

**PROCEDURA
PROCEDURA PER LA TUTELA DELL'AUTORE DI
SEGNALAZIONI DI CONDOTTE ILLECITE (CD.
WHISTLEBLOWER)
PC_SEPCO_001_SEPCO/ 2**

**Unità di riferimento:
DGHOLD\SEPCO**

Versione : 2

	Nome	Data
Redattori	SEPCO	13/07/2023
Controllori		
Approvatori	SEPCO	

--	--

Indice

1. SCOPO E CAMPO DI APPLICAZIONE	3
2. RIFERIMENTI	3
3. TERMINI E DEFINIZIONI	4
4. RESPONSABILITA'	6
4.1 I SOGGETTI CHE POSSONO FARE LE SEGNALAZIONI - "Whistleblowers"	6
4.2 IL RUOLO DEL RESPONSABILE DELLA PREVENZIONE DELLA CORRUZIONE E TRASPARENZA	6
4.3 RAPPORTI TRA IL RPCT E IL CUSTODE DELL'IDENTITÀ	7
5. INFORMAZIONE, FORMAZIONE E ADDESTRAMENTO	8
5.1 SENSIBILIZZAZIONE, PROMOZIONE E FORMAZIONE SUL TEMA DEL WHISTLEBLOWING	9
6. COMUNICAZIONE	9
7. REGISTRAZIONE/CONSERVAZIONE.....	9
7.1 CONSERVAZIONE DELLE SEGNALAZIONI.....	9
8. MODALITA' OPERATIVE	10
8.1 LA SEGNALAZIONE: OGGETTO, REQUISITI E CONTENUTO	10
8.2 SEGNALAZIONI DI ATTIVITÀ ILLECITE.....	11
8.2.1 CANALI DI SEGNALAZIONE INTERNI.....	12
A. IL SISTEMA TECNOLOGICO-INFORMATICO DI GESTIONE DELLE SEGNALAZIONI INTERNE	13
B. GESTIONE DELLE SEGNALAZIONI INTERNE DI CONDOTTE ILLECITE TRAMITE L'APPLICATIVO TECNOLOGICO-INFORMATICO	13
8.2.2 CANALE DI SEGNALAZIONE ESTERNO.....	14
8.3 TUTELA DEL WHISTLEBLOWER (IVI INCLUSO IL DIVIETO DI RITORSIONE)	15
8.4 SANZIONI	17
9 DISPOSIZIONI FINALI.....	18
10 CRONOLOGIA DELLE VARIAZIONI.....	19

--	--

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente documento disciplina la procedura di tutela della persona segnalante (il c.d. whistleblower), nonché le modalità attraverso cui quest'ultimo può effettuare una segnalazione di comportamenti illeciti, commissivi od omissivi, che costituiscano o possano costituire una violazione di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse delle Società del Gruppo AVM, di cui sia venuto a conoscenza nell'ambito del contesto lavorativo.

Obiettivi fondamentali della presente disciplina organizzativa, vigente per le Società del Gruppo AVM, sono quelli di:

- rimuovere i fattori che possano ostacolare o disincentivare il ricorso all'istituto del whistleblowing;
- evitare che un soggetto, venuto a conoscenza di condotte illecite nell'ambito del contesto lavorativo, ometta di segnalarle per il timore di subire conseguenze pregiudizievoli;
- garantire la massima riservatezza e la completa protezione del whistleblower.

2. RIFERIMENTI

Il 29 dicembre 2017 è entrata in vigore la Legge 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”* (pubblicata sulla Gazzetta Ufficiale, Serie Generale n. 291 del 14 dicembre 2017), avente lo scopo di incentivare la collaborazione dei lavoratori per favorire l'emersione dei fenomeni corruttivi all'interno di enti pubblici e privati.

L'articolo 2 della Legge n. 179/17 è intervenuto sul Decreto 231 inserendo all'articolo 6 *“Soggetti in posizione apicale e modelli di organizzazione dell'ente”* una nuova previsione che inquadra, nell'ambito del Modello 231, le misure legate alla gestione dell'istituto c.d. Whistleblowing.

Inoltre, il 30 marzo 2023 è entrato in vigore il Decreto Legislativo 10 marzo 2023, n. 24 di *“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”* (pubblicato sulla Gazzetta Ufficiale, Serie Generale n. 63 del 15 marzo 2023), introducendo una disciplina strutturata per garantire la protezione degli informatori/segnalanti o *“whistleblowers”*, ossia delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione Europea che ledono l'interesse pubblico o l'integrità dell'Amministrazione Pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato.

