PROCEDURA OPERATIVA 12.3	***Copia n°***	
"Gestione delle Segnalazioni"		

2	03/11/23	Revisione finalizzata al recepimento delle modifiche introdotte dal D.Lgs. 24/2023			CdA (vedasi verbale n. 731 del 11/12/2023)
1		Revisione finalizzata al recepimento delle modifiche organizzative intercorse ed alla compliance al MOG 231.			
Rev	**Data**	**Descrizione modifica**	**Emesso**	**Verificato**	**Approvato**

Sommario

1. SCOPO

La presente procedura risulta definita attraverso atto organizzativo adottato dall'organo di indirizzo di Cantine Settesoli.

Lo scopo della seguente procedura è definire e disciplinare le modalità e le procedure di inoltro/presentazione delle segnalazioni (sia interne che esterne), dei reclami, delle denunce (all'autorità giudiziaria o contabile) e delle divulgazioni pubbliche con cui le parti interessate, compresi i lavoratori, possono fornire evidenza di anomalie o criticità (anche potenziali), non conformità o segnalazioni/reclami in merito alle tematiche relative a:

- la commissione o tentativi di commissione di uno dei reati/condotte illecite contemplate dal D.Lgs. 231, ovvero violazioni o fraudolente elusioni del Modello di Organizzazione e di Gestione e/o del Codice Etico di Cantine Settesoli;
- la commissione o dei tentativi di commissione di un reato in materia di frode alimentare, sicurezza e conformità dei prodotti, sicurezza degli alimenti, protezione dei consumatori;
- la commissione o dei tentativi di commissione di un reato in materia di salute e sicurezza sul lavoro;
- la commissione o dei tentativi di commissione di un reato in materia di tutela dell'ambiente;
- comportamenti non corretti nella gestione del personale dipendente, con violazione dei principi e degli aspetti attinenti al Diritto del Lavoro;
- comportamenti non corretti in riferimento ai temi etici e sociali in genere, ivi inclusi quelli riguardanti abusi fisici, verbali o di carattere sessuale (da azienda a lavoratore o fra lavoratori);
- Mancata/carente/inefficace applicazione del Sistema di Gestione Integrato;
- Illeciti amministrativi, contabili, civili o penali (sia violazioni non del diritto dell'UE sia illeciti che rientrano nell'ambito di applicazione degli atti dell'UE o nazionali); in particolare, in aggiunta a quanto già sopra indicato, con riferimento ai seguenti settori:
    - Servizi, prodotti e prevenzione del riciclaggio
    - Salute pubblica
    - Tutela della vita privata, protezione dei dati personali e sicurezza delle reti e dei sistemi informativi
- Atti od omissioni che ledono gli interessi finanziari dell'Unione;
- Atti od omissioni riguardo al mercato interno, comprese:
    - le violazioni delle norme dell'UE in materia di concorrenza e di aiuti di Stato
    - le violazioni delle norme in materia di imposta sulle società
    - i meccanismi il cui fine sia ottenere un vantaggio fiscale

Con "parti interessate" si intende includere:

- lavoratori dipendenti/subordinati di Cantine Settesoli, inclusi anche:
    - lavoratori *part time*
    - lavoratori intermittenti
    - lavoratori a termine

    - lavoratori somministrati
    - apprendisti
    - lavoratori che forniscono prestazioni di lavoro occasionali
- lavoratori autonomi[1] ed i titolari di rapporti di collaborazione, inclusi anche:
    - quelli con prestazione d'opera continuativa e coordinata (vale a dire attività lavorativa organizzata autonomamente dal collaboratore), prevalentemente personale, anche se a carattere non subordinato
    - quelli attraverso rapporti di agenzia
    - quelli attraverso rapporti di rappresentanza commerciale
    - quelli attraverso collaborazioni etero-organizzative (prestazioni di lavoro prevalentemente personali, continuative, con modalità di esecuzione organizzate da Cantine Settesoli)
- i lavoratori/collaboratori che, presso Cantine Settesoli, forniscono beni o servizi o realizzano opere
- i liberi professionisti ed i consulenti
- i tirocinanti (a prescindere che risultino retribuiti o meno)
- le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche con esercizio semplicemente di fatto (ad es., componenti del CdA e dell'OdV)
- soggetti non qualificabili come lavoratori (ad es., i c.d. "facilitatori", vale a dire persone che assistono il segnalante nel processo di segnalazione e che operino nel contesto lavorativo del segnalante, quale un sindacalista che operi in proprio nome)
- persone, operanti nel contesto lavoratori del segnalante, e legate a quest'ultimo da stabili legami affettivi o di parentela entro il IV grado
- colleghi di lavoro del segnalante, che operino nello stesso contesto lavorativo, aventi con lo stesso rapporti abituali/correnti (in rientrano in tale categoria, di conseguenza, gli ex colleghi)
- enti di proprietà (esclusiva o con compartecipazione maggioritaria con terzi) del segnalante, o per i quali lo stesso lavora (non essendone proprietario), o che operano nel medesimo contesto lavorativo (senza un legame diretto vero e proprio né per quanto concerne la proprietà né in ambito di prestazione di lavoro/servizio)

Ulteriore scopo è quello di definire le modalità di protezione delle persone che segnalano tali violazioni (tutele offerte ai *whistleblower*) e relativo esercizio del potere sanzionatorio.

Infine, all'interno della stessa vengono anche riportate le procedure per la gestione delle succitate segnalazioni.

