appalto/subappalto), i consulenti, i collaboratori nello svolgimento della propria attività lavorativa presso TIM e/o le Società Controllate,

che sono in possesso di Informazioni su violazioni come definite nella presente Procedura.

Rientrano, altresì, tra i Destinatari, i soggetti fisici e giuridici, non ricompresi nelle precedenti categorie ma ai quali si applicano le misure di protezione previste dalla presente Procedura.

Quanto previsto nel presente documento si applica anche alle Segnalazioni anonime, purché adeguatamente circostanziate, come definite nella presente Procedura.

3. SCOPO E CAMPO DI APPLICAZIONE

La Procedura ha lo scopo di disciplinare il processo di trasmissione, ricezione, analisi e gestione delle Segnalazioni, compresa l'archiviazione e la successiva cancellazione sia delle Segnalazioni sia della documentazione ad esse correlata, con le modalità indicate nel presente documento.

La Procedura si applica a TIM e alle Società Controllate (come definite nella presente Procedura), che ne garantiscono la corretta e costante applicazione, nonché la massima diffusione interna ed esterna, nel rispetto delle prerogative di autonomia e indipendenza di ciascuna Società. Il presente documento costituisce inoltre un riferimento per Fondazione TIM e per le altre società controllate del Gruppo TIM non rientranti nel perimetro di applicazione della Procedura, che possono recepirla, in conformità alle normative, ai processi ed agli assetti organizzativi specifici e/o locali.

Sono escluse dal perimetro di applicazione della Procedura le Segnalazioni inerenti a:

- contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale del Segnalante, che attengono esclusivamente alla disciplina del rapporto di lavoro o ai rapporti con le figure gerarchicamente sovraordinate, salvo che siano collegate o riferibili alla violazione di norme o di regole/procedure interne;
- violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato dell'Unione Europea;
- violazioni disciplinate in via obbligatoria da atti dell'Unione Europea o nazionali, come indicati nell'art. 1, co. 2, lett. b), del d.lgs. n. 24/2023 (in materia di servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo, sicurezza dei trasporti e tutela dell'ambiente);
- fatti o circostanze rientranti nell'applicazione di disposizioni nazionali o dell'Unione Europea in materia di informazioni classificate, segreto forense o medico e di segretezza delle deliberazioni degli organi giurisdizionali, ovvero rientranti nell'applicazione di disposizioni nazionali in materia di procedura penale, di autonomia e indipendenza della magistratura, delle disposizioni sulle funzioni e attribuzioni del Consiglio Superiore della Magistratura, in materia di difesa nazionale e di ordine e sicurezza pubblica, nonché in materia di esercizio e tutela del diritto dei lavoratori di consultare i propri rappresentanti o i sindacati, di protezioni contro le condotte o gli atti illeciti posti in essere in ragione di tali consultazioni, di autonomia delle parti sociali e del loro diritto di stipulare accordi collettivi, nonché di repressione delle condotte antisindacali;
- comunicazioni relative al conflitto di interessi, ai sensi della procedura "La gestione dei conflitti di interessi Gruppo TIM". Qualora dette circostanze siano rilevanti anche ai sensi del Modello Organizzativo 231 dovranno essere oggetto di Segnalazione, come previsto dalla presente Procedura;
- le attività di competenza del Funzionario alla Sicurezza TIM, relative alla trattazione e gestione delle informazioni classificate ex DPCM 6 novembre 2015 n. 5 ("Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva") e successive modifiche;
- reclami commerciali, per i quali si rimanda ai servizi 119, 187, 191;
- richieste di esercizio dei diritti in materia di protezione dei dati personali nei confronti del Gruppo TIM (c.d. diritti privacy), ai sensi del Regolamento (UE) n. 2016/679 (Regolamento Generale sulla Protezione dei Dati - GDPR) e dei d.lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali) e successive modifiche e integrazioni, per le quali si rimanda ai dati di contatto del Data Protection Officer del Gruppo TIM e alla procedura "Sistema delle regole per l'applicazione della normativa sulla protezione dei dati personali nel Gruppo Telecom Italia". Qualora dette circostanze siano rilevanti anche ai sensi del Modello Organizzativo 231 dovranno essere oggetto di Segnalazione, come previsto dalla presente Procedura.

Le Segnalazioni rientranti nelle predette tipologie, ove pervengano attraverso i previsti canali *Whistleblowing*, verranno inoltrate alle competenti strutture aziendali a cura della Funzione Audit di TIM, che ne monitora comunque gli esiti per rilevare eventuali debolezze del sistema di controllo interno e di gestione dei rischi o impatti su processi sensibili 231.

Nel caso in cui la Segnalazione riguardi ambiti disciplinati dalla normativa “Golden Power” (per la cui definizione si rinvia alla Policy aziendale “Linee Guida Golden Power e Perimetro di Sicurezza Nazionale Cibernetica”), sono attivati meccanismi di confronto tra la Funzione Audit di TIM e le Organizzazioni di Sicurezza TIM, Sparkle e Telsy solo per l’approfondimento di aspetti inerenti alla normativa “Golden Power”, come previsto dalla citata Policy.