Inoltre, la presente procedura è stata predisposta in accordo con le normative di riferimento applicabili e alle norme di adesione volontaria, nonché ad eventuali documenti generali di riferimento per le Società del gruppo AVM, in particolare:

--	--

RIFERIMENTI NORMATIVI	Applicabilità
D.Lgs.81/2008 e s.m.i.	
D.Lgs.152/2006 e s.m.i.	
D-Lgs. 231/2001 e s.m.i.	x
Legge 190/2012 e s.m.i.	x
Regolamento (Ue) 2016/679	x
ISO 9001:2015	
ISO 14001:2015	
ISO 45001:2018	

Il trattamento dei dati personali deve essere conforme al GDPR - Regolamento UE 2016/679 e al Codice privacy - DLGS 196/03.

Le funzioni interessate devono procedere secondo i principi della privacy by design e by default, con particolare riferimento ai termini di conservazione previsti nel Registro della attività di trattamento (PS/088 Procedura per la tenuta e l'aggiornamento del Registro delle attività di trattamento), nonché a quanto contenuto nella informativa ai dipendenti e nelle lettere di autorizzazione al trattamento dei dati, rispettivamente rese ai sensi degli artt. 13 e 29 GDPR, nel REG/0004 Regolamento per l'utilizzo degli strumenti e delle dotazioni tecniche aziendali delle società del Gruppo AVM e nelle altre procedure aziendali in materia di tutela dei dati personali.

3. TERMINI E DEFINIZIONI

Si intende:

- per *whistleblowing*, la segnalazione di informazioni, riguardo ad un fatto o una condotta illecita o irregolare successa, percepita o al rischio della stessa, agli organi che, secondo quanto previsto dalla legge, possano agire efficacemente al riguardo;
- per *whistleblower*, la persona che segnala, divulga ovvero denuncia all'Autorità Giudiziaria o contabile, violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui sia venuta a conoscenza in un contesto lavorativo pubblico o privato;
- tutela del whistleblower*, la garanzia accordata al whistleblower di tutela e protezione, anche attraverso l'anonimato, contro ogni forma di discriminazione che potrebbe derivare direttamente e indirettamente dalla segnalazione di illecito;

--	--

- d) *custode dell'identità*, è il soggetto individuato dal Gruppo AVM che, dietro esplicita e motivata richiesta, consente al Responsabile della Prevenzione Corruzione e Trasparenza (in seguito RPCT) di accedere all'identità del segnalante. L'identità del segnalante non è nota al custode e quest'ultimo non è coinvolto nel trattamento dati personali presenti nella segnalazione.

--	--

4. RESPONSABILITA'

La descrizione generale dei ruoli e singole responsabilità vengono definite all'interno del documento *Definizione Struttura Organizzativa* e relativi organigrammi funzionali e della singola struttura aziendale.

4.1 I SOGGETTI CHE POSSONO FARE LE SEGNALAZIONI - “Whistleblowers”

I Destinatari della presente procedura (di seguito “Segnalanti” o “Whistleblowers”) sono i soggetti che operano nel contesto lavorativo delle Società del Gruppo, in qualità di:

- dipendenti;
- lavoratori autonomi; “
- collaboratori, liberi professionisti e consulenti;
- volontari e i tirocinanti, retribuiti e non retribuiti;
- azionisti e persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto.

Il whistleblower è legittimato ad effettuare la propria segnalazione nei casi in cui:

- il rapporto giuridico è in corso;
- durante il periodo di prova;
- il rapporto giuridico non è ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali;
- successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite prima dello scioglimento del rapporto stesso.

4.2 IL RUOLO DEL RESPONSABILE DELLA PREVENZIONE DELLA CORRUZIONE E TRASPARENZA

Il Responsabile della Prevenzione della Corruzione e Trasparenza (d'ora in poi RPCT) è individuato come soggetto preposto alla gestione delle segnalazioni interne.

Nel solo caso in cui il RPCT si trovi in posizione di conflitto di interessi rispetto alla condotta illecita segnalata ovvero nei casi di temporanea assenza dello stesso, giustificati da motivi sopravvenuti, le società del Gruppo AVM, in accordo con l'Organismo di Vigilanza, individuano un soggetto terzo idoneo a sostituirlo nella gestione e analisi della segnalazione. Tale soggetto terzo è attualmente identificato nel ruolo del Direttore Generale di gruppo; quest'ultimo all'avverarsi delle sovra specificate condizioni provvederà a richiedere alla funzione TECMO l'attivazione delle credenziali sostitutive di gestione della singola segnalazione e/o per il periodo di necessità, a seguito del quale l'operatività ritornerà unicamente in capo al RPCT.

--	--

Il ruolo del RPCT si sostanzia in una attività istruttoria. Spetta infatti al RPCT la valutazione dei requisiti essenziali per poter accordare al segnalante le tutele ivi previste.

