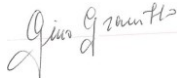
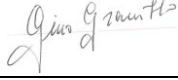
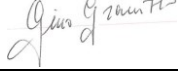


Registrazione delle Revisioni					
Rev.	Data	Descrizione della revisione	Redatto	Verificato RSI	Approvato PRE
00	04/01/22	Prima emissione a seguito adeguamento al mod.231 ed alla SA 8000	Federico Variati	Federico Variati	
01	15/02/22	Introduzione casella elettronica ente di certificazione	Federico Variati	Federico Variati	
02	24/11/22	Introduzione concetti ISO 37001 e Whistleblowing	Federico Variati	Federico Variati	

Lista di distribuzione			
Acronimo	Funzione	Acronimo	Funzione
PRE	Presidente CdA	CdA	Membri del CdA
AMM	Resp. Amministrazione	ACQ	Resp. Acquisti e Gare
COG	Resp. Controllo di gestione	COM	Resp. Commerciale
RPV	Resp. Divisione PV	TEC	Resp. Tecnico
GES	Resp. Operativo Acque (Lombardia)	ROA	Resp. Operativo Acque (Acerra)
RDW	Resp. Divisione Acque	ROW	Resp. Operativo Acque (Colleferro)
RDM	Resp. Divisione Meccanica	RSI	Resp. Sistema Gestione Integrato
RSPP	Resp. Servizio Prev. & Protezione	RU	Resp. delle Risorse Umane
LEG	Resp. Affari Legali	RIN	Resp. Sistemi Informatici
RRS	Resp. Ricerca & Sviluppo	SPT	Social Performance Team
OdV	Organismo di Vigilanza	RPC	Resp. Prevenzione della Corruzione
RLS	Rappresentante dei Lavoratori per la Sicurezza		

Indice

1	Scopo e campo di applicazione	3
1.1	Premessa	3
1.2	Scopo	3
2	Termini e definizioni	3
3	Documenti di riferimento	5
4	Riferimenti normativi.....	5
5	Oggetto della segnalazione.....	5
6	Contenuto della segnalazione	6
7	Destinatari della procedura (segnalanti)	6
8	Destinatario della segnalazione	7
9	Modalità di trasmissione della segnalazione.....	7
10	Il portale <i>Whistleblowing</i>	8
11	Gestione della segnalazione	9
12	Tutela e responsabilità del segnalante.....	9
13	Tutela del segnalato	10
14	Conservazione della documentazione e tutela della privacy	10
15	Sanzioni.....	11
16	Aggiornamento della policy	11
17	Sensibilizzazione.....	11
18	Allegati.....	11

1 Scopo e campo di applicazione

1.1 Premessa

Il 29 dicembre 2017 è entrata in vigore la legge 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" (pubblicata sulla Gazzetta Ufficiale, Serie Generale n. 291 del 14 dicembre 2017).

La struttura del provvedimento distingue la disciplina del settore pubblico (art. 1) da quella del settore privato (art. 2), ed è stata integrata la disposizione sull'obbligo del segreto d'ufficio, aziendale, professionale, scientifico e industriale (art. 3).

Per quanto riguarda il settore privato, l'articolo 2 della legge n. 179/17 interviene sul decreto 231 e inserisce all'articolo 6 ("Soggetti in posizione apicale e modelli di organizzazione dell'ente") una nuova previsione che inquadra nell'ambito del Modello organizzativo ex D. Lgs. 231/01 le misure legate alla presentazione e gestione delle segnalazioni.

La legge mira a incentivare la collaborazione dei lavoratori per favorire l'emersione di fenomeni corruttivi all'interno di enti pubblici e privati, anche con la previsione di sistemi che consentono ai lavoratori di segnalare in condizioni di sicurezza gli eventuali illeciti di cui vengono a conoscenza.

Infatti la legge disciplina:

- il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
- l'introduzione di sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate;
- la possibilità per il segnalante o l'organizzazione sindacale di denunciare all'Ispettorato nazionale del lavoro l'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni;
- la nullità del licenziamento ritorsivo o discriminatorio, nonché del mutamento di mansioni ai sensi dell'articolo 2103 del codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante;
- l'onere a carico del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, di dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.

