



ATTO ORGANIZZATIVO PER LA TUTELA DEL DIPENDENTE CHE SEGNALA ILLECITI

1. OGGETTO E DEFINIZIONI
2. IL SOGGETTO CHE INVIA LE SEGNALAZIONI
3. OGGETTO DELLA SEGNALAZIONE
4. REQUISITI ESSENZIALI DELLE SEGNALAZIONI
5. MODALITÀ DI INVIO DELLE SEGNALAZIONI
6. MODALITÀ DI GESTIONE DELLE SEGNALAZIONI
7. LA TUTELA DEL WHISTLEBLOWER
8. SANZIONI
9. MONITORAGGIO
10. TRATTAMENTO DATI PERSONALI



1. OGGETTO E DEFINIZIONI

1. Con il presente atto si intende individuare una procedura per la gestione delle segnalazioni di illeciti da parte dell'Autorità di Sistema Portuale del Mar Tirreno Settentrionale ai sensi e per gli effetti di cui all'articolo 54 *bis* del d.lgs. 165/01, come successivamente modificato e integrato, mediante un modello gestionale informatizzato *ad hoc*.

2. Ai fini del presente atto organizzativo si intende per:

- **AdSP:** Autorità di Sistema Portuale del Mar Tirreno Settentrionale;
- **ANAC:** Autorità Nazionale Anticorruzione;
- **D.lgs. 165/01:** decreto legislativo 30 marzo 2001, n. 165, come successivamente integrato e modificato, recante *"Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche"*
- **Art. 54-bis:** art. 54 *bis* del decreto legislativo 30 marzo 2001, n. 165, rubricato *"Tutela del dipendente pubblico che segnala illeciti"*;
- **Whistleblower:** il dipendente AdSP, il collaboratore o i dipendenti delle imprese fornitrici di beni, servizi e opere in favore dell'AdSP, che, in ragione del proprio rapporto di lavoro, segnala agli organi legittimati ad intervenire condotte illecite commesse ai danni dell'interesse pubblico;
- **Piattaforma:** lo strumento informatico SEGNALAZIONI.NET per l'invio e la gestione delle segnalazioni in conformità al dettato normativo;
- **RPCT:** Responsabile della prevenzione della corruzione e della trasparenza dell'AdSP;
- **Custode dell'identità digitale:** utente speciale destinato a custodire l'identità fornita;
- **UPD:** Ufficio procedimenti disciplinari;
- **Segnalazione:** segnalazione di illeciti di cui all'articolo 3.

2. IL SOGGETTO CHE INVIA LE SEGNALAZIONI

1. Possono inviare le segnalazioni i dipendenti dell'AdSP sia con contratto di lavoro a tempo indeterminato che con contratto di lavoro a tempo determinato, sia i lavoratori con contratto di somministrazione di lavoro.



2. Sono altresì soggetti legittimati all'invio delle segnalazioni i dipendenti delle imprese fornitrici di beni, servizi e opere in favore dell'AdSP.

3. Le tutele previste dall'art. 54 *bis* si applicano esclusivamente ai soggetti di cui a precedenti commi 1 e 2.

4. Le segnalazioni anonime e quelle eventualmente pervenute da soggetti estranei all'AdSP¹, potranno essere oggetto di valutazione solo se adeguatamente circostanziate e rese con dovizia di particolari tali da far emergere fatti e situazioni in relazione a contesti determinati.

3. OGGETTO DELLA SEGNALAZIONE

1. La segnalazione delle condotte illecite deve essere effettuata sulla base del principio di buona fede e nell'interesse dell'integrità dell'AdSP e deve riguardare fatti e/o notizie acquisite in occasione e/o a causa dello svolgimento delle mansioni lavorative, seppure in modo casuale.

2. La segnalazione non deve essere fondata su meri sospetti "o voci di corridoio" e non deve avere riguardo a doglianze di carattere personale del whistleblower o rivendicazioni/istanze che rientrano nella disciplina del rapporto di lavoro, o rapporti col superiore gerarchico o colleghi.