La segnalazione è considerata inammissibile per:

- a) manifesta mancanza di interesse all'integrità del Gruppo AVM;
- b) manifesta incompetenza del Gruppo AVM sulle questioni segnalate;
- c) manifesta infondatezza per l'assenza di elementi di fatto idonei a giustificare accertamenti;
- d) manifesta insussistenza dei presupposti di legge per l'esercizio dei poteri di vigilanza del Gruppo AVM;
- e) accertato contenuto generico della segnalazione di illecito tale da non consentire la comprensione dei fatti, ovvero segnalazione di illeciti corredata da documentazione non appropriata o inconferente;
- f) produzione di sola documentazione in assenza della segnalazione di condotte illecite o irregolarità;
- g) mancanza dei dati che costituiscono elementi essenziali della segnalazione di illeciti.

Nei suddetti casi l'RPCT procede all'archiviazione che viene comunicata al whistleblower tramite i canali di segnalazione interna (cfr. par. 8.2.1)

Nei casi di cui alle lett. c) e g), il RPCT, ove quanto denunciato non sia adeguatamente circostanziato, può chiedere al whistleblower, tramite il canale di segnalazione interna, elementi integrativi o anche di persona, ove il segnalante acconsenta.

Una volta valutata la qualifica del segnalante (cfr. par. 4.1), nonché la l'ammissibilità della segnalazione, quale segnalazione di whistleblowing, il RPCT avvia l'istruttoria interna sui fatti o sulle condotte segnalate con l'eventuale coinvolgimento delle funzioni responsabili e/o dell'Autorità Giudiziaria competente.

Spetta al RPCT compiere una prima imparziale delibazione sulla sussistenza di quanto rappresentato nella segnalazione, in coerenza con il dato normativo, che si riferisce a una attività "di verifica e di analisi" e non di accertamento sull'effettivo accadimento dei fatti.

Nel caso in cui il segnalante rientri nel novero dei soggetti legittimati ad assumere la qualifica di whistleblower, nonché la segnalazione sia ammissibile, e quindi sia considerata segnalazione di whistleblowing, il RPCT deve avviare l'istruttoria interna sui fatti o sulle condotte segnalate.

Non spetta al RPCT accertare le responsabilità individuali, svolgere controlli di legittimità o di merito su atti e provvedimenti adottati da figure del Gruppo AVM ad oggetto di segnalazione; la competenza è dell'Autorità Giudiziaria nei cui confronti il RPCT si limita a segnalare la circostanza.

4.3 RAPPORTI TRA IL RPCT E IL CUSTODE DELL'IDENTITÀ

Il Custode dell'identità è il soggetto individuato dal Gruppo AVM che, previo consenso espresso del segnalante e dietro esplicita e motivata richiesta del RPCT, consente a quest'ultimo e/o all'Autorità Giudiziaria di accedere all'identità del segnalante; per il gruppo

--	--

AVM tale soggetto attualmente è stato identificato nel ruolo del Responsabile Funzione Tecnologie della Mobilità (TECMO)

L'identità del segnalante non è nota al custode. Inoltre, il custode non è coinvolto nel trattamento dei dati personali presenti nella segnalazione (lo stesso opera in qualità di autorizzato al trattamento ex Reg. UE 2016/679).

L'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate senza il consenso espresso della stessa persona segnalante a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni. In particolare, nell'ambito del 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. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità.

Inoltre, in due casi espressamente previsti dal D.Lgs. 24/2023, per rivelare l'identità del segnalante, oltre al consenso espresso dello stesso, si richiede anche una comunicazione scritta delle ragioni di tale rivelazione:

- nel procedimento disciplinare laddove il disvelamento dell'identità del segnalante sia indispensabile per la difesa del soggetto a cui viene contestato l'addebito disciplinare;
- nei procedimenti instaurati in seguito a segnalazioni interne o esterne laddove tale rivelazione sia indispensabile anche ai fini della difesa della persona coinvolta.

Una volta soddisfatti i suddetti requisiti, il Responsabile della gestione della segnalazione esprime motivatamente tale necessità al Custode dell'Identità; questi dopo aver idoneamente accertato l'effettiva presenza della necessità, disvela l'identità al suddetto Responsabile.

Le comunicazioni tra RPCT e Custode dell'identità, al fine del rispetto dell'anonimato, si avvalgono prioritariamente del sistema tecnologico-informatico di corrispondenza ad uso esclusivo degli stessi; eventuale documentazione di supporto utile al rilascio dell'identità (ad.es. provvedimenti dell'autorità giudiziaria), potranno essere verificati di persona dal Custode dell'identità.

5. INFORMAZIONE, FORMAZIONE E ADDESTRAMENTO

La presente procedura è ad oggetto di formazione per tutti i soggetti aziendali; in particolare vi si devono rapportare e promuovere tutti i process owners nella stesura, verifica e approvazione di regolamenti, procedure, istruzioni operative, disposizioni di servizio e nella redazione dei contratti e dei documenti che regolano i rapporti negoziali con soggetti terzi richiamati dalla normativa.