Tea Tek (di seguito indicato come "Società") nello spirito di dare concreta applicazione all'art. 6 comma 2-bis lett. a) e b) del D. Lgs. 231/2001, come introdotto dalla Legge 179/2017, ha posto a disposizione dei segnalanti, per effettuare le segnalazioni, oltre al canale tradizionale costituito dalla posta raccomandata, un "Portale Whistleblowing" - idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante nelle attività di gestione delle segnalazioni.

1.2 Scopo

La presente procedura si propone di disciplinare il processo di ricezione, analisi e gestione delle Segnalazioni trasmesse, da parte del personale e di soggetti terzi al fine di denunciare fenomeni illeciti e comportamenti sospetti, irregolarità nella conduzione aziendale, atti o fatti che possano costituire una violazione delle norme, interne ed esterne, che disciplinano l'attività della Società, dei principi e delle regole di comportamento contenuti nel Codice Etico, nonché delle previsioni contenute nel Modello 231 e nel SGI, adeguato alle normative SA 8000 e ISO 37001, adottato dalla Società.

2 Termini e definizioni

Termini, acronimi e definizioni sono riportati nel Manuale del SGI, nei documenti di riferimento e nel D.Lgs. 81/2008. Nel seguito si riportano quelli di interesse per la presente procedura:

CdA (Consiglio di Amministrazione): Organo collegiale al quale è affidata la gestione della società per azioni;

Presidente CdA: Membro del CdA che presiede il consiglio di amministrazione. Detiene la rappresentanza legale della società ed è tenuto ad agire secondo quanto deliberato dal CdA stesso. Definisce la Politica e le strategie aziendali. Definito anche Datore di Lavoro;

SPT (Social Performance Team): Termine utilizzato per indicare un gruppo di lavoro “misto” costituito dai Rappresentanti dei Lavoratori per la SA 8000 e rappresentanti della Direzione (*management*). Questo team ha un ruolo cruciale nell’implementazione della SA8000, in quanto esso è tenuto a condurre periodicamente e in forma scritta delle valutazioni dei rischi per identificare ed attribuire un ordine di priorità alle aree di reale o potenziale non conformità allo standard;

Audit: Attività atta a misurare la conformità di determinati sistemi, processi, prodotti a determinate caratteristiche richieste e a verificarne l’applicazione;

Datore di Lavoro: Soggetto titolare del rapporto di lavoro nel cui ambito il lavoratore presta la propria attività o, comunque, ha la responsabilità dell’organizzazione stessa o dell’unità produttiva in quanto esercita poteri decisionali e di spesa;

Non Conformità: si definisce “Non Conformità” il “non soddisfacimento di requisiti specificati”, od anche “anomalia”, gli “inconvenienti”, le “carenze”, i “comportamenti non corretti” rilevati nello svolgimento delle attività aziendali, nei limiti in cui tali situazioni risultano in contrasto con specifiche, disposizioni, direttive, norme, procedure, vincoli tecnici, etc. che regolamentano le attività stesse o comunque risultino in contrasto con la funzionalità del servizio erogato;

Organismo di Vigilanza (OdV): indica un [organo](#) che vigili sulla [responsabilità degli enti](#), per reati commessi nell’interesse o vantaggio a favore di questi ultimi;

Rappresentante dei Lavoratori per la Sicurezza: “Persona eletta o designata per rappresentare i lavoratori per quanto concerne gli aspetti della salute e della sicurezza durante il lavoro”. È la figura che rappresenta gli altri lavoratori nell’ambito della sicurezza e prevenzione nei luoghi di lavoro. Da non confondere o considerare responsabile in quanto trattasi esclusivamente di un rappresentante, rappresenta infatti l’intermediario tra il Datore di Lavoro e i lavoratori stessi. È una delle figure principali della sicurezza in quanto tocca direttamente con mano la realtà lavorativa aziendale e può scorgere problematiche che il Datore di Lavoro e/o il Responsabile del Servizio di Prevenzione e Protezione potrebbero non vedere. Il Responsabile dei Lavoratori per la Sicurezza raccoglie tutte le richieste, in ambito della sicurezza e della salute, da parte di tutti gli altri lavoratori per porle al Datore di Lavoro, al fine del miglioramento della realtà aziendale;