4. RIFERIMENTI

RIFERIMENTI NORMATIVI ESTERNI

- Decreto Legislativo 8 giugno 2001 n. 231 (“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 (Regolamento Generale sulla Protezione dei Dati - GDPR);
- Decreto Legislativo 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali) e successive modifiche ed integrazioni;
- Direttiva (UE) 2019/1937 riguardante la protezione delle persone che segnalano violazioni del diritto dell’Unione (cd. *Whistleblowing*);
- Decreto Legislativo 10 marzo 2023 n. 24, pubblicato in G.U. in data 15.03.2023, recante il recepimento della Direttiva (UE) 2019/1937;
- Decreto-legge 15 marzo 2012, n. 21, convertito in Legge 11 maggio 2012, n. 56 (“Norme in materia di poteri speciali sugli assetti societari nei settori della Difesa e della Sicurezza Nazionale, nonché per le attività di rilevanza strategica nei settori dell’Energia, dei Trasporti e delle Comunicazioni”) come modificato dalla legge 51/2022 ex DL 21/2022 (Decreto Ucraina) e successivi DPCM di approvazione dei piani 5G annuali;
- Decreto del Presidente del Consiglio dei Ministri del 28 settembre 2017 (che stabilisce che TIM è soggetta agli obblighi di cui al citato D.L. n. 21/2012);
- DPCM 6 novembre 2015 n. 5 (“Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva”) e successive modifiche;
- 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) come modificato dal DPCM 20 giugno 2025;
- DPCM 2 novembre 2017 (“Comunicazione a TIM adozione del decreto attuativo della legge sulla Golden Power”);
- Decreto-legge 21 settembre 2019, n. 105 convertito in Legge 18 novembre 2019 n. 133 (“Disposizioni urgenti in materia di Perimetro di Sicurezza Nazionale e Cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica”);
- DPCM 1 agosto 2022 n. 133 (“Nuovo Regolamento di procedura per l’esercizio dei poteri speciali”).

RIFERIMENTI NORMATIVI INTERNI

- Modello Organizzativo 231 di TIM e delle Società Controllate;
- Codice Etico e di Condotta del Gruppo TIM;
- Definizione e Formalizzazione di Policy, Procedure ed Istruzioni Operative di Gruppo;
- Policy “Rispettare i Diritti Umani nel Gruppo Telecom Italia”;
- Policy gestione degli episodi di molestia di genere, sessuale, di stalking e di bullismo;
- Gestione del procedimento disciplinare personale non Dirigente;
- Sistema di Gestione Anticorruzione di TIM e delle Società Controllate che lo adottano;
- Policy Anticorruzione del Gruppo TIM;
- Procedura Organizzativa “Tax Risk Management”;
- Procedura “La gestione dei conflitti di interessi nel Gruppo TIM”;
- Linee Guida “Golden Power e Perimetro di Sicurezza Nazionale Cibernetica”.

5. DESCRIZIONE DEL PROCESSO E RESPONSABILITÀ

5.1 Scopo e descrizione del processo

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

Per le Segnalazioni riguardanti le Società Controllate, l'*owner* del processo è il rispettivo Organismo di Vigilanza, ferme restando le citate responsabilità e prerogative del Collegio Sindacale di pertinenza.

Al fine di dare seguito alle Segnalazioni, gli Organismi di Vigilanza di TIM e della Società Controllate si avvalgono del supporto della Funzione Audit di TIM, nel rispetto dei principi stabiliti dagli Standard Internazionali per la pratica professionale dell'Internal Audit emanati dall'Institute of Internal Auditors (IIA) e dal Codice Etico e di Condotta del Gruppo TIM.

La Funzione Audit di TIM, nell'ambito delle attività di supporto all'Organismo di Vigilanza, svolge altresì gli approfondimenti istruttori richiesti da ANAC sulle Segnalazioni esterne ovvero sulle Divulgazioni pubbliche riguardanti TIM e/o le Società Controllate, dandone informativa all'Organismo di Vigilanza di riferimento.

Le Funzioni aziendali di TIM e delle Società Controllate, eventualmente interessate da Enti, Istituzioni o Autorità esterne in merito a Segnalazioni esterne o Divulgazioni pubbliche, attivano tempestivamente la Funzione Audit di TIM per gli approfondimenti di competenza.

5.2 La trasmissione della Segnalazione

I Destinatari della presente Procedura che vengono a conoscenza di Informazioni su violazioni di leggi e regolamenti, del Codice Etico e di Condotta del Gruppo TIM, del Modello Organizzativo 231, nonché del sistema di regole e procedure vigenti nel Gruppo TIM, sono tenuti ad effettuare una Segnalazione attraverso i canali di segnalazione interni di seguito descritti.

Chiunque riceve una Segnalazione, in qualsiasi forma (orale o scritta), deve trasmetterla tempestivamente, e comunque entro 7 giorni dal suo ricevimento, all'Organismo di Vigilanza di riferimento, anche per il tramite della Funzione Audit di TIM, attraverso i canali di segnalazione interni di seguito descritti, dando contestuale notizia della trasmissione al Segnalante (ove noto). È, altresì, tenuto a trasmettere l'originale della Segnalazione, inclusa eventuale documentazione di supporto, nonché l'evidenza della comunicazione al Segnalante dell'avvenuto inoltro della Segnalazione. Non può trattenere copia dell'originale e deve eliminare eventuali copie in formato digitale, astenendosi dall'intraprendere qualsiasi iniziativa autonoma di analisi e/o approfondimento. Lo stesso è tenuto alla riservatezza dell'identità del Segnalante, delle Persone coinvolte e/o comunque menzionate nella Segnalazione, del contenuto della Segnalazione e della relativa documentazione.

La mancata comunicazione di una Segnalazione ricevuta nonché la violazione dell'obbligo di riservatezza costituiscono una violazione della Procedura e potranno comportare l'adozione di provvedimenti disciplinari.