--	--

5.1 SENSIBILIZZAZIONE, PROMOZIONE E FORMAZIONE SUL TEMA DEL WHISTLEBLOWING

Il Responsabile della prevenzione della corruzione e trasparenza nell'ambito del piano di formazione 231-190, e con la pubblicazione della presente procedura sensibilizza i soggetti aziendali alle finalità dell'istituto del "whistleblowing" mettendo a disposizione informazioni chiare sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni interne, nonché sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni esterne. Le suddette informazioni sono rese facilmente disponibili nella "Intranet" aziendale e in ambito di "Trasparenza" ove si trovano indicate la presente disciplina e le risposte a domande frequenti (c.d. faq), comprensive dei link di dettaglio alla normativa di riferimento.

Il Gruppo AVM di concerto con l'RPCT e gli ODV si riserva di intraprendere ulteriori iniziative di sensibilizzazione e di promozione, ritenuti idonei a divulgare la conoscenza dell'istituto ed a determinare la creazione di un contesto culturale e sociale favorevole alla diffusione della procedura.

L'RPCT inserisce nella Relazione Annuale di cui all'art. 1 comma 14 della L. 190/2012 e nel registro di "Trasparenza" il numero delle segnalazioni ricevute.

6. COMUNICAZIONE

La presente procedura viene comunicata internamente con la pubblicazione a mezzo Archiflow e/o SPRISS, nei riguardi di tutti i soggetti aziendali coinvolti ed ODV; esternamente viene comunicata in ambito di Trasparenza e dai dirigenti process owners coinvolti nei diversi rapporti negoziali con i soggetti terzi. L'RPCT provvede in favore di singole richieste, in particolare, si rapporta con il DPO e/o eventuali Enti Terzi di Certificazione.

7. REGISTRAZIONE/CONSERVAZIONE

Tutta la documentazione di sistema è reperibile in Archiflow.

Le modalità e tempistica di conservazione della documentazione di sistema viene riportata all'interno della singola procedura e/o IOP e comunque non può essere inferiore ad 1 anno.

7.1 CONSERVAZIONE DELLE SEGNALAZIONI

Le segnalazioni sono archiviate e conservate per il tempo necessario al trattamento della segnalazione dei dati e dei documenti oggetto della segnalazione, e comunque non oltre i cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

--	--

8. MODALITA' OPERATIVE

8.1 LA SEGNALAZIONE: OGGETTO, REQUISITI E CONTENUTO

I Destinatari che rilevino o vengano a conoscenza di possibili comportamenti illeciti o irregolarità sono tenuti a segnalare, tramite i canali di seguito indicati, i fatti, gli eventi e le circostanze che gli stessi ritengano, in buona fede e sulla base di ragionevoli elementi di fatto, aver determinato tali violazioni e/o condotte non conformi ai sensi della normativa vigente.

Nello specifico, oggetto di segnalazione possono essere i comportamenti, gli atti o le omissioni che ledono l'interesse pubblico o l'integrità delle Società del Gruppo consistenti in:

- a) Violazioni di disposizioni normative nazionali:
 - illeciti amministrativi, contabili, civili o penali;
 - condotte illecite rilevanti ai sensi del decreto legislativo 8 giugno 2001, n. 231 o violazioni dei Modelli 231 delle Società del Gruppo AVM e dei relativi allegati;
- b) Violazioni di disposizioni normative europee:
 - illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e 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 riguardanti il mercato interno (a titolo esemplificativo: violazioni in materia di concorrenza e di aiuti di Stato);
 - atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione.

In aggiunta, la segnalazione può avere anche ad oggetto:

- le informazioni relative alle condotte volte ad occultare le violazioni sopra indicate;
- le attività illecite non ancora compiute ma che il whistleblower ritenga ragionevolmente possano verificarsi in presenza di elementi concreti precisi e concordanti;

--	--

- i fondati sospetti, la cui nozione dovrà essere oggetto di interpretazione al tavolo delle linee Guida.

La segnalazione deve essere fatta in buona fede e non deve essere fondata su meri sospetti o voci. Inoltre, la segnalazione deve essere il più possibile circostanziata e offrire il maggior numero di elementi per consentire alla Società di effettuare le dovute verifiche ed attività istruttorie. Al tempo stesso, si specifica che non è necessario che il segnalante sia certo dell'effettivo avvenimento dei fatti denunciati e dell'autore degli stessi: si ritiene sufficiente che il segnalante, in base alle proprie conoscenze, ritenga altamente probabile l'essersi verificato di un fatto illecito.

È necessario che le condotte illecite segnalate siano state apprese in ragione del rapporto di lavoro, ossia a causa o in ragione di esso: si deve trattare di fatti accaduti all'interno del Gruppo AVM o comunque relativi ad esso.