Responsabile del Servizio di Prevenzione e Protezione: Si tratta della figura in possesso dei requisiti e delle capacità di cui all’art.32 D. Lgs. 81/2008. Per lo svolgimento delle funzioni specifiche è richiesto un attestato di frequenza, con verifica dell’apprendimento, a specifici corsi di formazione adeguati alla natura dei rischi presenti sul luogo di lavoro e relativi alle attività lavorative. Il Responsabile del Servizio di Prevenzione e Protezione svolge essenzialmente funzioni e compiti di supporto tecnico ed organizzativo per il Datore di Lavoro, i dirigenti, i preposti; inoltre ha compiti relazionali con i lavoratori e i loro rappresentanti (es. informazione ai lavoratori), anche su specifici problemi riguardanti l’azienda;

Responsabile del Sistema di gestione Integrato: Funzione avente la responsabilità di implementare il Sistema di gestione Integrato sulla base degli obiettivi definiti dalla Direzione e di farsi garante della conformità del Sistema alle norme di riferimento (quali ad esempio, ISO 9001, ISO14001, etc.). In riferimento ad una specifica norma, ad esempio la ISO 9001, egli assume il ruolo di Assicurazione della Qualità;

Responsabile per la prevenzione della corruzione: La persona o le persone aventi la responsabilità e l’autorità per il funzionamento del sistema di gestione per la prevenzione della corruzione;

PRE vedi Presidente CdA;

MI	Manuale del sistema di gestione Integrato;
OdV	Organismo di Vigilanza;
RPC	Responsabile per la prevenzione della corruzione;
RSI	vedi Responsabile del Sistema di gestione Integrato;
SIG	Sistema di gestione Integrato;
SPT	Social Performance Team.

3 Documenti di riferimento

- ❖ Manuale del sistema di gestione Integrato (MI);
- ❖ Manuale del sistema di responsabilità sociale (MRS);
- ❖ Modello organizzativo 231;
- ❖ Codice Etico;
- ❖ Politica di responsabilità sociale AL10MI01-POL;
- ❖ PR01-DOC "Gestione della documentazione e della comunicazione";

4 Riferimenti normativi

- ❖ D. Lgs. 231/01 "Disciplina della responsabilità amministrativa delle persone giuridiche, delle Società e delle associazioni anche prive di personalità giuridica, a norma dell'art.11 della legge 29 settembre 2000, n. 300" del 08/06/2011 e successivi aggiornamenti;
- ❖ D. Lgs. n. 196 del 30 giugno 2003 – Codice in materia di protezione dei dati personali – e successive modifiche e/o variazioni;
- ❖ Regolamento UE 2016/679 del Parlamento e del Consiglio del 27 aprile 2016 relativo alla Protezione delle persone fisiche con riguardo al trattamento dei dati personali;
- ❖ Legge 30 novembre 2017 n° 179, G.U. 14/12/2017 "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";
- ❖ SA 8000:2014 (*Social Accountability International*) norma internazionale sulla responsabilità sociale di impresa;
- ❖ UNI ISO 37001:2016 "Sistemi di gestione per la prevenzione della corruzione- Requisiti e guida all'utilizzo".

5 Oggetto della segnalazione

L'obbligo di segnalazione vige ogni qual volta il destinatario del Modello abbia il ragionevole e legittimo sospetto o la consapevolezza – entrambi fondati su elementi di fatto precisi e concordanti - di comportamenti penalmente illeciti o comunque tesi ad aggirare le prescrizioni del Modello realizzati da altri destinatari (di livello apicale o non apicale).

In particolare, la segnalazione rilevante ha ad oggetto due tipi di condotte:

- comportamenti illeciti rilevanti ai sensi del D.lgs. 231/01, dunque condotte penalmente rilevanti in quanto suscettibili di integrare reati "presupposto" richiamati dal D.lgs. 231/01, anche nella forma del semplice tentativo, delle quali i Destinatari abbiano avuto notizia sulla base di elementi di fatto gravi, precisi e concordanti;
- violazioni del Codice Etico, del Modello Organizzativo 231 e delle procedure interne del SIG fondate su elementi di fatto precisi e concordanti, di cui i Destinatari siano venuti a conoscenza in ragione delle funzioni svolte. In tal caso la segnalazione ha ad oggetto condotte che, quand'anche non abbiano rilevanza penale diretta, in ogni caso contravvengono al sistema di prevenzione dei reati messo in atto dalla Società, in quanto violano i principi di controllo (generali o specifici), i presidi o le procedure aziendali richiamate nel Modello organizzativo.