Al fine di dare diligente seguito alle Segnalazioni interne ricevute, TIM e le Società Controllate si sono dotate di un proprio Portale informatico, accessibile dalla pagina dedicata al "*Whistleblowing*" presente sia sul sito internet di TIM e delle Società Controllate (ove attivato) sia sulle rispettive pagine intranet aziendali.

Il Portale consente di trasmettere, anche in maniera anonima, sia una Segnalazione propria sia una Segnalazione ricevuta da un terzo, previa presa visione dell'"Informativa *Privacy*", pubblicata sulla pagina dedicata al "*Whistleblowing*" presente sia sul sito internet di TIM e delle Società Controllate (ove attivato) sia sulle rispettive pagine intranet aziendali.

Sui suddetti siti e pagine intranet dedicati al *Whistleblowing* è altresì pubblicata la presente Procedura e sono disponibili informazioni sui presupposti per effettuare una Segnalazione tramite canale interno nonché informazioni su canali, procedure e presupposti per effettuare le Segnalazioni esterne e le Divulgazioni pubbliche. Inoltre, è disponibile una sezione di Frequently Asked Questions (FAQ) che contiene le risposte alle domande più frequenti utili a garantire la corretta trasmissione delle Segnalazioni.

Al termine dell'inserimento, il Segnalante deve annotare la data e il Codice Identificativo Unico (ticket alfanumerico che identifica in modo univoco la Segnalazione), automaticamente prodotto dal Portale, che

consente di seguire nel tempo lo stato di lavorazione della Segnalazione, garantendo riservatezza e anonimato.

Le Segnalazioni possono essere altresì trasmesse:

- in forma orale, tramite sistemi di messaggistica vocale, al Numero Verde indicato sui predetti siti internet e pagine intranet dedicati al “*Whistleblowing*” di TIM e delle Società Controllate (ove attivato). Il canale orale è gestito operativamente dalla Funzione Audit di TIM, per conto dell’Organismo di Vigilanza di TIM e/o delle Società Controllate di riferimento, con le garanzie di riservatezza previste dalla presente Procedura;
- a mezzo posta ordinaria, indirizzata all’Organismo di Vigilanza 231 di TIM e/o delle Società Controllate, presso la sede legale della società di riferimento.

Il Segnalante può inoltre chiedere di effettuare una Segnalazione orale mediante un incontro diretto con un membro dell’Organismo di Vigilanza di TIM e/o delle Società Controllate di riferimento e/o, per suo conto, con il personale della Funzione Audit coinvolto nelle attività di supporto all’Organismo di Vigilanza di cui alla presente Procedura. In tal caso, previo consenso del Segnalante, il colloquio è documentato a cura del personale addetto mediante registrazione su un dispositivo idoneo alla conservazione e all’ascolto oppure mediante verbale, che il Segnalante può verificare, rettificare e confermare mediante sottoscrizione.

Eventuali Segnalazioni indirizzate al Collegio Sindacale di TIM o di una delle Società Controllate, incluse le denunce ex art. 2408 c.c., pervenute all’Organismo di Vigilanza di TIM e/o di una delle Società Controllate e/o alla Funzione Audit di TIM, sono trasmesse tempestivamente al Collegio Sindacale di TIM o delle Società Controllate di riferimento. Resta salva per l’Organismo di Vigilanza di TIM e/o della Società Controllata di riferimento la facoltà di svolgere autonomi approfondimenti, direttamente o con il supporto della Funzione Audit, su fatti e circostanze di rilevanza ai sensi del Modello Organizzativo 231.

Analogamente, il Collegio Sindacale di TIM o delle Società Controllate trasmette tempestivamente, e comunque entro 7 giorni dal suo ricevimento, all’Organismo di Vigilanza di TIM o di una delle Società Controllate, anche per il tramite della Funzione Audit, eventuali Segnalazioni pervenute al predetto organo sociale ma indirizzate e/o di competenza dell’Organismo di Vigilanza di riferimento ai sensi del Modello Organizzativo 231, dando contestuale notizia della trasmissione al Segnalante.

5.3 La registrazione della Segnalazione

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.

La consultazione delle informazioni presenti sul Portale è limitata al solo personale della Funzione Audit coinvolto nelle attività di supporto all’Organismo di Vigilanza di cui alla presente Procedura, abilitato con specifici profili funzionali di accesso al sistema, tracciati attraverso *log*.

I componenti dell’Organismo di Vigilanza di TIM e delle Società Controllate possono comunque accedere direttamente al Portale, tramite un apposito profilo funzionale di sola visualizzazione, per prendere visione delle Segnalazioni di rispettiva competenza.

5.4 Classificazione e analisi preliminare della Segnalazione

Il personale della Funzione Audit coinvolto nelle attività di supporto all’Organismo di Vigilanza di cui alla presente Procedura analizza e classifica le Segnalazioni, per definire quelle potenzialmente rientranti nel campo di applicazione della presente Procedura.

Nell'ambito di tali attività di supporto, la Funzione Audit di TIM fornisce al Segnalante¹ tramite il Portale:

- entro 7 giorni dalla data di ricezione della Segnalazione, un avviso di ricevimento della stessa;
- entro 3 mesi dall'avviso di ricevimento della Segnalazione o, in mancanza di tale avviso, entro 3 mesi dalla scadenza del termine di 7 giorni dalla presentazione della stessa, un riscontro con informazioni sul seguito che viene dato o si intende dare alla Segnalazione, specificando se la Segnalazione rientra o meno nell'ambito di applicazione del d.lgs. n. 24/2023.