Le segnalazioni oggetto della presente procedura concernono le violazioni di disposizioni di cui il segnalante sia venuto a conoscenza nel contesto lavorativo (vale a dire sia chi ha un rapporto di lavoro propriamente detto con Cantine Settesoli sia chi ha un rapporto giuridico qualificato diverso con quest'ultima), e che siano in grado di ledere:

[1] Risultano esclusi, invece, da tale ambito gli imprenditori (compresi i piccoli imprenditori)

- L'interesse pubblico
- L'integrità di Cantine Settesoli

I fatti segnalati, inoltre, possono essere stati appresi sia grazie alla funzione ricoperta, sia attraverso notizie acquisite in occasione, od a causa, dello svolgimento delle proprie mansioni lavorative, sia in modo casuale.

Il concetto di "violazione" ricopre tutti quei comportamenti, atti od omissioni che ledano o l'interesse pubblico o l'integrità di Cantine Settesoli, e possono riguardare sia le violazioni stesse sia le informazioni su tali violazioni; nel dettaglio:

- Informazioni o fondati sospetti su violazioni già commesse od illeciti che, anche se non ancora compiuti, si ritenga possano essere commessi in Cantine Settesoli, sulla base di elementi concreti, precisi e concordanti
- Condotte tese ad occultare tali violazioni

2. ESCLUSIONI

Non risultano oggetto della succitata protezione, e quindi esclusi dal campo di applicazione della presente procedura:

- Contestazioni, rivendicazioni o richieste legate ad un interesse personale del segnalante, che attengono esclusivamente ai propri rapporti individuali di lavoro (inclusi quelli con le figure gerarchicamente sovraordinate);
- Segnalazioni di violazioni già disciplinate in via obbligatoria (ad es., segnalazioni in materia di abusi di mercato);
- Mere irregolarità (a meno che le stesse non costituiscano elementi concreti/indici sintomatici tali da far ritenere ragionevolmente al whistleblower la possibilità di commissione di una delle violazioni previste all'interno del campo di applicazione).

3. RIFERIMENTI

- D. Lgs. 10 marzo 2023, n. 24 Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali
- Linee Guida ANAC
- D. lgs. 231/01 e s.m.i. - 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
- D.Lgs. 81/08 e s.m.i. - Testo unico sulla sicurezza
- D.Lgs. 152/06 e s.m.i. - Testo Unico in materia ambientale
- L. 30/11/17, n. 179 e s.m.i. - 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

- D. Lgs. 30/06/03, n. 196 e s.m.i. - Codice in materia di protezione dei dati personali
- D. Lgs. 10/08/18, n. 101 e s.m.i. - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
- UNI EN ISO 9001 ed. corrente
- UNI EN ISO 14001 ed. corrente
- OHSAS 18001 ed. corrente
- BSCI - Code of Conduct
- Eti-base-code
- Modello di Organizzazione, Gestione e Controllo (ai sensi del D.lgs. 231/01)
- Codice Etico
- PO 10.14 Gestione dei flussi informativi OdV

4. **MODALITÀ OPERATIVE**

Le segnalazioni devono cercare di essere il più circostanziate possibili; nel dettaglio, devono risultare chiari i seguenti elementi:

- Quando e dove si è verificato il fatto oggetto di segnalazione
- Descrizione del fatto
- Generalità/altri elementi utili per l'identificazione del soggetto a cui vengono attribuiti i fatti segnalati

Tutte le tipologie di canali di segnalazione sotto riportati garantiscono, tramite l'utilizzo di avanzati strumenti di crittografia[2] (presenti all'interno della piattaforma[3]

[2] L'architettura di sicurezza garantisce che nessuna terza parte (compresi i dipendenti di EQS Group stesso: EQS non può, quindi, recuperare le password di sistema e, di conseguenza, se vengono perse tutte le password di perde l'accesso al sistema di gestione dei casi) abbia accesso ai sistemi, alle segnalazioni od ai dati dei clienti. Ogni sistema client è crittografato con chiavi di crittografia individuali (né EQS né il providing di hosting hanno accesso alle chiavi di crittografia necessarie per decifrare i dati e, quindi, non possono leggere le informazioni sensibili contenute nei report inviati). Tutti i dati personali sensibili sono criptati nel database; vengono utilizzati due livelli di chiavi di crittografia: la "chiave master" e le "chiavi di crittografia dei dati". La chiave master viene utilizzata per proteggere le chiavi dei dati (chiavi asimmetriche e simmetriche del cliente). La chiave master (tramite la password utente) e le chiavi dati (tramite la chiave master) sono bloccate in modo tale che solo un utente amministratore/case manager possa decifrare e leggere i report inviati. Le password degli utenti amministratori non vengono memorizzate nel sistema in chiaro; in aggiunta, tale piattaforma prevede: i più recenti firewall e restrizioni IP per proteggere i sistemi dagli attacchi informatici, file detox (scansionamento di tutti gli allegati con sistemi di pulizia dei file impedendo l'entrata nel sistema di virus, compresi quelli di tipo "0-day"; rimozione dei metadati che potrebbero rivelare l'identità del segnalante nei file caricati), brute force attack (metodo di lockout/blocco per prevenire gli attacchi di forza bruta: ad es., su numero massimo di accessi non riusciti prima della sospensione dell'account o su numero di minuti di sospensione dell'account), autenticazione a due fattori via e-mail (per prevenire il furto di identità ed assicurare che terze persone possano accedere con i dati di accesso del segnalante), certificati SSL, tecnologie di miglioramento della privacy PET (privacy by design), conformità all'OWASP (Open Web Application Security Project)