Alcuni esempi, non esaustivi, di possibili segnalazioni rilevanti ai predetti fini comprendono:

- situazioni di conflitto di interesse ritenute non conosciute dall'azienda;
- tentativi/atti di corruzione di amministratori o dipendenti verso terzi (pubblici ufficiali o anche privati);
- frodi commesse nell'interesse aziendale;
- intenzionale comunicazione di informazioni false a Pubbliche Amministrazioni.

- operazioni societarie o di business per cui si sospetta possa derivare un rischio sanzionatorio per la Società ai sensi del D. Lgs. 231/01;
- situazioni di difformità o di presunta difformità ad uno o più requisiti della SA 8000, coerentemente alla politica di responsabilità sociale adottata dall'azienda;
- situazioni di corruzione o di presunta difformità ad uno o più requisiti della ISO 37001.

Non saranno meritevoli di segnalazione:

- Le mere voci o i "sentito dire";
- Le doglianze di carattere personale del segnalante o sue rivendicazioni/istanze.

Le segnalazioni devono essere fatte in buona fede, con spirito di responsabilità, avere carattere di interesse per il bene comune, rientrare nelle tipologie di non conformità per cui il sistema è stato implementato.

6 Contenuto della segnalazione

Le segnalazioni non devono contenere dati eccedenti, bensì solo i dati necessari per dimostrare la fondatezza della denuncia. Di norma, quindi non andranno inseriti dati particolari*, né dati personali idonei a rivelare lo stato di salute o giudiziari. Qualora le segnalazioni contenessero suddette categorie di dati personali, riferiti al segnalante o a terzi, e gli stessi non risultassero necessari per il perseguimento delle suddette finalità, la società provvederà a distruggerli o, se ciò non risultasse possibile, ad oscurarli, fatti salvi i casi autorizzati dalla legge o da un provvedimento dell'Autorità Garante per la protezione dei dati personali.

Qualora la segnalazione non rientri nella competenza dell'OdV, del SPT o del RPC secondo la definizione dell'ambito oggettivo appena descritto, l'Organismo esorterà il segnalante ad inoltrarla all'area aziendale/organo competente e/o alle Autorità competenti. Tali segnalazioni sono, in ogni caso, considerate "protette". Ciò significa che l'organismo preposto non rivela l'identità o i dati personali di chiunque abbia trasmesso tale segnalazione senza averne ottenuto previamente l'esplicito consenso – sempre che la sua divulgazione non sia imposta dalla legge, da indagini o successivi procedimenti giudiziari.

In tutti i casi sopra indicati di comunicazione, il Titolare garantisce che verranno sempre adottate le opportune misure atte ad evitare una non necessaria circolazione delle informazioni, al fine di garantire la opportuna riservatezza in vista delle particolari finalità dei trattamenti in oggetto.

**informazioni idonee a rivelare l'origine razziale ed etnica, gli orientamenti sessuali, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale.*

7 Destinatari della procedura (segnalanti)

In particolare, i Destinatari della presente procedura sono:

- i vertici aziendali e i componenti degli organi sociali;
- i dipendenti, i clienti, i fornitori, i consulenti, i collaboratori e, più in generale, chiunque sia in relazione d'interessi con le società su indicate;

I destinatari, a conoscenza di fatti potenzialmente oggetto di segnalazione, sono tenuti ad effettuare le segnalazioni fornendo tutti gli elementi utili per effettuare le verifiche e gli accertamenti necessari a valutarne la fondatezza ed indicando, almeno i seguenti elementi:

- A meno che la segnalazione non sia anonima, le generalità del soggetto che effettua la segnalazione, con indicazione della posizione o funzione svolta nell'ambito dell'azienda;
- descrizione dei fatti oggetto di segnalazione con indicazione delle circostanze conosciute (di modo, di tempo e di luogo) relative ai fatti segnalati;
- ogni informazione o prova che possa fornire un utile riscontro circa la sussistenza di quanto segnalato, in particolare anche l'indicazione di eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione;
- l'insussistenza di eventuali interessi privati collegati alla segnalazione e la propria buona fede;
- elementi identificativi del Segnalato;

- qualsiasi altra informazione ritenuta rilevante ai fini della segnalazione.

8 Destinataro della segnalazione

In caso di difformità, o presunte tali, al mod.231 adottato dall'azienda, l'Organismo di Vigilanza ex D.lgs. 231/2001 rappresenta il destinatario delle segnalazioni di illeciti.