Rimangono, invece, escluse dall'ambito del D.Lgs. 24/2023, e pertanto non possono essere oggetto di segnalazione, divulgazione pubblica o denuncia:

- le contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante che attengono esclusivamente ai propri rapporti individuali di lavoro o di impiego pubblico, ovvero inerenti ai propri rapporti di lavoro o di impiego pubblico con le figure gerarchicamente sovraordinate;
- le segnalazioni di violazioni laddove già disciplinate in via obbligatoria dagli atti dell'Unione europea o nazionali indicati nella parte II dell'allegato al decreto ovvero da quelli nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nella parte II dell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nella parte II dell'allegato al decreto;
- le segnalazioni attinenti ai rapporti individuali di lavoro e quelle in materia di sicurezza e difesa nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato pertinente dell'Unione europea.

Responsabile: Whistleblowers

8.2 SEGNALAZIONI DI ATTIVITÀ ILLECITE

Le segnalazioni devono essere trasmesse attraverso i canali appositamente predisposti, tramite un applicativo tecnologico-informatico accessibile dall'intranet aziendale nella sezione "applicativi" o dal sito web aziendale sezione società trasparente.

Oltre ai canali di segnalazione interna alle Società del Gruppo, nei casi espressamente previsti dal D.Lgs. 24/2023 e ferma restando la preferenza per il canale interno, il segnalante può effettuare la propria segnalazione attraverso ulteriori canali, c.d. esterni, illustrati al paragrafo 8.2.2.

--	--

I canali interni ed esterni garantiscono, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità del segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione. La riservatezza è garantita altresì con riguardo al contenuto della segnalazione e della relativa documentazione.

8.2.1 CANALI DI SEGNALAZIONE INTERNI

I canali di segnalazione interna prevedono l'effettuazione di segnalazioni, in forma scritta e orale, tramite un applicativo tecnologico-informatico online accessibile dalla intranet aziendale, dal sito web aziendale o dal link di seguito indicato:

<https://gruppoavmspa.segnalazioni.net>

Una volta eseguito l'accesso all'applicativo tecnologico-informatico, la persona segnalante può scegliere di effettuare una segnalazione scritta, compilando l'apposito modulo, ovvero in forma orale mediante un sistema di messaggistica vocale da effettuare nell'apposita sezione dedicata.

La segnalazione orale, previo consenso della persona segnalante, è documentata a cura del RPCT mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante trascrizione integrale. In caso di trascrizione, la persona segnalante può verificare, rettificare o confermare il contenuto della trascrizione mediante la propria sottoscrizione.

Inoltre, il segnalante può richiedere un incontro diretto con il RPCT che deve essere fissato da quest'ultimo entro un termine ragionevole. In tale caso, la segnalazione, previo consenso della persona segnalante, è documentata a cura del RPCT mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale. In caso di verbale, la persona segnalante può verificare, rettificare e confermare il verbale dell'incontro mediante la propria sottoscrizione.

Il segnalante deve fornire tutti gli elementi utili a consentire l'avvio dell'istruttoria procedimentale di accertamento e riscontro della fondatezza condotta illecita oggetto della segnalazione.

A tal fine, è necessario che la segnalazione contenga le seguenti informazioni a pena di inammissibilità:

- una chiara, dettagliata e completa descrizione dei fatti illeciti;
- l'ente, le circostanze di tempo e di luogo in cui si sono verificati i fatti;
- le generalità (o altri elementi quali la qualifica, il ruolo o il servizio di appartenenza) dei soggetti coinvolti;
- le generalità di altri soggetti eventualmente coinvolti e/o che possono riferire sul fatto;
- l'indicazione di eventuali imprese o altre persone giuridiche coinvolte;
- l'indicazione di eventuali documenti che possono confermare la fondatezza dei fatti;
- area alla quale può essere riferito il fatto;

--	--

- Direzione/Settore/Servizio cui può essere riferito il fatto;
- indicazione delle motivazioni sull'illiceità dei fatti;
- ogni altra informazione che possa fornire un utile riscontro circa la fondatezza e la sussistenza dei fatti illeciti segnalati.

Responsabile: Whistleblowers

A. IL SISTEMA TECNOLOGICO-INFORMATICO DI GESTIONE DELLE SEGNALAZIONI INTERNE

Come indicato al paragrafo precedente, le segnalazioni interne sono gestite dal RPCT attraverso un sistema tecnologico-informativo, che consente:

- a) l'invio della segnalazione (orale o scritta), mediante un apposito modello che garantisce la raccolta di tutti gli elementi utili alla ricostruzione del fatto e all'accertamento della fondatezza di quanto segnalato. All'interno del sistema sono, altresì, specificate le modalità di compilazione e di invio della segnalazione;
- b) la separazione dei dati identificativi del segnalante dal contesto della segnalazione, prevedendo l'adozione di codici sostitutivi dei dati identificativi, in modo che la segnalazione possa essere processata in modalità anonima e rendere possibile la successiva ricostruzione dell'identità del segnalante solamente mediante l'espresso consenso di quest'ultimo e, comunque, nei soli casi previsti dall'art. 12 del D.lgs. 24/2023;
- c) la tutela della riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione;
- d) la gestione delle segnalazioni in modo trasparente attraverso un iter procedurale definito e comunicato all'esterno con termini certi per l'avvio e la conclusione dell'istruttoria;
- e) la tutela del soggetto che gestisce le segnalazioni da pressioni e discriminazioni, dirette e indirette;
- f) il rispetto della protezione e dell'anonimato del segnalante, nell'ambito delle comunicazioni tra quest'ultimo e il RPCT;
- g) un controllo degli accessi al sistema, ai fini del trattamento delle segnalazioni, riservato esclusivamente ai soggetti che ne hanno diritto;
- h) la gestione delle informazioni e il trasporto dei dati in rete attraverso l'adozione di un protocollo sicuro "https";
- i) di fornire una risposta, su richiesta del segnalante, solo alla scadenza dei termini previsti per la conclusione dell'istruttoria o consentire a quest'ultimo di verificare lo stato di avanzamento della pratica.

B. GESTIONE DELLE SEGNALAZIONI INTERNE DI CONDOTTE ILLECITE TRAMITE L'APPLICATIVO TECNOLOGICO-INFORMATICO

--	--

Il procedimento di gestione delle segnalazioni interne garantisce la riservatezza dell'identità del segnalante dalla ricezione e in ogni contatto successivo alla segnalazione; esso si sviluppa attraverso le seguenti principali fasi:

- a) il segnalante si accredita sull'applicativo tecnologico-informatico di gestione delle segnalazioni;
- b) il segnalante invia una segnalazione (scritta o orale) all'interno dell'applicativo tecnologico-informatico e riceve, subito dopo la separazione dei suoi dati identificativi dal contesto della segnalazione da parte dell'applicativo tecnologico-informatico, un codice sostitutivo utile per i successivi accessi;
- c) la segnalazione arriva direttamente al Responsabile della prevenzione della corruzione che prende in carico la segnalazione per una prima sommaria istruttoria e rilascia alla persona segnalante apposito avviso di ricevimento della segnalazione entro 7 giorni dalla data di ricezione; il RPCT, in qualità di responsabile della gestione della segnalazione, mantiene le interlocuzioni con il soggetto segnalante e, se necessario, chiede chiarimenti e/o integrazioni al segnalante e/o a eventuali altri soggetti coinvolti nella segnalazione, con l'adozione delle necessarie cautele;
- d) il RPCT dà diligente seguito alle segnalazioni ricevute;
- e) il RPCT può decidere, sulla base della valutazione dei fatti oggetto della segnalazione, in caso di evidente e manifesta infondatezza, di archiviare la segnalazione. In caso contrario, valuta a chi inoltrare la segnalazione in relazione ai profili di illiceità riscontrati (ad es. Autorità Giudiziaria);
- f) il segnalante può monitorare lo stato di avanzamento dell'istruttoria accedendo al sistema di gestione utilizzando il codice identificativo ricevuto;
- g) il RPCT fornisce un riscontro al segnalante rispetto alle attività di accertamento entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione, dando conto delle misure previste o adottate o da adottare al fine di dare seguito alla segnalazione e dei motivi della scelta effettuata.

Responsabile: Whistleblowers e RPCT

8.2.2 CANALE DI SEGNALAZIONE ESTERNO

In alternativa ai canali di segnalazione interna sopra riportati, i soggetti segnalanti hanno la possibilità, esclusivamente nei casi previsti dal D.lgs. 24/2023, di effettuare segnalazioni attraverso i canali esterni di seguito indicati.

L'accesso a tali canali è consentito solo al ricorrere di determinate condizioni espressamente previste dall'art. 6 del D.lgs. 24/2023 ovvero:

- nel caso in cui non sia prevista, nell'ambito del 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 a quanto previsto dall'articolo 4;

--	--

- nel caso in cui la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito;
- nel caso in cui la persona segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;
- nel caso in cui la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

a) ***Il ruolo dell'A.N.A.C.***

Le segnalazioni whistleblowing possono essere trasmesse ad A.N.A.C. mediante i canali appositamente predisposti dall'Autorità stessa:

- piattaforma informatica;
- segnalazioni orali;
- incontri diretti fissati entro un termine ragionevole.

b) ***Divulgazione pubblica***

Con la divulgazione pubblica le informazioni sulle violazioni sono rese di pubblico dominio tramite la stampa o mezzi elettronici o comunque attraverso mezzi di diffusione in grado di raggiungere un numero elevato di persone; l'RPCT provvederà ad attività di monitoraggio nei confronti della stampa locale e di almeno un quotidiano di rilevanza nazionale, con eventuali approfondimenti sui c.d. social e quant'altro ritenuto utile.