Le Segnalazioni riguardanti episodi di molestie di genere, sessuale, di stalking e di bullismo sono trasmesse dalla Funzione Audit all'Organismo di Vigilanza di TIM a cui è attribuita la gestione delle stesse quando, in ragione della loro particolare gravità oggettiva e soggettiva, possono essere qualificate come "fatti rilevanti", potenzialmente lesivi dell'integrità etica della Società.

Ove sprovviste di tale carattere di "rilevanza", l'Organismo di Vigilanza di TIM dispone che le stesse siano trasmesse dalla Funzione Audit, per il seguito di competenza, alla Funzione Chief Human Resources & Organization Office di TIM, in applicazione di quanto previsto dalla Policy "Gestione degli episodi di molestia di genere, sessuale, di stalking e di bullismo". Al termine del processo di gestione di tali Segnalazioni, la commissione prevista dalla predetta Policy comunica alla Funzione Audit gli esiti delle verifiche effettuate e gli eventuali provvedimenti adottati dalla Funzione Chief Human Resources & Organization Office, per la successiva informativa e proposta di chiusura all'Organismo di Vigilanza di riferimento.

La Funzione Audit in via preliminare valuta, anche tramite eventuali analisi documentali, la sussistenza dei presupposti necessari per l'avvio della successiva fase istruttoria, dando priorità alle Segnalazioni adeguatamente circostanziate, e comunica le suddette evidenze all'Organismo di Vigilanza di TIM e, per le Segnalazioni sulle Società Controllate, anche all'Organismo di Vigilanza della Società Controllata di riferimento.

Per le Segnalazioni di propria competenza, l'Organismo di Vigilanza, su base documentale e anche in considerazione degli esiti delle preliminari analisi svolte dalla Funzione Audit, valuta:

- l'avvio della successiva fase di istruttoria;
- per le "Segnalazioni relative a fatti rilevanti", la tempestiva informativa al Comitato per il controllo e i rischi e al Collegio Sindacale di riferimento, per le autonome valutazioni;
- la chiusura delle Segnalazioni, in quanto: i) generiche o non adeguatamente circostanziate; ii) palesemente infondate; iii) riferite a fatti e/o circostanze oggetto in passato di specifiche attività istruttorie già concluse, ove dalle preliminari verifiche svolte non emergano nuove informazioni tali da rendere necessari ulteriori approfondimenti; iv) "circostanziate verificabili", per le quali, alla luce degli esiti delle preliminari verifiche svolte, non emergono elementi tali da supportare l'avvio della successiva fase di istruttoria; v) "circostanziate non verificabili", per le quali, alla luce degli esiti delle preliminari verifiche svolte, non risulta possibile, sulla base degli strumenti di analisi a disposizione, svolgere ulteriori approfondimenti per verificare la fondatezza della Segnalazione.

Al fine di acquisire elementi informativi, l'Organismo di Vigilanza ha facoltà di:

- richiedere alla Funzione Audit, fermi restando i vigenti flussi informativi, l'attivazione di audit sui fatti segnalati;
- svolgere, anche direttamente, nel rispetto di eventuali specifiche normative applicabili, approfondimenti tramite, ad esempio, formale convocazione e audizioni del Segnalante, del Segnalato e/o delle Persone coinvolte nella Segnalazione e/o comunque informate sui fatti, nonché richiedere ai predetti soggetti la produzione di relazioni informative e/o documenti;
- avvalersi, se ritenuto opportuno, di esperti o periti esterni a TIM e/o alle Società Controllate.

¹ Tali indicazioni non si applicano nei casi in cui risulti impossibile dare riscontro al segnalante (es. segnalazione tramite lettera cartacea anonima ricevuta presso la sede aziendale e/o da dipendenti/componenti degli organi di controllo).

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, il Presidente dell'Organismo di Vigilanza di TIM informa i Presidenti del Consiglio di Amministrazione e del Collegio Sindacale di TIM per la gestione congiunta.

Se la Segnalazione coinvolge uno dei tre Presidenti, lo stesso è sostituito dal componente dell'organo sociale/Organismo di Vigilanza di TIM anagraficamente più anziano. Se la Segnalazione coinvolge l'intero organo sociale/Organismo di Vigilanza di TIM, l'istruttoria sarà gestita dai Presidenti degli altri due organi sociali/Organismo di Vigilanza di TIM.

Se la Segnalazione riguarda il Responsabile della Funzione Audit di TIM e/o le Funzioni dallo stesso dipendenti il Presidente dell'Organismo di Vigilanza di TIM informa i Presidenti del Consiglio di Amministrazione e del Collegio Sindacale di TIM per la gestione congiunta.

Nelle predette ipotesi gli esiti degli approfondimenti istruttori sono oggetto di una nota di chiusura della Segnalazione a firma dei Presidenti che hanno gestito congiuntamente la Segnalazione. Gli esiti degli approfondimenti istruttori sono altresì sintetizzati in un report condiviso periodicamente con l'Organismo di Vigilanza, il Collegio Sindacale e il Consiglio di Amministrazione, garantendo le tutele previste per segnalanti, segnalati e altri soggetti protetti (es. soggetti intervistati).

5.5 L'esecuzione dell'istruttoria

La fase istruttoria della Segnalazione ha l'obiettivo di:

- procedere, nei limiti degli strumenti a disposizione della Funzione Audit, ad approfondimenti e analisi specifiche per verificare la ragionevole fondatezza delle circostanze fattuali segnalate;
- ricostruire i processi gestionali e decisionali seguiti sulla base della documentazione e delle evidenze rese disponibili;
- fornire eventuali indicazioni in merito all'adozione delle necessarie azioni di rimedio volte a correggere possibili carenze di controllo, anomalie o irregolarità rilevate sulle aree e sui processi aziendali esaminati.