In caso di difformità, o presunte tali, ai requisiti SA 8000 (responsabilità sociale), il SPT (Social Performance Team) o il RSI (Responsabile del Sistema Integrato) rappresentano i destinatari delle segnalazioni. Eventuali altri canali di segnalazione (esterni all'azienda – canale SAI ed Ente di Certificazione) sono riportati all'interno della Politica di Responsabilità Sociale AL10MI01-POL.

In caso di difformità, o presunte tali, ai requisiti ISO 37001 (anticorruzione), il Responsabile per la Prevenzione della Corruzione rappresenta il destinatario delle segnalazioni.

I destinatari assicurano il corretto svolgimento del processo di segnalazione delle violazioni e riferisce, direttamente e senza indugio, all'Organo Amministrativo le informazioni oggetto di segnalazione, qualora la violazione sia stata accertata.

L'Organismo di Vigilanza, in qualità di Destinatario della Segnalazione:

- è autonomo e indipendente rispetto alle funzioni operative, non dipendendo gerarchicamente da nessuna di esse;
- garantisce un giudizio equo e imparziale sulla segnalazione ricevuta;
- rispetta gli obblighi di riservatezza del segnalante e del segnalato.

Il SPT, in qualità di Destinatario della Segnalazione:

- analizza le segnalazioni pervenute e si attiva per predisporre il trattamento, collaborando per l'individuazione di azioni correttive;
- garantisce un giudizio equo e imparziale sulla segnalazione ricevuta;
- rispetta gli obblighi di riservatezza del segnalante e del segnalato.

Il RPC, in qualità di Destinatario della Segnalazione:

- analizza le segnalazioni pervenute e si attiva per predisporre le opportune indagini in relazione agli eventi di corruzione segnalati;
- garantisce un giudizio equo e imparziale sulla segnalazione ricevuta;
- rispetta gli obblighi di riservatezza del segnalante e del segnalato.

9 Modalità di trasmissione della segnalazione

Un soggetto Segnalante, qualora abbia il ragionevole sospetto che si sia verificato o che possa verificarsi una delle violazioni precedentemente indicate in accordo al mod.231, ha la possibilità di effettuare una Segnalazione all'OdV (Organismo di Vigilanza) utilizzando i canali di seguito riportati:

- Tramite la casella di posta elettronica odvteatek@gmail.com
- Tramite posta tradizionale in modalità raccomandata a/r all'indirizzo dell'azienda T.E.A. Tek S.p.A, Via Maddaloni snc Consorzio Area 80011 Acerra (NA), con destinatario l'Organismo di Vigilanza
- Tramite il portale Whistleblowing, come specificato nel paragrafo successivo.

Un soggetto Segnalante, qualora abbia il ragionevole sospetto che si sia verificato o che possa verificarsi una delle violazioni che vada contro i principi SA 8000 adottati dall'azienda, ha la possibilità di effettuare una Segnalazione utilizzando i canali di seguito riportati:

- Tramite la casella di posta elettronica spt.teatek@gmail.com;
- Tramite la casella di posta crs@it.bureauveritas.com;
- Tramite il portale SAI <https://sa-intl.org/services/assurance/sa8000-complaints-and-feedback/>;

- Tramite il portale Whistleblowing, come specificato nel paragrafo successivo.

Un soggetto Segnalante, qualora abbia il ragionevole sospetto che si sia verificato o che possa verificarsi una delle violazioni che vada contro i principi della ISO 37001 adottata dall'azienda, ha la possibilità di effettuare una Segnalazione utilizzando i canali di seguito riportati:

- Tramite la casella di posta elettronica anticorruzione.teatek@gmail.com;
- Tramite posta tradizionale in modalità raccomandata a/r all'indirizzo dell'azienda T.E.A. Tek S.p.A, Via Maddaloni snc Consorzio Area 80011 Acerra (NA), con destinatario Responsabile per la Prevenzione della Corruzione;
- Tramite il portale Whistleblowing, come specificato nel paragrafo successivo.

10 Il portale Whistleblowing

Il Portale Whistleblowing è raggiungibile per i *Whistleblowers* al seguente indirizzo web dedicato:

<https://teatekspa.whistlelink.com/>

La piattaforma consente a chiunque (dipendenti e collaboratori, fornitori e qualsiasi altro soggetto che abbia avuto o intenda avere rapporti d'affari con la Società) - attraverso un percorso guidato on-line – di effettuare le segnalazioni garantendo l'anonimato del segnalante; il sistema, infatti, consente di inviare segnalazioni senza l'obbligo di registrarsi né di dichiarare le proprie generalità. Qualora il Segnalante scelga di indicare le proprie generalità, ne è garantita la riservatezza.