[3] La piattaforma adottata da Cantine Settesoli è EQS Integrity Line, ed il servizio risulta disponibile 24/7 (Software as a Service per il cui utilizzo sono necessari solamente un browser web ed una connessione ad internet) da qualsiasi dispositivo (lingue disponibili: italiano ed inglese); il sistema, inoltre, è: conforme ai requisiti europei in materia di

adottata da Cantine Settesoli), la riservatezza, durante tutte le fasi del procedimento e fino alla conclusione dello stesso:

- dell'identità dei soggetti segnalanti
- dell'identità dei soggetti coinvolti o segnalati (eccezione: segnalazioni oggetto di denunzia alle Autorità giudiziarie)
- dell'identità dei soggetti menzionati all'interno della segnalazione (eccezione: segnalazioni oggetto di denunzia alle Autorità giudiziarie)
- del contenuto della segnalazione
- della relativa documentazione

In particolare, risulta particolarmente importante il divieto di rivelare a persone diverse da quelle competenti a ricevere/dare seguito alle segnalazioni sia l'identità del segnalante sia qualsiasi altra informazione da cui la stessa si possa evincere (direttamente od indirettamente), a meno di espresso consenso da parte del segnalante[4]. Di conseguenza, è previsto l'oscuramento dei dati personali se, per ragioni istruttorie, anche altri soggetti devono essere messi a conoscenza del contenuto della segnalazione e/o della documentazione allegata (incluso anche il caso in cui la stessa debba essere trasmessa ad autorità competente). In aggiunta, i dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non devono essere raccolto o, se raccolti accidentalmente, devono essere cancellati immediatamente (principio di minimizzazione).

Nei casi in cui si renda necessario rivelare l'identità del segnalante, è necessario rispettare le seguenti condizioni:

- consenso del segnalante
- fornito avviso al segnalante mediante comunicazione scritta dei motivi della rivelazione della propria identità/dati riservati

Cantine Settesoli mette a disposizioni informazioni chiare su canali, procedure, soggetti gestori delle segnalazioni interne e presupposti (di scelta dei diversi canali) per l'effettuazione delle segnalazioni, sia interne che esterne, attraverso il proprio sito web (alla pagina *https://www.cantinesettesoli.it/il-modello-di-business/*), ed attraverso l'esposizione nei propri luoghi di lavoro (cartella di rete *O:\Qualità OdV\Manuale di Gestione integrato\Procedure\PO 12.3 Gestione delle segnalazioni* e tutti i punti ove presente l'informativa di *whistleblowing*: ad es., in prossimità delle

protezione dei dati ed alle norme del GDPR (protezione dei dati certificata ISAE 3000), la sicurezza dei dati dei relativi data center e sviluppo software è certificata secondo ISO 27001, conforme alla Direttiva europea sull'accessibilità del web senza barriere Web Content Accessibility Guidelines (secondo WCAG 2.1) al fine di permettere l'utilizzo del sistema anche a persone con difficoltà visive, conforme alla Supply Chain Law, dotato di un sistema di backup giornaliero dei dati (backup conservati per 90 giorni), dotato di un sistema che replica tutti i dati tra 3 data center, predefinito con un criterio di password che soddisfa gli standard di buona pratica in materia di password, dotato di un sistema di timeout automatico della sessione dopo 30 minuti (necessaria password per accedere nuovamente) nel sistema di gestione dei casi e nella casella di posta elettronica protetta, dotato di un principio "4 Eyes Principle" per le funzioni più critiche (ad es., creazione utente, cancellazione caso) in modo che invece di un solo utente che esegue tali attività un secondo utente deve confermare l'azione per ogni caso specifico, dotato di un sistema grazie al quale tutte le azioni significative eseguite dagli utenti amministratori vengono registrate (ad es., creazione utente, modifica permessi, qualsiasi azione relativa ad una nuova segnalazione) e visualizzate con l'audit trail del sistema

[4] Inclusi: procedimento penale, procedimento dinanzi alla Corte dei Conti, procedimento disciplinare

cassette postali). Tra le informazioni messe a disposizione, di particolare rilevanza risulta quella relativa alla differenza tra segnalazione ordinaria e segnalazione di *whistleblowing* (specificazione dello scenario all'interno della segnalazione, riservatezza dell'identità, tutele previste, gestione in caso di recapito erroneo a soggetto non competente, diverse conseguenze). Cantine Settesoli, inoltre, effettua corsi di formazione, per i propri dipendenti, che trattano tali temi.

Per quanto riguarda la scelta del canale di segnalazione da parte del *whistleblower*, lo stesso dovrà favorire, in via prioritaria, l'uso del canale interno; il procedere con l'utilizzo del canale esterno deve essere considerato soltanto nel caso in cui ricorra una delle seguenti condizioni:

- canale di segnalazione interna non attivo
- precedente segnalazione interna da parte del segnalante senza alcun seguito (vale a dire, il gestore delle segnalazioni, entro i termini previsti, non abbia intrapreso alcuna attività circa l'ammissibilità della segnalazione, a verifica della sussistenza di quanto segnalato, la comunicazione dell'esito dell'istruttoria)
- fondati motivi del segnalante di ritenere che ad un'eventuale segnalazione interna non verrebbe dato efficace seguito (ad es., in caso di accordo tra chi riceve la segnalazione e la persona coinvolta nella violazione, conoscenza di occultamento/distruzione di prove di condotte illecite, conflitto di interessi del gestore delle segnalazioni in quanto segnalante o segnalato nella segnalazione) o che la stessa possa determinare rischio di ritorsioni (ad es., in ragione di situazioni/eventi già verificatisi: precedente minaccia di subire pregiudizi in caso di segnalazione o conoscenza di ritorsioni precedenti/violazioni obbligo di riservatezza)
- fondati motivi del segnalante di ritenere che la violazione possa costituire pericolo imminente/palese per il pubblico interesse (e, quindi, richieda evidentemente un intervento urgente da parte dell'autorità pubblica per la salvaguardia di un interesse collettivo, quali salute, sicurezza, protezione ambientale)