Non rientrano nel perimetro di analisi dell'istruttoria, se non nei limiti della manifesta irragionevolezza, le valutazioni di merito o di opportunità, discrezionali o tecnico-discrezionali, degli aspetti decisionali e gestionali di volta in volta operate dalle strutture/posizioni aziendali coinvolte, in quanto di esclusiva competenza di queste ultime.

La Funzione Audit nel corso degli approfondimenti può richiedere integrazioni o chiarimenti al Segnalante. Inoltre, ove ritenuto utile per gli approfondimenti, può acquisire informazioni dalle Persone coinvolte nella Segnalazione, le quali hanno anche facoltà di chiedere di essere sentite o di produrre osservazioni scritte o documenti. In tali casi, anche al fine di garantire il diritto di difesa, viene dato avviso alla Persona coinvolta dell'esistenza della Segnalazione, pur garantendo la riservatezza sull'identità del Segnalante e delle altre Persone coinvolte e/o menzionate nella Segnalazione.

La Funzione 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.

Le attività istruttorie sono svolte ricorrendo, a titolo non esaustivo, a: i) dati/documenti aziendali utili ai fini dell'istruttoria (es. estrazioni da sistemi aziendali e/o altri sistemi specifici utilizzati); ii) banche dati esterne (es. info provider/banche dati su informazioni societarie); iii) fonti aperte; iv) evidenze documentali acquisite presso le strutture aziendali; v) ove opportuno, dichiarazioni rese dai soggetti interessati o acquisite nel corso di interviste verbalizzate.

5.6 Reporting

A conclusione di ciascuna attività istruttoria gli esiti sono comunicati all'Organismo di Vigilanza di TIM e, per le Segnalazioni sulle Società Controllate, anche all'Organismo di Vigilanza della Società Controllata di riferimento.

Gli esiti degli approfondimenti sono sintetizzati in un report condiviso periodicamente con l'Organismo di

Vigilanza o, per le Segnalazioni “relative a fatti rilevanti” e/o con analisi complesse, in una nota istruttoria, in cui sono riportati:

- un giudizio di ragionevole fondatezza/non fondatezza sui fatti segnalati;
- l’esito delle attività svolte e le risultanze di eventuali precedenti attività istruttorie svolte sui medesimi fatti/soggetti segnalati o su fatti analoghi a quelli oggetto della Segnalazione;
- eventuali indicazioni in merito alle necessarie azioni correttive sulle aree e sui processi aziendali esaminati, adottate dal competente *management* che viene informato sugli esiti delle analisi.

Al termine dell’attività istruttoria, l’Organismo di Vigilanza di riferimento delibera la chiusura della Segnalazione evidenziando l’eventuale inosservanza di norme/procedure, fatte salve le esclusive prerogative e competenze della Funzione Chief Human Resources & Organization Office quanto all’esercizio dell’azione disciplinare.

Inoltre, se all’esito dell’istruttoria emergono:

- possibili fattispecie di rilevanza penale o di responsabilità civile, l’Organismo di Vigilanza può disporre di comunicare le risultanze alla Funzione Legal, Regulatory & Tax, per le valutazioni di competenza;
- ipotesi di inosservanza di norme/procedure o fatti di possibile rilevanza sotto il profilo disciplinare o giuslavoristico, l’Organismo di Vigilanza dispone di comunicare gli esiti alla Funzione Chief Human Resources & Organization Office, per le valutazioni di competenza, che provvede a dare comunicazione all’Organismo di Vigilanza delle determinazioni assunte. Inoltre, la Funzione Chief Human Resources & Organization Office di TIM fornisce trimestralmente all’Organismo di Vigilanza un’informativa sui provvedimenti disciplinari assunti a seguito di approfondimento di Segnalazioni.

Le Segnalazioni chiuse, in quanto palesemente infondate, se non anonime, sono trasmesse alla Funzione Chief Human Resources & Organization Office 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.

La Funzione Audit fornisce mensilmente all’Organismo di Vigilanza di TIM un report di sintesi di tutte le Segnalazioni pervenute nel periodo e di dettaglio di quelle rientranti nel perimetro della Procedura, con l’evidenza dello stato di avanzamento e degli esiti delle istruttorie concluse, per le quali propone la chiusura.

A valle dell’informativa verso l’Organismo di Vigilanza di TIM, la Funzione Audit fornisce periodicamente al Comitato per il controllo e i rischi e al Collegio Sindacale di TIM un report di sintesi delle Segnalazioni pervenute e degli esiti delle attività istruttorie concluse.

Anche su richiesta dei predetti organi sociali, l’Organismo di Vigilanza può disporre la comunicazione del dettaglio degli approfondimenti svolti ovvero la trasmissione delle note istruttorie di chiusura delle Segnalazioni.

A valle dell’informativa verso l’Organismo di Vigilanza, inoltre, la Funzione Audit di TIM comunica eventuali elementi di riscontro emersi dagli approfondimenti in merito a sospette frodi con potenziali impatti:

- sotto il profilo fiscale, alla Funzione Compliance - Compliance Operations & Assurance, per quanto di competenza, e alla Funzione Legal, Regulatory & Tax - Tax Office - Direct Taxes and Tax Risk Management, per l’attivazione del processo di istruttoria con il coinvolgimento della Funzione Tax Office competente, come previsto dalla Procedura “Tax risk management” di TIM;
- in materia di anticorruzione, alla Funzione di conformità per la prevenzione della corruzione di TIM e/o della Società Controllata di riferimento, individuata ai sensi del Sistema di Gestione Anticorruzione, secondo lo Standard ISO 37001, per le attività di competenza.