La piattaforma consente di dialogare in modo riservato con il segnalante, senza possibilità, per il ricevente o altri soggetti, di rintracciare l'origine della segnalazione.

L'accesso al Portale Whistleblowing è, infatti, soggetto alla politica "no-log" al fine di impedire l'identificazione del segnalante che intenda rimanere anonimo: ciò significa che i sistemi informatici aziendali non sono in grado di identificare il punto di accesso al portale (indirizzo IP) anche nel caso in cui l'accesso venisse effettuato da un computer connesso alla rete aziendale.

Le segnalazioni trasmesse mediante il Portale Whistleblowing sono ricevute esclusivamente dai componenti dell'Organismo di Vigilanza. L'associazione dell'identità del segnalante alla segnalazione può, infatti, essere effettuata esclusivamente dall'organismo preposto alla gestione delle segnalazioni (OdV – Organismo di Vigilanza).

Il trattamento dei dati contenuti nelle segnalazioni avverrà con logiche di organizzazione ed elaborazione in grado di garantire la sicurezza, l'integrità e la riservatezza dei dati stessi nel rispetto delle misure organizzative, fisiche e logiche previste dalle disposizioni vigenti.

In particolare, la trasmissione dei dati forniti dal segnalante mediante l'utilizzo della piattaforma è gestita con protocollo HTTPS. Sono inoltre applicate tecniche di cifratura, garantendo in questo modo la riservatezza delle informazioni trasmesse.

Le segnalazioni "anonime", ossia effettuate senza identificazione del soggetto segnalante, verranno prese in considerazione qualora adeguatamente circostanziate e rese con dovizia di particolari, ove cioè siano in grado di far emergere fatti e situazioni relazionandoli a contesti determinati.

Dopo l'accesso al Portale il segnalante sarà guidato nella compilazione di un questionario composto da domande aperte che gli permetteranno di fornire gli elementi caratterizzanti la segnalazione (fatti, contesto temporale, dimensioni economiche, etc.).

Nel corso della compilazione del detto modulo il Portale chiederà al segnalante se intende o meno rivelare la propria identità. In ogni caso il segnalante potrà fornire le proprie generalità anche in un secondo momento, attraverso il sistema di messagistica previsto dal Portale.

Nel momento dell'invio della segnalazione il Portale rilascerà al segnalante un codice identificativo univoco. Questo numero, conosciuto solamente dal segnalante, non potrà essere recuperato in alcun modo in caso di smarrimento. Il codice servirà al segnalante per accedere, sempre tramite il Portale, alla propria segnalazione al

fine di: monitorarne lo stato di avanzamento; inserire ulteriori elementi per circostanziare la segnalazione; fornire le proprie generalità; rispondere ad eventuali domande di approfondimento.

11 Gestione della segnalazione

Le segnalazioni ricevute dai componenti dell'Organismo di Vigilanza, dal team SPT o dal RPC sono soggette al seguente iter istruttorio.

Le segnalazioni la cui genericità non consenta neppure di avviare una verifica indirizzandola verso prospettive concrete, non saranno prese in considerazione e verranno immediatamente archiviate.

Le segnalazioni ed i relativi documenti a supporto, saranno oggetto di analisi preliminare da parte dell'Organismo di Vigilanza, da parte del SPT o da parte del RPC, al fine di verificare la presenza di dati ed informazioni utili e sufficienti a valutare l'astratta fondatezza della segnalazione per avviare gli ulteriori approfondimenti.

Effettuata tale analisi, qualora, l'OdV, il SPT o il RPC verifichi che il fatto riportato non ha impatto ai fini del D. Lgs. 231/01, della SA 8000 o della ISO 37001, tuttavia può essere rilevante per l'Azienda, inviterà il segnalante ad inoltrarla all'organo/organismo competente.