Al fine di evitare che il segnalante, ad es. durante il proprio rapporto di lavoro od anche prima dell'instaurazione dello stesso o dopo il relativo scioglimento, al solo scopo di salvaguardare od ottenere l'occupazione, a causa di situazioni di squilibrio o "timore", anche sotto il profilo di eventuali ritorsioni, dismetta i propri diritti, eventuali rinunce o transazioni (integrali o parziali) sono ritenute valide se effettuate:

- in sede giudiziale
- in sede amministrativa, presso le commissioni di conciliazione
- presso le commissioni di certificazione dei contratti di lavoro
- presso i collegi di conciliazione ed arbitrato sindacale
- presso i collegi di conciliazione ed arbitrato irrituale

4.1. Inoltro delle segnalazioni (canale interno)

Cantine Settesoli assicura che la predisposizione e l'attivazione di questo tipo di canale di segnalazione sono avvenute a seguito del rispettivo benestare delle relative rappresentanze sindacali.

Cantine Settesoli ha identificato, quale soggetto "gestore delle segnalazioni" (all'interno della piattaforma adottata, definiti "*Case Manager*"):

- Presidente del Collegio Sindacale (soggetto esterno)
- Presidente dell'Organismo di Vigilanza[5] (soggetto esterno)

Ambo tali soggetti, comunque, assicurano le prerogative di autonomia, imparzialità, indipendenza e specifica formazione in materia sia di *privacy* sia di *whistleblowing*. Inoltre, tali soggetti risultano autorizzati al trattamento dei dati personali da parte di Cantine Settesoli.

I lavoratori possono effettuare segnalazioni (scritte od orali) o dare suggerimenti alla Direzione (reclami che possono essere presentati in modo anonimo) secondo le seguenti modalità (canali di segnalazione):

- Piattaforma *software* per la gestione delle segnalazioni
- Inoltro segnalazione tramite compilazione del "M.12.3 Modulo di Segnalazione" e inserimento all'interno di una delle apposite cassette postali posizionate in più siti della Cantina. Tale modalità di segnalazione deve, però, essere conforme ai seguenti passaggi:
    - La segnalazione deve riportare se il segnalante intenda o meno avvalersi della riservatezza della propria identità e delle altre tutele previste per il *whistleblower*
    - La segnalazione deve essere inserita all'interno di una prima busta chiusa
    - All'interno di una seconda busta chiusa, invece, devono essere inseriti i dati identificativi del segnalante ed una copia del documento di riconoscimento dello stesso (in caso di segnalazione in forma non anonima)
    - La prima e la seconda busta chiusa, infine, devono essere inserite all'interno di una terza busta chiusa, riportante all'esterno la dicitura "RISERVATA AL GESTORE DELLA SEGNALAZIONE";
- sistema di messaggistica vocale, attraverso la piattaforma *software* per la gestione delle segnalazioni;
- su richiesta dal segnalante, incontro diretto fissato con il gestore delle segnalazioni, entro un termine ragionevole, attraverso la piattaforma *software* per la gestione delle segnalazioni.

A discrezione del segnalante, le segnalazioni possono essere eseguite in forma anonima (in tal caso, le misure di protezione risultano applicabili soltanto se il segnalante sia successivamente identificato), confidenziale o sottoscritta.

Quando un segnalante invia una segnalazione tramite la piattaforma, gli viene fornito un numero di segnalazione (Case ID) generato automaticamente dal sistema e gli

[5] Tale soggetto può risultare anche quale possibile segnalante, con tutte le conseguenti tutele del caso

viene chiesto di creare una password specifica per la segnalazione. L'ID della segnalazione e la password vengono utilizzati per accedere al sistema e comunicare successivamente con il case manager. Il sistema, inoltre, attraverso un testo predefinito, invita il segnalante a rimuovere i metadati da qualsiasi file prima di caricarlo (opzionalmente, il file originale può essere reso completamente non disponibile per i case manager).

Cantine Settesoli garantisce, che nessuna forma di discriminazione sarà esercitata su dipendenti e parti interessate in seguito ad eventuali segnalazioni inoltrate. Nello specifico sono previste le seguenti tutele nei confronti sia del *whistleblower* sia degli altri soggetti interessati:

- Divieto di ritorsioni adottate in ragione della segnalazione
- Misure di sostegno
- Limitazioni della responsabilità

In questo frangente, con ritorsioni si deve considerare qualsiasi comportamento, provvedimento, atto od omissione, nel contesto lavorativo del segnalante, anche semplicemente tentato o minacciato (in tali casi, il segnalante deve fornire elementi da cui desumere l'effettività della minaccia o del tentativo di ritorsione, ad es. riunione con più persone durante la quale è stato discusso il licenziamento del segnalante, o licenziamento non realizzato per vizio formale nella procedura, o minaccia di licenziamento o di mutamento delle funzioni durante un colloquio con il proprio datore di lavoro), posto in essere in ragione della segnalazione, e che provoca, o può potenzialmente provocare, al segnalante, direttamente od indirettamente, un danno ingiusto. Ciò include:

- Licenziamento ritorsivo/discriminatorio o sospensione
- Retrocessione di grado o mancata promozione
- Mutamento di funzioni, cambiamento di luogo di lavoro, riduzione dello stipendio, modifica dell'orario di lavoro
- Sospensione o restrizioni alla formazione
- Note di merito negative o referenze negative
- Misure disciplinari od altre sanzioni
- Coercizione, intimidazione, molestie, ostracismo
- Discriminazione o trattamento sfavorevole
- Mancata conversione di contratto di lavoro a termine in contratto di lavoro a tempo indeterminato (ove presente legittima aspettativa a detta conversione)
- Mancato rinnovo o risoluzione anticipata di contratto di lavoro a termine
- Danni (anche reputazionali) su *social media*, o pregiudizi economici/finanziari (incluse perdite di opportunità economiche e di redditi)
- Inserimento in elenchi impropri, che può comportare l'impossibilità di trovare occupazione
- Conclusione anticipata od annullamento del contratto di fornitura di beni/servizi
- Annullamento di licenza/permesso
- Richiesta di sottoposizione ad accertamenti psichiatrici/medici
- Pretesa di risultati impossibili da raggiungere nei modi e tempi indicati

- Valutazione della *performance* artificiosamente negativa
- Revoca ingiustificata di incarichi
- Ingiustificato mancato conferimento di incarichi (con contestuale attribuzione ad altri)
- Reiterato rigetto di richieste (ad es., ferie/congedi)
- Suggerimento o proposta dell'adozione di una qualsiasi forma di ritorsione nei confronti del *whistleblower*

Per quanto concerne, invece, le misure di sostegno, le stesse vengono fornite da enti del terzo settore (elenco istituito presso ANAC e pubblicato sul proprio sito) nella forma di informazioni, assistenza e consulenza (a titolo gratuito) su:

- Modalità di segnalazione
- Protezione da ritorsioni
- Diritti della persona coinvolta
- Modalità e condizioni di accesso al patrocinio (a spese dello Stato)

Infine, con riferimento alle limitazioni di responsabilità in caso di rivelazione/diffusione di informazioni, il segnalante non risulta punibile (ed è esclusa anche ogni altre ulteriore responsabilità di natura sia civile sia amministrativa) in caso di rivelazione/diffusione di informazioni su violazioni:

- Coperte da obbligo di segreto d'ufficio, professionale, scientifico-industriale, dovere di fedeltà/lealtà
- Relative a tutela del diritto d'autore
- Relative a protezione dei dati personali
- Offensive della reputazione della persona coinvolta/denunciata

Tali limitazioni di responsabilità, però, ricorrono nel caso sussistano le seguenti condizioni:

- Al momento della rivelazione/diffusione c'erano fondati motivi per ritenere che la rivelazione/diffusione di tali informazioni fosse necessaria per svelare la violazione
- La segnalazione è stata effettuata seguendo il procedimento corretto illustrato nella presente procedura
- Si applica con riguardo ai soli comportamenti/atti/omissioni collegati alla segnalazione e strettamente necessari alla rivelazione della violazione
- L'acquisizione delle informazioni sulle violazioni, o l'accesso alle stesse od ai documenti, siano avvenuti lecitamente (ad es., accesso a messaggi di posta elettronica di un collega di lavoro con il suo consenso)

I presupposti per l'applicazione delle misure di protezione sono:

- Al momento della segnalazione, il segnalante avesse il fondato motivo di ritenere che le informazioni sulle violazioni fossero vere ed oggettive
- Il segnalante si sia basato su una convinzione ragionevole (non sufficienti semplici sospetti o "voci di corridoio") che le informazioni sulle violazioni segnalate fossero veritiere e rientranti nel campo di applicazione oggettivo del *whistleblowing*

- La segnalazione si basa su circostanze concrete allegate ed informazioni effettivamente acquisibili tali da far ritenere ragionevolmente che le informazioni sulle violazioni segnalate siano pertinenti, in quanto rientranti fra gli illeciti considerati nel whistleblowing
- Sussista un rapporto di consequenzialità tra la segnalazione e le misure ritorsive subite

Al fine di tale applicazione, invece, risultano del tutto irrilevanti la certezza circa l'effettivo accadimento dei fatti, l'identità dell'autore, l'errore genuino nel riportare i fatti ed i motivi per i quali il segnalante ha effettuato la segnalazione.

Le tutele, invece, non sono garantite e viene irrogata relativa sanzione disciplinare al segnalante nei seguenti casi:

- Diffamazione o calunnia
- Informazioni false riportate intenzionalmente con dolo o colpa grave

In tali casi, la comunicazione dell'avvio del procedimento viene inviata al *whistleblower*, il quale può presentare, entro 30 giorni dalla stessa, memorie scritte, documenti e deduzioni. Entro 120 giorni, successivamente, verrà adottato e comunicato al *whistleblower* il provvedimento conclusivo che può essere di archiviazione (nel caso di assenza dei presupposti di fatto o di diritto per la comminazione della sanzione) o sanzionatorio.

Per quanto concerne, invece, le divulgazioni pubbliche, il segnalante beneficia delle protezioni previste nel caso in cui, al momento di tale divulgazione, si verifichi almeno una delle seguenti condizioni:

- Precedente effettuazione di una segnalazione interna ed esterna (o direttamente esterna, nel caso ne ricorrano le condizioni) senza ricevimento di riscontro nei tempi previsti
- Fondato motivo del segnalante, sulla base di circostanze concrete allegate ed informazioni effettivamente acquisibili, di ritenere che la violazione possa costituire un pericolo imminente/palese per il pubblico interesse
- Fondato motivo del segnalante di ritenere che la segnalazione esterna possa comportate il rischio di ritorsioni o non avere efficace seguito in ragione di specifiche circostanze del caso concreto (ad es., rischio di occultamento/distruzione prove, rischio di collusione/coinvolgimento tra chi riceve la segnalazione e l'autore della violazione)

Il ricevimento di eventuali segnalazioni o reclami (con riferimento esclusivamente al controllo dell'eventuale presenza di moduli di segnalazione compilati all'interno delle cassette postali) è monitorato dalla funzione Assicurazione Qualità con cadenza mensile.