Inoltre, la Funzione Audit fornisce:

- semestralmente alla Funzione di conformità per la prevenzione della corruzione di TIM e delle Società Controllate di riferimento, informazioni di sintesi sul numero e tipologia di Segnalazioni pervenute riguardanti possibili illeciti di natura corruttiva;

- semestralmente alla Funzione Legal, Regulatory & Tax di TIM informazioni di sintesi sul numero e tipologia di Segnalazioni pervenute riguardanti condotte sospette o presunte violazioni della normativa antitrust e del Codice di condotta Antitrust del Gruppo TIM;
- annualmente alla Funzione Sustainability di TIM i contributi di competenza ai fini della redazione della Relazione di sostenibilità del Gruppo TIM, con particolare riferimento alle Segnalazioni rientranti nel perimetro di applicazione della Policy “Rispettare i Diritti Umani nel Gruppo Telecom Italia”.

5.7 Azioni correttive: il monitoraggio

Se dalle analisi sulle aree e sui processi aziendali esaminati emerge la necessità di formulare raccomandazioni volte all'adozione di opportune azioni di rimedio, è responsabilità del *management* delle aree/processi oggetto di verifica definire un piano di azioni correttive per la rimozione delle criticità rilevate e di garantirne l'implementazione entro le tempistiche definite, dandone comunicazione alla Funzione Audit che cura il monitoraggio sullo stato di attuazione delle azioni.

L'Organismo di Vigilanza di riferimento monitora l'avanzamento delle azioni correttive attraverso l'informativa periodicamente fornita dalla Funzione Audit.

5.8 Trattamento dei dati personali e conservazione della documentazione

Ogni trattamento dei dati personali, anche nel contesto del Portale, è effettuato nel rispetto degli obblighi di riservatezza di cui all'art. 12 del d.lgs. n. 24/2023 ed in conformità alla normativa sulla protezione dei dati personali di cui al Regolamento (UE) 2016/679 (Regolamento Generale sulla Protezione dei Dati – GDPR), al decreto legislativo 30 giugno 2003 n. 196 e al decreto legislativo 18 maggio 2018 n. 51.

La tutela dei dati personali è assicurata oltre che al Segnalante (per le segnalazioni non anonime), al Facilitatore nonché alla Persona coinvolta o menzionata nella segnalazione.

Ai possibili interessati viene resa un'informativa sul trattamento dei dati personali attraverso la pubblicazione sul portale dedicato.

In ottemperanza all'art. 13, comma 6, del d.lgs. n. 24/2023, è stato effettuato un Privacy Impact Assessment (PIA), redatto ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (Regolamento Generale sulla Protezione dei Dati - GDPR), al fine di definire le misure tecniche ed organizzative necessarie a ridurre il rischio per i diritti degli interessati, comprese le misure di sicurezza necessarie a prevenire trattamenti non autorizzati o illeciti.

Al fine di garantire la gestione e la tracciabilità delle Segnalazioni e delle attività conseguenti, la Funzione Audit cura la predisposizione e l'aggiornamento di tutte le informazioni riguardanti le Segnalazioni ed assicura, avvalendosi del Portale, la conservazione di tutta la correlata documentazione di supporto per il tempo strettamente necessario alla loro definizione, e comunque per non più di 5 anni, decorrenti dalla data di comunicazione dell'esito finale della Segnalazione all'Organismo di Vigilanza.

I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati tempestivamente.

Gli originali delle segnalazioni pervenute in forma cartacea sono conservati in apposito ambiente protetto.

5.9 Controlli periodici

Con periodicità semestrale, viene svolto un controllo di completezza, a cura di personale della Funzione Audit diverso da quello coinvolto nelle attività di supporto all'Organismo di Vigilanza di cui alla presente Procedura, 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 presente Procedura.

6. GARANZIE E TUTELE

6.1 La tutela dell'identità del Segnalante

Le Segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse.

Fatti salvi gli obblighi di legge, l'identità del Segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate, senza il consenso espresso dello stesso, a persone diverse da quelle competenti a ricevere o a dare seguito alle Segnalazioni, espressamente autorizzate a trattare tali dati ai sensi degli artt. 29 e 32, par. 4, del Regolamento (UE) 2016/679 (Regolamento Generale sulla Protezione dei Dati – GDPR) e dell'art. 2 - *undecies* del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).

In particolare, l'identità del Segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità possono essere rivelate solo previo consenso espresso dello stesso:

- nell'ambito del procedimento disciplinare, qualora la contestazione sia fondata, in tutto o in parte, sulla Segnalazione e la conoscenza dell'identità del Segnalante sia indispensabile per la difesa dell'incolpato;
- nell'ambito del procedimento instaurato in seguito a Segnalazioni interne o esterne, se la rivelazione dell'identità del Segnalante o di qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità è indispensabile anche ai fini della difesa della Persona coinvolta.

A tal fine, in tali casi è data preventiva comunicazione scritta, al Segnalante delle ragioni della rivelazione dei dati riservati.

Il personale del Gruppo TIM coinvolto nella gestione delle Segnalazioni è tenuto alla riservatezza dell'identità del Segnalante, delle Persone coinvolte e/o comunque menzionate nella Segnalazione, del contenuto della Segnalazione e della relativa documentazione.