Nel caso, invece, in cui l'Organismo di Vigilanza, il SPT o il RPC ritenga sussistente un ragionevole presupposto di fondatezza/attendibilità, si passerà ad un'indagine approfondita sui fatti oggetto della stessa, al fine di appurarne la fondatezza. Nello svolgimento della suddetta analisi il Destinatario potrà avvalersi - per specifici aspetti trattati nelle segnalazioni e qualora ritenuto necessario - del supporto di altre funzioni aziendali per quanto di competenza e potrà richiedere ulteriori informazioni e/o documentazione al segnalante mediante il portale stesso.

Qualora a conclusione della fase di analisi preliminare emerga l'assenza di elementi sufficientemente circostanziati o l'infondatezza dei fatti richiamati, la segnalazione sarà archiviata con le relative motivazioni. In tal caso, l'Organismo di Vigilanza, il SPT o il RPC provvederà ad informare il segnalante della conclusione e degli esiti dell'indagine svolta.

Laddove, a seguito delle analisi preliminari emergano o siano comunque desumibili elementi utili e sufficienti per valutare fondata la segnalazione, verrà avviata la successiva fase degli approfondimenti specifici.

L'Organismo di Vigilanza / SPT / RPC provvederà a:

- avviare le analisi specifiche avvalendosi, se ritenuto opportuno, delle strutture competenti della Società;
- concordare con il management responsabile della funzione interessata dalla segnalazione, l'eventuale "action plan" necessario per la rimozione delle debolezze di controllo rilevate;
- concordare con l'Amministratore Delegato e le Funzioni interessate eventuali iniziative da intraprendere a tutela degli interessi della Società;
- richiedere, se possibile, l'avvio di un procedimento disciplinare nei confronti del segnalante, nel caso di segnalazioni in relazione alle quali siano accertate la malafede del segnalante e/o l'intento meramente diffamatorio, eventualmente confermati anche dalla infondatezza della stessa segnalazione;
- alla conclusione dell'approfondimento svolto, sottoporre i risultati alla valutazione dell'Amministratore Delegato o del Collegio Sindacale, a seconda dell'oggetto della segnalazione, affinché vengano intrapresi i più opportuni provvedimenti;
- concludere l'istruttoria in qualunque momento se, nel corso dell'istruttoria medesima, sia accertata l'infondatezza della segnalazione.

Le attività sopra descritte non sono necessariamente svolte in maniera sequenziale.

12 Tutela e responsabilità del segnalante

La Società garantisce la riservatezza dell'identità del Segnalante a partire dalla fase di ricezione della segnalazione, nel rispetto delle previsioni di legge. A tal fine i dati personali identificativi del segnalante non

sono direttamente visualizzabili nella segnalazione e sono conservati in modo da essere visibili esclusivamente all'organismo preposto alla gestione della segnalazione. La società adotta tutte le garanzie previste dalla legge al fine di tutelare la riservatezza dell'identità del segnalante, in modo che la stessa non sia rivelata a terzi senza l'espresso consenso di quest'ultimo, salvo il caso di segnalazioni in mala fede o diffamatorie.

Nessuna ritorsione o discriminazione, diretta o indiretta, può derivare in capo a chi abbia effettuato una segnalazione in buona fede, a prescindere che la segnalazione si sia poi rivelata fondata o meno.

Sono previste sanzioni nei confronti di chi viola le misure di tutela e riservatezza del segnalante.

La tutela del segnalante non è, invece, garantita nel caso di segnalazioni effettuate con **dolo** o **colpa grave** o che si dovessero rivelare false, infondate, con contenuto diffamatorio o comunque effettuate al solo scopo di danneggiare la Società, il segnalato o altri soggetti interessati dalla segnalazione.

In caso di procedimento disciplinare, l'identità del segnalante non può essere rivelata ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa; l'identità del segnalante potrà essere rivelata soltanto laddove:

- la contestazione sia fondata, in tutto o in parte, sulla segnalazione stessa e la conoscenza dell'identità del segnalante sia assolutamente indispensabile per la difesa dell'incolpato; e
- vi sia il consenso del segnalante.

Sono previste sanzioni nei confronti del segnalante, ove si riuscisse a risalire allo stesso nel caso di segnalazioni effettuate con dolo o colpa grave o che si dovessero rivelare false, infondate, con contenuto diffamatorio o comunque effettuate al solo scopo di danneggiare la Società, il segnalato o altri soggetti interessati dalla segnalazione.

La Società potrà, inoltre, intraprendere le opportune iniziative anche in sede giuridica.