3. Sono oggetto di segnalazione tutte le condotte in cui si riscontri un abuso da parte di un soggetto del potere a lui affidato, in particolare:

- le presunte condotte illecite che configurano ipotesi di reato contro la Pubblica Amministrazione di cui al Titolo II, Capo I del Codice penale (in particolare ipotesi di corruzione per l'esercizio della funzione, corruzione per atto contrario ai doveri d'ufficio e corruzione in atti giudiziari, disciplinate rispettivamente agli artt. 318, 319 e 319-ter del predetto Codice);
- le presunte condotte poste in essere in violazione di qualsiasi disposizione adottata dall'AdSP nell'esercizio delle proprie funzioni (es. regolamenti, codice di condotta, ecc.);
- le presunte condotte illecite che possono avere riflessi sulla attività amministrativa, a prescindere dalla rilevanza penale, e pertanto pongono in evidenza un mal funzionamento dell'AdSP;

¹ Non riconducibili alle categorie di cui all'articolo 2, commi 1 e 2.



- le condotte che possono arrecare un pregiudizio patrimoniale o un pregiudizio all'immagine dell'AdSP.

4. La segnalazione inviata al RPCT o all'ANAC, non sostituisce, laddove ne ricorrano i presupposti, quella all'Autorità Giudiziaria.

5. Restano ferme le disposizioni in materia di responsabilità penale e disciplinare a carico del *whistleblower* per le ipotesi di segnalazione calunniosa o diffamatoria ai sensi del Codice penale e dell'articolo 2043 del Codice Civile.

4. REQUISITI ESSENZIALI DELLE SEGNALAZIONI

1. Le segnalazioni saranno oggetto di valutazione esclusivamente nel caso in cui siano adeguatamente circostanziate e complete degli elementi ritenuti essenziali quali: l'identità del *whistleblower*, la sua qualifica, il periodo temporale in cui si è verificato il fatto, la descrizione dei fatti.

2. Non saranno oggetto di valutazione le segnalazioni in cui i fatti siano descritti in modo generico tale da non consentire la comprensione dei fatti segnalati, o corredate da documentazione non appropriata o inconferente, ovvero prive degli elementi essenziali sopra elencati.

3. La segnalazione avente ad oggetto presunte condotte illecite imputabili al RPCT deve essere inviata ad ANAC secondo le modalità da questa stabilite.

5. MODALITÀ DI INVIO DELLE SEGNALAZIONI

1. Le segnalazioni possono essere inviate a mezzo dell'apposita piattaforma disponibile all'indirizzo <https://portialtotirreno.segnalazioni.net>.

2. Il *whistleblower* deve necessariamente compilare i campi obbligatori² del *form* per poter inviare la segnalazione.

3. La piattaforma provvede alla cifratura e alla memorizzazione della segnalazione separando il contenuto dall'identità del *whistleblower* e inviandole rispettivamente al RPCT e al Custode dell'identità digitale.

4. Nel caso in cui il *whistleblower* abbia inviato la segnalazione come "utente non registrato", è tenuto a conservare il *codice della segnalazione* e la password rilasciati al termine della

² Contrassegnati dall'asterisco rosso.



procedura di invio di ogni segnalazione, in quanto indispensabili per i successivi accessi al fine di verificare lo stato di avanzamento della segnalazione e/o inserire ulteriore documentazione³.

5. Nel caso in cui il *whistleblower* sia un soggetto registrato, ovvero, sebbene non registrato fornisca comunque, compilando gli appositi campi della piattaforma, i propri dati identificativi a completezza della segnalazioni, la piattaforma provvede alla cifratura dell'identità nei modi di cui al comma 3.

6. Nei casi di cui al comma 5 il custode dell'identità digitale può consentire la visibilità dei dati identificativi al RPCT esclusivamente a seguito di sua istanza formale adeguatamente motivata ovvero nei casi previsti dalla Legge, senza in ogni caso poter che il custode medesimo possa visualizzare i dati in parola.

7. Le segnalazioni inviate in forma anonima in prima istanza, potranno essere successivamente integrate con le generalità del segnalante ai fini di acquisire l'eventuale tutela legale.

6. MODALITÀ DI GESTIONE DELLE SEGNALAZIONI

1. Il RPCT è il soggetto destinatario delle segnalazioni ed è tenuto alla gestione delle stesse, ivi compresa la verifica della fondatezza nel rispetto dei principi di imparzialità e riservatezza.

2. Il RPCT svolge le attività previste con il supporto del personale addetto al Servizio Anticorruzione e Trasparenza dell'AdSP.

3. Entro 5 giorni dalla ricezione della segnalazione, il RPCT comunica al *whistleblower* la presa in carico della stessa e procede ad un esame preliminare in ordine alla sussistenza dei requisiti essenziali.