Nella divulgazione pubblica, ove il segnalante riveli volontariamente la propria identità, non viene in rilievo la tutela della riservatezza, ferme restando tutte le altre forme di protezione previste dal D.lgs 24/2023 per il whistleblower. Laddove, invece, il segnalante divulghi violazioni utilizzando, ad esempio, uno pseudonimo o un nickname, che comunque non ne consente l'identificazione, A.N.A.C. tratterà la divulgazione alla stregua di una segnalazione anonima e avrà cura di registrarla, ai fini della conservazione, per garantire al divulgatore, in caso di disvelamento successivo dell'identità dello stesso, le tutele previste se ha comunicato ritorsioni.

c) ***Denuncia all'Autorità Giurisdizionale***

Il segnalante può inoltrare una denuncia di condotte illecite di cui questi siano venuti a conoscenza nel contesto lavorativo alle Autorità nazionali competenti, giudiziarie e contabili. Si specifica che in tale contesto possono essere denunciati esclusivamente i reati procedibili d'ufficio.

Responsabile: Whistleblowers

8.3 TUTELA DEL WHISTLEBLOWER (IVI INCLUSO IL DIVIETO DI RITORSIONE)

Il Gruppo AVM garantisce l'applicazione di misure di protezione, previste dalla normativa vigente, a favore dei segnalanti, nonché ai seguenti soggetti:

--	--

- facilitatore (persona fisica che assiste il segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve rimanere riservata);
- persone del medesimo contesto lavorativo della persona segnalante, di colui che ha sporto una denuncia o di colui che ha effettuato una divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
- colleghi di lavoro della persona segnalante o della persona che ha sporto una denuncia o effettuato una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;
- enti di proprietà della persona segnalante o per i quali le stesse persone lavorano nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone.

Il responsabile della segnalazione è tenuto a valutare che al momento della segnalazione il segnalante avesse fondati motivi per credere che i fatti riportati fossero veri.

La tutela cessa nel caso in cui sia confermata l'irrilevanza delle motivazioni del segnalante ed anche in caso di condanna in primo grado per diffamazione o calunnia.

Tutela della riservatezza

Nell'incoraggiare i destinatari a segnalare tempestivamente possibili comportamenti illeciti o irregolarità, il Gruppo AVM garantisce l'anonimato del segnalante, nonché la riservatezza della segnalazione e dei dati ivi contenuti, anche nell'ipotesi in cui la stessa dovesse rivelarsi errata o infondata a seguito delle verifiche effettuate.

L'identità del segnalante non può essere rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni; inoltre, il divieto di rivelare l'identità del whistleblower è da riferirsi non solo al nominativo del segnalante ma anche a tutti gli elementi della segnalazione, dai quali si possa ricavare, anche indirettamente, l'identificazione del segnalante.

È tutelata anche l'identità delle persone coinvolte e delle persone menzionate nella segnalazione.

Protezione delle ritorsioni

All'interno del Gruppo AVM vige il divieto di ritorsione intesa come qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'Autorità Giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto.

Il Gruppo AVM, inoltre, si riserva il diritto di adottare le opportune azioni contro chiunque ponga in essere, o minacci di porre in essere, atti di ritorsione contro coloro che abbiano presentato segnalazioni in conformità alla presente procedura, fatto salvo il diritto degli aventi causa di tutelarsi legalmente qualora siano state riscontrate in capo al segnalante responsabilità di natura penale o civile legate alla falsità di quanto dichiarato o riportato.

--	--

È previsto il divieto di ritorsione anche nei confronti delle persone diverse dal segnalante suesposte (ad es. persone che sono legate al segnalante da uno stabile legame affettivo o di parentela entro il quarto grado).

Limitazione delle responsabilità

È prevista una specifica limitazione di responsabilità per il segnalante rispetto alla rivelazione e alla diffusione di alcune categorie di informazioni. Si tratta nello specifico di limitazioni che operano al ricorrere di determinate condizioni in assenza delle quali vi sarebbero conseguenze in termini di responsabilità penale, civile, amministrativa.

La limitazione di responsabilità per chi segnala, denuncia o effettua divulgazioni pubbliche, opera esclusivamente nei casi in cui:

- al momento della rivelazione o diffusione vi siano fondati motivi per ritenere che le informazioni siano necessarie per far scoprire la violazione. Il segnalante, pertanto, deve ragionevolmente ritenere, e non in base a semplici illazioni, che quelle informazioni debbano svelarsi perché indispensabili per far emergere la violazione;
- la segnalazione, la divulgazione pubblica o la denuncia sia stata effettuata nel rispetto delle condizioni previste dal D.Lgs. n. 24/2023 per beneficiare delle tutele (fondato motivo di ritenere che le informazioni sulle violazioni fossero vere e rientrassero tra le violazioni segnalabili ai sensi del d.lgs. n. 24/2023; segnalazioni, interne ed esterne, divulgazioni pubbliche effettuate nel rispetto delle modalità e delle condizioni previste dalla normativa, ecc.).