13 Tutela del segnalato

La Società garantisce adeguata protezione alle persone direttamente o indirettamente oggetto della segnalazione.

La segnalazione non è sufficiente ad avviare alcun procedimento disciplinare verso il segnalato.

Non si potrà quindi sanzionare disciplinarmente il soggetto segnalato sulla base di quanto affermato dal segnalante, senza che vi siano riscontri oggettivi e senza che si sia proceduto ad indagare i fatti oggetto di segnalazione.

Ciò potrebbe avvenire eventualmente in base ad altre evidenze riscontrate e accertate a partire dalla segnalazione stessa.

Qualora l'Organismo di Vigilanza, il SPT o il RPC, a seguito di concreti riscontri acquisiti a riguardo della segnalazione, decida di procedere con l'attività istruttoria, il segnalato potrà essere contattato e gli verrà assicurata la possibilità di fornire ogni eventuale e necessario chiarimento.

14 Conservazione della documentazione e tutela della privacy

I dati personali conferiti dal segnalante al momento della registrazione e le informazioni contenute nelle segnalazioni e negli eventuali documenti alle stesse allegati, nonché i dati eventualmente acquisiti in sede di istruttoria dall'organismo preposto, sono trattati in conformità alla Policy di protezione dei dati personali adottata dalla Società, nel rispetto dei principi di correttezza, liceità, trasparenza e tutela della riservatezza e dei diritti di tutti gli interessati (segnalante, segnalato ed eventuali soggetti terzi coinvolti), ed in ottemperanza agli obblighi imposti dalla normativa sulla privacy e dalla legge 30 novembre 2017, n. 179, recante *"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"*.

L'Organismo di Vigilanza / il SPT / il RPC cura l'archiviazione di tutta la documentazione a supporto della segnalazione ricevuta. I dati personali relativi alle segnalazioni vengono conservati e mantenuti per il periodo necessario al completamento della verifica dei fatti esposti nella segnalazione e per successivi **5 anni dalla**

chiusura della segnalazione, salvo eventuali procedimenti scaturenti dalla gestione della segnalazione (disciplinari, penali, contabili) nei confronti del segnalato o del segnalante (dichiarazioni in mala fede, false o diffamatorie). In tal caso saranno conservati per tutta la durata del procedimento e fino allo spirare dei termini di impugnazione del relativo provvedimento.

I dati personali contenuti nelle Segnalazioni possono essere comunicati agli uffici competenti dell'Azienda per l'attivazione della tutela giudiziaria e/o disciplinare connessa alla segnalazione, ovvero alle Autorità competenti in presenza di violazioni delle normative applicabili.

Tutti i dettagli relativi al trattamento dei dati personali degli interessati coinvolti nella segnalazione sono forniti nell'informativa sul trattamento ex. art. 13 GDPR, somministrata in sede di inoltro della segnalazione tramite la piattaforma ed allegata alla presente.

15 Sanzioni

La violazione dei principi fissati nella presente procedura viene perseguita, con tempestività ed immediatezza.

Tea Tek si riserva il diritto di intraprendere azioni disciplinari nei confronti del segnalante in caso di abuso dello strumento "Whistleblowing", ad esempio in ipotesi di segnalazioni manifestamente opportunistiche e/o al solo scopo di danneggiare il segnalato o soggetti comunque interessati dalla segnalazione e ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione dell'istituto oggetto della presente procedura.

Le sanzioni verranno applicate sulla base dello **Statuto dei Lavoratori (legge n. 300/1970)** e dei singoli Contratti Collettivi Nazionali.

16 Aggiornamento della policy

La presente Procedura e il Portale *Whistleblowing* saranno oggetto di revisione periodica per garantire il costante allineamento alla normativa di riferimento nonché in funzione dell'operatività e della esperienza maturata.

17 Sensibilizzazione

L'organizzazione intraprende iniziative di comunicazione e sensibilizzazione della presente procedura mediante divulgazione sul server aziendale e tramite iniziative di formazione rivolte a tutto il personale allo scopo di comunicare le finalità delle segnalazioni, dell'istituto del *Whistleblowing* e le modalità per il suo corretto utilizzo; sui relativi diritti e obblighi; sulle conseguenze degli abusi nel suo utilizzo; sui risultati che l'attuazione della norma ha prodotto.

18 Allegati

- MO01PR21-SEG "Segnalazione SA8000";
- Informativa Privacy per i segnalanti.