Al ricevimento di eventuali segnalazioni per mezzo della modulistica "M.12.3 Modulo di Segnalazione" deve seguire una protocollazione riservata, mediante autonomo registro, da parte del gestore delle segnalazioni, attraverso la piattaforma *software* per la gestione delle segnalazioni.

Nel caso in cui, erroneamente, una segnalazione interna venisse presentata ad un soggetto diverso dal gestore delle segnalazioni, la stessa dovrà essere trasmessa, entro 7 giorni dal ricevimento, al gestore stesso (garantendone sempre la riservatezza) e, contestualmente, si dovrà provvedere a dare notizia della relativa trasmissione al segnalante (se lo stesso dichiara espressamente di voler usufruire delle tutele da *whistleblower* o ciò risulti, comunque, desumibile dalla segnalazione o da altri comportamenti). In caso non si verificasse tale scenario, la segnalazione è da considerarsi quale segnalazione ordinaria.

Con riferimento alle segnalazioni inerenti al D. Lgs. 231/01, le stesse devono essere indirizzate all'OdV della società (ad es., attraverso l'apposizione, da parte del segnalante, all'inizio della propria segnalazione, della dicitura "*alla c.a. dell'O.d.V.*") e gestite secondo le modalità ed i principi di cui alla procedura **PO 10.14 Gestione dei flussi informativi OdV**.

4.2. Inoltro delle segnalazioni (canale esterno)

Il soggetto preposto alla gestione delle segnalazioni esterne è, in prima istanza, ANAC (Autorità Nazionale AntiCorruzione – unico soggetto competente a valutare le segnalazioni e l'eventuale applicazione delle sanzioni). Successivamente, la stessa potrebbe, in base alla competenza della segnalazione, coinvolgere altre autorità esterne (ad es., Autorità giudiziaria, Autorità amministrativa, Istituzioni/organi/organismi dell'Unione Europea).

Anche eventuali ritorsioni devono essere comunicate all'ANAC tramite la propria piattaforma informatica (nel caso inviate a soggetti diversi da ANAC, quest'ultimi garantiscono la riservatezza dell'identità del segnalante e la trasmettono ad ANAC, notificandone contestualmente il segnalante), fornendo elementi oggettivi dai quali si possa dedurre la consequenzialità tra la segnalazione effettuata e la lamentata ritorsione.

Anche in questo caso vengono garantiti (ad es., attraverso strumenti di crittografia, accessi con autenticazione informatica a più fattori, oscuramenti), anche in caso di utilizzo di canali diversi o di ricevimento da parte di personale diverso da quello succitato addetto al trattamento delle segnalazioni (con trasmissione, entro 7 giorni dal ricevimento, a quest'ultimo, e relativo notizia di trasmissione al segnalante):

- Riservatezza dell'identità del segnalante, della persona coinvolta, della persona menzionata
- Riservatezza del contenuto della segnalazione (e della relativa documentazione)

Le segnalazioni esterne possono essere effettuate nelle seguenti forme (vedasi, per maggiori dettaglio sulle modalità di acquisizione delle segnalazioni esterne, Regolamento e Linee Guida ANAC pubblicate all'interno del proprio sito istituzionale):

- Scritta, attraverso compilazione ed invio modulistica presente all'interno dell'apposita area della piattaforma informatica (disponibile nel sito istituzione di ANAC), senza preventiva necessità di autenticazione, fornendo sia le

informazioni obbligatorie sia il maggior numero possibile di quelle facoltative in modo chiaro, preciso e circostanziato; tale piattaforma informatica permette al segnalante di accedere alla propria segnalazione fino a 5 anni successivi alla data di chiusura del fascicolo da parte di ANAC (attraverso il codice alfanumerico fornito al segnalante all'esito dell'inoltro della segnalazione, utile anche per monitorare lo svolgimento del procedimento, integrare la propria segnalazione, e dialogare in modo anonimo e sicuro con ANAC)

- Orale, attraverso linee telefoniche (con operatore messo a disposizione da ANAC), sistemi di messaggistica vocale (attraverso registrazioni di massimo 15 minuti e successivo inserimento sulla piattaforma ANAC nei giorni/fasce orarie stabilite e pubblicate nel sito istituzione ANAC) o, su richiesta motivata del segnalante, incontro diretto (fissato entro un termine ragionevole); in tali casi, ANAC garantisce comunque la riservatezza mediante l'utilizzo di un protocollo su apposito registro riservato

Anche in questo caso, l'ANAC provvede a:

- Dare avviso al segnalante del ricevimento della segnalazione entro 7 giorni dallo stesso (salvo esplicita richiesta contraria del segnalante o casi in cui ANAC ritenga che tale avviso potrebbe pregiudicare la protezione della riservatezza dell'identità del segnalante)
- Dare riscontro al segnalante entro 3/6 mesi dalla data di avviso di ricevimento, od entro 3/6 mesi e 7 giorni dal ricevimento della segnalazione esterna
- Comunicare al segnalante l'esito finale della procedura (archiviazione, trasmissione ad autorità amministrative/giudiziarie competenti, raccomandazioni/sanzioni amministrativa)

All'interno di tale ambito ricadono anche:

- Presentazione di denunce alle autorità competenti (giudiziaria/contabile)
- Divulgazioni pubbliche, tramite stampa o mezzi elettronici quali:
    - Piattaforme *web* o *social media*
    - Mezzi di informazione giornalistica
    - Rappresentanti eletti
    - Organizzazioni della società civile
    - Sindacati
    - Organizzazioni imprenditoriali/professionali

  Le condizioni per una divulgazione pubblica sono le seguenti:

    - Precedente segnalazione interna ed esterna (o direttamente esterna) da parte del segnalante senza riscontro sul seguito, nei termini previsti, per quanto riguarda le misure adottate, o da adottare
    - Fondato motivo (su circostanze ed informazioni concrete allegate/acquisibili, non sufficienti semplici illazioni) del segnalante di ritenere che la violazione possa costituire un pericolo imminente/palese per il pubblico interesse

- Fondato motivo del segnalante di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito (ad es., rischio di occultamento/distruzione prove, chi riceve la segnalazione sia colluso con l'autore della violazione o coinvolto nella violazione stessa, archiviazione immotivata causa accordi tra chi riceve la segnalazione e la persona coinvolta nella violazione)

Nel caso in cui il segnalante riveli volontariamente la propria identità, non sussiste, in questo scenario, la tutela della riservatezza (ferme restando, invece, tutte le altre forme di protezione). Nel caso, invece, di utilizzo di uno pseudonimo/*nickname* che non consenta l'identificazione del segnalante, la divulgazione viene trattata come una segnalazione anonima da parte di ANAC.

4.2.1. Inoltro delle comunicazioni di ritorsioni

Per quanto concerne la comunicazione di ritorsioni, la stessa deve riportare, a pena di inammissibilità:

- Denominazione e recapiti completi dell'interessato ed, ove disponibile, un indirizzo PEC (che ANAC utilizzerà per eventuali comunicazioni)
- Autore della presunta ritorsione
- Fatti origine della comunicazione
- Documenti a sostegno della comunicazione

Questa tipologia di comunicazione viene considerata inammissibile, ed archiviata d'ufficio con relativa comunicazione attraverso piattaforma informatica all'autore della stessa, in caso di:

- Manifesta infondatezza per assenza di elementi di fatto idonei a giustificare accertamenti
- Manifesta insussistenza dei presupposti di legge per l'esercizio dei poteri di vigilanza dell'ANAC
- Finalità palesemente emulativa
- Accertato contenuto generico della comunicazione o, comunque, tale da non consentire la comprensione dei fatti, o comunicazione corredata da documentazione non appropriata/inconferente
- Produzione di sola documentazione (in assenza di comunicazione)
- Mancanza di dati che costituiscono elementi essenziali della comunicazione

In questo caso, laddove occorra acquisire informazioni, chiarimenti o documentazione ulteriore, l'ANAC può:

- Convocare in audizione i soggetti in possesso degli stessi
- Inviare loro una richiesta di integrazione documentale con termine entro il quale fornire riscontro non superiore a 30 giorni

Tanto l'autore della comunicazione quanto il presunto responsabile della ritorsione possono accedere agli atti amministrativi del procedimento sanzionatorio.

A seguito dell'avvio del procedimento, può anche essere effettuata eventuale comunicazione di presunte ritorsioni, ulteriori e diverse da quelle originariamente indicate, nel caso in cui le stesse si siano verificate successivamente alla contestazione degli addebiti.

Infine, il provvedimento conclusivo del procedimento, sia esso di archiviazione (per riscontrata assenza dei presupposti di fatto o di diritto per la comminazione di una sanzione) piuttosto che sanzionatorio (in caso, invece, di accertamento), viene comunicato sia al presunto responsabile sia al *whistleblower*. In quest'ultimo caso, inoltre, l'Autorità giudiziaria adotta tutte le misure necessarie ad assicurare la tutela:

- Risarcimento danni/pagamento indennità risarcitoria (incluso versamento contributi previdenziali ed assistenziali)
- Nullità del licenziamento
- Reintegrazione nel posto di lavoro o, a discrezione del lavoratore, pagamento indennità sostitutiva
- Ordine di cessazione della condotta posta in essere
- Dichiarazione di nullità degli atti adottati

4.3. Gestione delle segnalazioni (canale interno)

Al ricevimento di una segnalazione anonima interna, Cantine Settesoli è tenuta a:

- Registrare la stessa in forma anonima (se desiderato dal segnalante), attraverso la piattaforma *software* per la gestione delle segnalazioni[6]
- Conservarne la documentazione (in una forma che consenta l'identificazione degli interessati) per un periodo non superiore al tempo necessario per trattare e dare adeguato seguito alla segnalazione e, comunque, non superiore ai 5 anni[7] a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione[8] (attraverso la piattaforma *software* per la gestione delle segnalazioni, con la relativa funzione di estrapolazione del report automatico per l'archiviazione del caso), secondo il principio di "limitazione della conservazione"[9]. Al fine di valutare il tempo necessario di conservazione i dati sono sottoposti ad esame periodico per verificarne la persistente necessità di conservazione (piuttosto che cancellati od anonimizzati una volta decorso tale termine).