La riservatezza è garantita anche a chi segnala prima dell'inizio o successivamente alla cessazione del rapporto di lavoro, ovvero nel periodo di prova, qualora dette informazioni siano state acquisite nell'ambito del contesto lavorativo oppure nella fase selettiva o precontrattuale.

È altresì garantita la riservatezza sull'identità delle Persone coinvolte e/o menzionate nella Segnalazione, nonché sull'identità e sull'assistenza prestata dai Facilitatori, con le medesime garanzie previste per il Segnalante.

La violazione dell'obbligo di riservatezza, fatte salve le eccezioni di cui sopra, può comportare nei confronti dell'interessato l'irrogazione di sanzioni amministrative pecuniarie da parte di ANAC nonché l'adozione di provvedimenti disciplinari da parte della Funzione Chief Human Resources & Organization Office, in linea con le previsioni di cui al paragrafo 8 del Modello Organizzativo 231 ("Sistema Disciplinare").

6.2 Misure di protezione

Nei confronti del Segnalante è vietato il compimento di atti ritorsivi, intesi come qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della Segnalazione interna o esterna/Divulgazione pubblica/denuncia, che provoca o può provocare al Segnalante, in via diretta o indiretta, un danno ingiusto.

La protezione è garantita anche al Segnalante anonimo, che ritiene di aver subito ritorsioni ed è stato successivamente identificato.

Le misure di protezione si applicano nei limiti e alle condizioni previste dal capo III del d.lgs. n. 24/2023 e sono estese anche a:

- le categorie di Segnalanti che non rientrano nell'ambito di applicazione oggettivo e/o soggettivo previsto dal d.lgs. n. 24/2023;
- i Facilitatori, le persone del medesimo contesto lavorativo del Segnalante che sono legate ad esso da uno stabile legame affettivo o di parentela entro il quarto grado, i colleghi di lavoro del Segnalante che lavorano nel medesimo contesto lavorativo e che hanno con esso un rapporto abituale e corrente;
- gli enti di proprietà del Segnalante o per i quali lo stesso lavora nonché gli enti che operano nel medesimo contesto lavorativo del Segnalante.

Chi ritiene di aver subito una ritorsione in ragione della Segnalazione può comunicarlo ad ANAC.

Gli atti ritorsivi eventualmente assunti in ragione della Segnalazione sono nulli e le persone che sono state licenziate a causa della Segnalazione hanno diritto a essere reintegrate nel posto di lavoro in attuazione della disciplina applicabile al lavoratore.

Ferma restando l'esclusiva competenza di ANAC in merito all'eventuale applicazione delle sanzioni amministrative di cui all'art. 21 del d.lgs. n. 24/2023, si rinvia alla specifica disciplina contenuta al paragrafo 8 del Modello Organizzativo 231 ("Sistema Disciplinare") per eventuali conseguenze sul piano disciplinare di competenza della Funzione Chief Human Resources & Organization Office.

7. GLOSSARIO

Ai fini della presente Procedura si intende per:

- **Contesto lavorativo:** le attività lavorative o professionali, presenti o passate, svolte dal Personale TIM o dal Terzo nell'ambito dei rapporti giuridici da questi instaurati con TIM S.p.a. (di seguito TIM) e/o con le Società Controllate;
- **Divulgazione pubblica:** rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone. Ai sensi dell'art. 15, comma 1, del d.lgs. n. 24/2023, il Segnalante può effettuare una divulgazione pubblica qualora ricorra una delle seguenti condizioni: i) ha già effettuato una Segnalazione sia interna sia esterna, ovvero ha effettuato direttamente una Segnalazione esterna e non è stato dato riscontro nei termini previsti in merito alle misure previste o adottate per dare seguito alle Segnalazioni; ii) ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse; iii) ha fondato motivo di ritenere che la Segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto, come quelle in cui possano essere occultate o distrutte prove oppure in cui vi sia fondato timore che chi ha ricevuto la Segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa;
- **Facilitatore:** la persona fisica che assiste il Segnalante nel processo di Segnalazione e che opera nel medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata;
- **Gruppo TIM:** TIM e/o le sue società controllate;
- **Informazioni sulle violazioni:** informazioni, adeguatamente circostanziate, compresi i fondati sospetti, riguardanti violazioni conseguenti a comportamenti, atti od omissioni commessi o che, sulla base di elementi concreti, potrebbero essere commessi nonché elementi riguardanti condotte, anche omissive, volte ad occultare tali violazioni. Rientrano anche le informazioni su violazioni acquisite nell'ambito di un rapporto giuridico non ancora iniziato o nel frattempo terminato, qualora dette informazioni siano state acquisite nell'ambito del contesto lavorativo, compreso il periodo di prova, oppure nella fase selettiva o precontrattuale;
- **Modello Organizzativo 231:** il modello di organizzazione, gestione e controllo adottato da TIM e dalle Società Controllate ai sensi del d.lgs. n. 231/2001;
- **Organismo di Vigilanza:** l'Organismo di TIM, ovvero il Collegio Sindacale delle Società Controllate nelle funzioni di Organismo di Vigilanza, nominato ai sensi dell'art. 6, punto 1, lett. b) del d.lgs. n. 231/2001, dotato di autonomi poteri d'iniziativa e controllo che ha il compito di vigilare sul funzionamento e sull'osservanza del Modello Organizzativo 231 e di curarne l'aggiornamento;
- **Persona coinvolta:** la persona fisica o giuridica menzionata nella Segnalazione effettuata tramite il canale interno o esterno, denuncia, Divulgazione pubblica, come soggetto a cui la violazione è attribuita o comunque riferibile;
- **Personale TIM:** coloro che sono legati a TIM o alle Società Controllate da un rapporto di lavoro subordinato o di prestazione occasionale nonché i Vertici aziendali e i componenti degli organi sociali e dell'Organismo di Vigilanza di TIM e delle Società Controllate (anche qualora esercitino tali funzioni in via di mero fatto);