4. Qualora la segnalazione risulti ammissibile, il RPCT comunica al *whistleblower* l'avvio dell'istruttoria entro e non oltre 15 giorni dalla presa in carico di cui al precedente comma 3.

5. Nella fase istruttoria il RPCT può richiedere chiarimenti allo stesso *whistleblower* e/o ad altri soggetti coinvolti eventualmente dalla segnalazione adottando le eventuali necessarie cautele al fine di tutelare la riservatezza del *whistleblower* e degli eventuali altri soggetti segnalati.

³ Nel caso in cui il whistleblower, quale utente non registrato, smarrisca la password non potrà più accedere alla segnalazione.



6. Nel caso in cui all'esito dell'istruttoria la segnalazione risulti fondata, in tutto o in parte, il RPCT provvederà, in relazione alla natura della violazione:

- a comunicare l'esito dell'accertamento al Dirigente Responsabile del Settore di appartenenza dell'autore della violazione accertata affinché adottati i provvedimenti di competenza, incluso, sussistendone i presupposti, l'esercizio dell'azione disciplinare, purché la competenza, per la gravità dei fatti, non spetti direttamente all'UPD, che in tal caso provvederà direttamente;
- a presentare segnalazione all'Autorità Giudiziaria competente e/o alla Corte dei conti e/o all'ANAC in quanto e per quanto ne sussistano i presupposti di legge;
- ad adottare o a proporre di adottare, se la competenza è di altri soggetti o organi, tutti i necessari provvedimenti amministrativi per il pieno ripristino della legalità.

7. Il RPCT comunica al *whistleblower*, entro 60 giorni dell'avvio dell'istruttoria, le risultanze della istruttoria e gli eventuali atti e attività al riguardo intraprese.

7. LA TUTELA DEL WHISTLEBLOWER

1. L'identità del *whistleblower* è protetta in ogni contesto, a partire dal momento dell'invio della segnalazione.

2. Coloro che ricevono la segnalazione, o sono coinvolti nella relativa gestione, anche solo accidentalmente, sono tenuti a tutelare la riservatezza delle correlate informazioni. La violazione dell'obbligo di riservatezza è comunque fonte di responsabilità disciplinare, fatte salve ulteriori forme di responsabilità previste dall'ordinamento.

3. La tutela del *whistleblower* non trova applicazione nei casi espressamente previsti per legge.

4. Salvo quanto previsto al successivo comma 5, l'identità del *whistleblower* non è mai rivelata nell'ambito di un procedimento disciplinare attivato in relazione e/o in seguito della segnalazione.

5. Qualora la contestazione dell'addebito disciplinare risulti fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del *whistleblower* risulti assolutamente indispensabile alla difesa del segnalato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso del *whistleblower*.



6. La segnalazione, come previsto dall'art. 54 bis, comma 4, del d.lgs. 30 marzo 2001, n. 165, è sottratta:

- all'accesso come istituto disciplinato dagli articoli 22 e seguenti della Legge 7 agosto 1990, n. 241;
- all'accesso civico generalizzato disciplinato dall'articolo 5 del d.lgs. 14 marzo 2013, n. 33.

8. SANZIONI

1. Per quanto non espressamente previsto dal presente atto organizzativo si rimanda al Codice di comportamento dell'AdSP allegato al Piano triennale anticorruzione e trasparenza 2018 – 2020, nonché alla contrattazione di lavoro di riferimento.

9. MONITORAGGIO

1. Il RPCT monitora le segnalazioni pervenute con cadenza annuale, al fine di evidenziare:
 - il numero complessivo di segnalazioni pervenute;
 - la distinzione tra quelle archiviate, quelle per le quali l'istruttoria si è conclusa e quelle in corso.
2. I dati numerici di sintesi vengono riportati nella relazione annuale di monitoraggio prevista dal Piano Triennale della Prevenzione alla Corruzione adotta dall'AdSP.
3. Le segnalazioni e la correlata documentazione di supporto sono conservati per un periodo di cinque anni.

10. TRATTAMENTO DATI PERSONALI

1. Il trattamento dei dati personali conferiti all'AdSP MTS nell'ambito delle attività disciplinate dal presente Regolamento avviene in conformità alle disposizioni di cui decreto legislativo 30 giugno 2003, n. 196, come modificato dal decreto legislativo 10 agosto 2018, n. 101 e del Regolamento UE 2016/679 denominato General Data Protection Regulation (GDPR) e unicamente per le finalità oggetto del presente Regolamento.