[6] Per garantire l'anonimato/riservatezza, la piattaforma assicura che nessun indirizzo IP, tracciamento dei cookie, dati personali o marca temporale venga memorizzata nel sistema; le preferenze vengono memorizzate in modo permanente nel browser, assicurando che ogni volta che il segnalante torna al proprio canale di segnalazione sicuro, il browser rilevi le voci dell'archivio locale riconoscendo lo stesso dominio e lo stesso protocollo utilizzati durante l'ultima visita al sistema

[7] Eventuali periodi più lunghi devono essere giustificati da: archiviazione nel pubblico interesse, ricerca scientifica o storica, fini statistici

[8] Punto applicabile anche alle segnalazioni esterne

[9] Tale principio si applica, ovviamente, anche ai seguenti casi: segnalazione attraverso linea telefonica registrata o sistema di messaggistica vocale registrato, linea telefonica o sistema di messaggistica vocale non registrati (ma documentati per iscritto), segnalazione orale nel corso di un incontro con il personale addetto (documentato mediante registrazione o mediante verbale)

Al momento Cantine Settesoli non ha ancora attivato la possibilità di inoltrare segnalazioni orali attraverso linea telefonica dedicata; ciò nonostante, nel caso ciò venisse successivamente messo in atto, tale modalità dovrà rispettare quanto segue:

- Se presente registrazione: post consenso del segnalante, la segnalazione verrà registrata (su dispositivo idoneo alla conservazione ed all'ascolto) o trascritta integralmente
- Se non presente registrazione: segnalazione riportata per iscritto mediante resoconto dettagliato della conversazione

In ambo i casi il segnalante avrà la possibilità di verificare, rettificare o confermare i contenuti attraverso la propria sottoscrizione.

Nel caso di segnalazione fatta nel corso di un incontro diretto su richiesta del segnalante, sempre previo consenso di quest'ultimo, la stessa viene documentata attraverso:

- Registrazione (su dispositivo idoneo alla conservazione ed all'ascolto)
- Verbale d'incontro (anche in questo caso lo stesso può essere verificato, rettificato o confermato dal segnalante prima della propria sottoscrizione)

Il gestore delle segnalazioni, una volta ricevuta una segnalazione interna, è tenuto, nel dettaglio, a:

- Rilasciare al segnalante l'avviso di ricevimento della stessa entro 7 giorni dalla data di ricezione (attraverso la piattaforma *software* per la gestione delle segnalazioni, e la relativa funzione di reminder per il rispetto scadenze)
- Mantenere le comunicazioni dirette con il segnalante e richiedere allo stesso, ove necessario, eventuali integrazioni (attraverso la piattaforma *software* per la gestione delle segnalazioni, grazie alla relativa funzione di chat criptata con il segnalante); in particolare, il gestore può:
  - Chiedere chiarimenti, documenti ed ulteriori informazioni al segnalante (anche di persona)
  - Acquisire atti o documenti da altri uffici
  - Coinvolgere terze persone
- Dare diligente e corretto seguito alla segnalazione (attraverso la piattaforma *software* per la gestione delle segnalazioni), con particolare riferimento a:
  - Rispetto delle tempistiche di riscontro
  - Tutela della riservatezza dei dati e delle identità
  - Modalità di conservazione
  - Adeguata procedimentalizzazione della gestione (processi interni trasparenti per l'effettuazione preliminare dell'analisi della fondatezza e della sussistenza dei fatti segnalati, esito delle indagini, criteri utilizzati per le eventuali misure da adottare). Dato che l'applicabilità delle tutele previste per il segnalante risulta collegata alla valutazione della presenza dei requisiti essenziali della segnalazione ai fini della relativa ammissibilità, al fine di valutare quest'ultimi il gestore delle segnalazioni potrà far riferimento a:

- Manifesta infondatezza per assenza di elementi di fatto idonei a giustificare accertamenti
- Contenuto generico, tale da non consentire la comprensione dei fatti
- Documentazione a corredo non appropriata od inconferente

Il gestore delle segnalazioni deve, quindi, effettuare una prima imparziale deliberazione sulla sussistenza di quanto segnalato. Nel caso in cui quest'ultima venga ritenuta ammissibile, lo stesso avvia l'istruttoria interna per valutarne la sussistenza, sempre nel rispetto di:

- Specifiche norme di settore
- Limiti in materia di controlli a distanza
- Disposizioni riguardo al divieto, da parte del datore di lavoro, di acquisire e trattare informazioni e fatti non rilevanti per la valutazione dell'attitudine professionale dei lavoratori, o comunque afferenti la propria sfera privata
- Normativa in materia di protezione dei dati personali

A questo punto:

- Se vengono ravvisati elementi di manifesta infondatezza, si procede con l'archiviazione (con relativa adeguata motivazione)
- In caso di fondatezza, invece, il gestore delle segnalazioni dovrà rivolgersi immediatamente agli organi preposti competenti interni od esterni (non è compito del gestore delle segnalazioni, infatti, né accertare eventuali responsabilità individuali, né effettuare controlli di legittimità/merito)

- Fornire riscontro alla segnalazione entro 3 mesi dalla data di avviso di ricevimento, o entro 3 mesi e 7 giorni dalla data di presentazione (attraverso la piattaforma *software* per la gestione delle segnalazioni, e la relativa funzione di reminder per il rispetto scadenze). Tale riscontro deve tradursi nella comunicazione al segnalante delle informazioni sul seguito dato, o che si intende dare, alla segnalazione; a seconda dei casi, può consistere in:
  - Comunicazione di archiviazione
  - Avvio di inchiesta interna (con eventuali risultati)
  - Provvedimenti adottati
  - Rinvio ad autorità competente per ulteriori indagini

Nelle procedure di segnalazione interna (ma lo stesso vale anche in caso di segnalazione esterna), la persona coinvolta può essere sentita o, su propria richiesta, viene sentita anche attraverso l'acquisizione di osservazioni scritte/documenti.

5. **ALLEGATI**

- **M.12.3 MSEG - Modulo di Segnalazione**

- Manuale Operativo Piattaforma EQS Integrity Line