Misure di sostegno

Le misure di sostegno consistono in informazioni, assistenza e consulenze a titolo gratuito sulle modalità di segnalazione e sulla protezione dalle ritorsioni offerta dalle disposizioni normative nazionali e da quelle dell'Unione europea, sui diritti della persona coinvolta, nonché sulle modalità e condizioni di accesso al patrocinio a spese dello Stato.

Nello specifico, è pubblicato sul sito dell'A.N.A.C. l'elenco degli enti del Terzo settore che forniscono alle persone segnalanti misure di sostegno.

8.4 SANZIONI

Ai sensi dell'art. 21 del D.Lgs. 24/2023, ANAC applica al responsabile le seguenti sanzioni amministrative pecuniarie:

- a) da 10.000 a 50.000 euro quando accerta che sono state commesse ritorsioni o quando accerta che la segnalazione è stata ostacolata o che si è tentato di ostacolarla o che è stato violato l'obbligo di riservatezza di cui all'articolo 12;
- b) da 10.000 a 50.000 euro quando accerta che non sono stati istituiti canali di segnalazione, che non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni ovvero che l'adozione di tali procedure non è conforme a quelle di cui agli articoli 4 e 5, nonché quando accerta che non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute;

--	--

- c) da 500 a 2.500 euro, nel caso di cui all'articolo 16, comma 3, salvo che la persona segnalante sia stata condannata, anche in primo grado, per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'Autorità Giudiziaria o contabile.

In aggiunta all'irrogazione delle sanzioni amministrative pecuniarie di competenza dell'ANAC, il Gruppo AVM prevede l'irrogazione di sanzioni disciplinari nelle seguenti ipotesi:

- per coloro che accerta essere responsabili degli illeciti di cui al comma 1 del D.Lgs 24/2023;
- per coloro che hanno commesso ritorsioni, hanno ostacolato la segnalazione o hanno tentato di ostacolarla, hanno violato l'obbligo di riservatezza;
- qualora non siano stati istituiti canali di segnalazione, non siano state adottate procedure per l'effettuazione e la gestione delle segnalazioni (o tali procedure non sono conformi a quanto indicato dagli articoli 4 e 5 del D.Lgs. 24/2023), quando non è stata svolta attività di verifica e analisi della segnalazione ricevuta;
- a seguito di una segnalazione, nel caso di responsabilità penale per i reati di diffamazione o calunnia, ovvero responsabilità civile per aver riferito informazioni false riportate intenzionalmente, nei casi di dolo o colpa grave.

Le sanzioni previste dal CCNL di riferimento irrogabili dal Gruppo AVM saranno differenti in relazione alla qualifica del soggetto che ha commesso la violazione, nel rispetto del principio di gradualità della sanzione e di proporzionalità alla gravità dell'infrazione.

Per una trattazione esaustiva delle sanzioni in materia whistleblowing si rimanda al "Regolamento disciplinare" del Gruppo AVM.

9 DISPOSIZIONI FINALI

La presente procedura costituisce presidio del sistema di controllo interno di compliance aziendale e come tale risulta parte integrante del "Modello di Organizzazione, Gestione e controllo (cd MOG 231)" delle singole società del gruppo AVM, risultandone soggetta al relativo sistema sanzionatorio.

Eventuali segnalazioni di illeciti, di irregolarità e di condotte corruttive collegate, riguardanti comportamenti, atti o omissioni che ledono l'interesse pubblico o l'integrità dell'operato del gruppo AVM possono essere attivate in forma anonima nei confronti del Responsabile della Prevenzione, Corruzione e Trasparenza, tramite il sistema di segnalazione Whistleblowing, accessibile dall'intranet e dai siti internet aziendali.

L'attività di vigilanza sul sistema procedurale, finalizzata ad una valutazione d'adequatezza e tenuta del sistema di controllo interno dei MOG 231, è in capo agli Organismi di Vigilanza delle singole società del gruppo, cui vanno inviate segnalazioni relative all'aggiornamento, violazioni e deroghe alle singole procedure.

--	--

10 CRONOLOGIA DELLE VARIAZIONI

Mittente	Descrizione	Codice Documento	Versione	Approvazione
SEPCO	Prima emissione	PS/078	0	18/01/2018
SEPCO	Aggiornamento normativo	PS/078	1	10/02/2021
SEPCO	Aggiornamento normativo	PC_SEPCO_001_SEPCO	2	13/07/2023