- **Segnalante:** la persona che effettua una Segnalazione tramite il canale di Segnalazione interno o esterno, denuncia, Divulgazione pubblica;
- **Segnalazione:** la comunicazione, scritta o orale, di informazioni riferibili al Personale TIM e/o a Terzi su violazioni di leggi e regolamenti, del Codice Etico e di Condotta del Gruppo TIM, del Modello Organizzativo 231, nonché del sistema di regole e procedure vigenti nel Gruppo TIM, tra le quali - a titolo non esaustivo - la Policy “Rispettare i Diritti Umani nel Gruppo Telecom Italia”, la Procedura “Tax Risk Management”, il Sistema di Gestione Anticorruzione di TIM e la Policy Anticorruzione del Gruppo Telecom Italia;
- **Segnalazione anonima:** Segnalazione in cui le generalità del Segnalante non sono esplicitate né risultano identificabili in maniera univoca;
- **Segnalazione circostanziata:** Segnalazione in cui le informazioni/asserzioni sono caratterizzate da un grado di dettaglio sufficiente, almeno astrattamente, a far emergere circostanze e fatti precisi e concordanti e relazionate a contesti determinati, nonché a consentire di identificare elementi utili ai fini della verifica della fondatezza della Segnalazione stessa (ad esempio, elementi che consentono di identificare il soggetto che ha posto in essere i fatti segnalati, il contesto, il luogo e il periodo temporale delle circostanze segnalate, valore, cause e finalità delle condotte, anomalie relative al sistema di controllo interno, documentazione a supporto, ecc.). Nell’ambito delle Segnalazioni circostanziate si distinguono le informazioni/asserzioni: i) “verificabili”, qualora in base ai contenuti della Segnalazione sia possibile in concreto svolgere verifiche in ambito aziendale sulla fondatezza, nei limiti delle attività e con gli strumenti di analisi a disposizione di Audit; ii) “non verificabili”, qualora sulla base degli strumenti di analisi a disposizione, non risulta possibile svolgere verifiche sulla fondatezza della Segnalazione. Le verifiche su circostanze e valutazioni riconducibili ad elementi intenzionali e/o soggettivi risentono dei limiti propri delle attività di Audit e dei relativi strumenti a disposizione;
- **Segnalazione esterna:** la comunicazione, scritta od orale, di Informazioni sulle violazioni effettuata dal Segnalante tramite il canale di segnalazione esterno attivato dall’Autorità Nazionale Anticorruzione (ANAC). Ai sensi dell’art. 6, comma 1, del d.lgs. n. 24/2023, il Segnalante può effettuare una Segnalazione esterna qualora ricorra una delle seguenti condizioni: i) non è prevista, nell’ambito del suo contesto lavorativo, l’attivazione obbligatoria del canale di segnalazione interna ovvero questo, anche se obbligatorio, non è attivo o, anche se attivato, non è conforme; ii) ha già effettuato una Segnalazione interna e la stessa non ha avuto seguito; iii) ha fondati motivi di ritenere che, se effettuasse una Segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero determinerebbe condotte ritorsive; iv) ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- **Segnalazione interna:** la comunicazione, scritta od orale, di Informazioni sulle violazioni effettuata dal segnalante tramite il canale interno;
- **Segnalazione relativa a fatti rilevanti:** i) Segnalazione che riguarda i Vertici aziendali e i componenti degli organi sociali e dell’Organismo di Vigilanza di TIM e/o delle Società Controllate; ii) Segnalazione per la quale, anche dalle preliminari analisi, siano configurabili gravi violazioni al Modello Organizzativo 231, tali da esporre la società al rischio di responsabilità penale-amministrativa ai sensi del d.lgs. n. 231/2001; iii) Segnalazione su anomalie operative aziendali e/o illeciti e/o frodi e/o abusi per le quali, all’esito delle verifiche preliminari, sia stimabile per TIM e/o per le Società Controllate un impatto quali-quantitativo significativo sul bilancio (in termini di tematiche di contabilità, revisione legale dei conti, controlli interni sull’informativa finanziaria). 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. La significatività dell’impatto sotto l’aspetto quantitativo viene valutata dall’Organismo di Vigilanza d’intesa con il Chief Financial Office della società di riferimento;
- **Società Controllate:** le società controllate del Gruppo TIM, escluse le società quotate e quelle estere, alle quali si applica in via diretta la presente Procedura;
- **Terzi:** le persone fisiche o giuridiche, diverse dal Personale TIM, che intrattengono, a vario titolo, rapporti di lavoro, di collaborazione o d’affari con TIM e/o con le Società Controllate, ivi compresi - a titolo non esaustivo - i clienti, i partner, i fornitori (anche in regime di appalto/subappalto), i lavoratori autonomi o titolari di rapporti di collaborazione, i liberi professionisti, i consulenti, gli agenti e intermediari, i volontari



e tirocinanti (retribuiti o non retribuiti), ovvero chiunque sia legittimo portatore di interesse nei confronti dell'attività aziendale del Gruppo TIM.