Regione Calabria

Responsabile della Prevenzione della Corruzione e della Trasparenza della Giunta Regionale

Prot 79238 del 20.02.2023

Ai Dirigenti Generali dei Dipartimenti
della Giunta Regionale e Strutture Equiparate
Ai Dirigenti Referenti PCT
A tutto il personale a mezzo AD Globale

Oggetto: circolare sull'utilizzo del software per le segnalazioni degli illeciti "*whistleblowing"*

Gent.mi,

con le precedenti circolari n. 346917 del 03.08.2021 e n. 168530 del 20.5.2020, questo RPCT ha diramato le indicazioni utili ad effettuare le segnalazioni di un illecito di interesse generale di cui si è venuti conoscenza nell'ambito dell'amministrazione pubblica, il "*whistleblowing"*.

Il cd. "*whistleblowing"* è uno strumento fondamentale per la lotta alla corruzione, introdotto in Italia nel 2014, purtroppo ancora visto con troppo sospetto, ma che consente, invece, di rimediare al malfunzionamento delle pubbliche amministrazioni, partecipando attivamente tramite la segnalazione di illeciti, irregolarità o illegalità di cui si è venuti a conoscenza durante il rapporto di lavoro, in virtù dell'ufficio rivestito, oppure durante lo svolgimento delle proprie mansioni lavorative all'interno della amministrazione pubblica.

Al malfunzionamento delle amministrazioni pubbliche si può rimediare, e il "*whistleblowing*" può essere un utile alleato: adottare un sistema di *whistleblowing* significa rafforzare il proprio sistema di controllo interno e avere la possibilità di scoprire eventuali frodi e criticità prima che diano luogo a più gravi danni e/o responsabilità.

Come è noto, la Regione Calabria, al fine di rendere esecutive le prescrizioni normative in materia, si è dotata di un software, ad oggi perfettamente funzionante e regolarmente implementato, che puo' essere utilizzato, al bisogno, dal dipendente *whistleblower* per effettuare le segnalazioni di cui sopra.

Ad oggi, tuttavia, lo strumento informatico, dotato di alte potenzialità, risulta, purtroppo, poco utilizzato.

Con la presente circolare, pertanto, si vogliono fornire ulteriori indicazioni sulle modalità operative dello strumento dedicato alla segnalazione degli illeciti, e, facendo seguito alle precedenti comunicazioni in materia di *whistleblowing* a firma della scrivente, si sollecita nelle SS.LL. un'azione di sensibilizzazione rispetto alle iscrizioni dei propri dipendenti e collaboratori al software in uso presso la Regione Calabria.

Si ricorda che è possibile l'iscrizione non solo di tutti i dipendenti, ma anche di collaboratori e consulenti, titolari di incarichi negli uffici di diretta collaborazione delle autorità politiche, collaboratori di imprese fornitrici di beni e servizi.

La presente circolare sarà oggetto di aggiornamento non appena sarà effettivo il D.Lgs. sull'attuazione della Direttiva Ue 2019/1937 del Parlamento Europeo e del Consiglio 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, il cui schema è stato approvato in esame preliminare il 9 dicembre 2022.

CIRCOLARE SUL FUNZIONAMENTO DEL SOFTWARE INFORMATICO "*WHISTLEBLOWING*" E SUL COMPORTAMENTO DEL DIPENDENTE, CONSULENTE O COLLABORATORE CHE SEGNALA L'ILLECITO "*WHISTLEBLOWER*"

Quale utile strumento di prevenzione della corruzione, ed ai sensi dell'art. 54 bis del D.lgs. n.165/2001, per come modificato dalla L. n. 179/2017, il dipendente, consulente o collaboratore dell'amministrazione regionale, fermo restando l'obbligo di denuncia alla autorità giudiziaria, può utilizzare il software per segnalare eventuali situazioni di illecito nell'amministrazione di cui sia venuto a conoscenza per ragioni di ufficio (*whistleblowing*).

La segnalazione è effettuata al Responsabile per la Prevenzione della Corruzione e della Trasparenza attraverso il software dedicato, che garantisce la riservatezza della identità del segnalante e del contenuto della segnalazione mediante un sistema di crittografia.

In via preliminare, occorre, quindi, sollecitare l'iscrizione al software di tutti i dipendenti, consulenti e collaboratori: si ribadisce che l'iscrizione non vincola l'effettuazione di nessuna segnalazione, ma la agevola nel caso in cui sia necessaria e consente di familiarizzare con il sistema informatico nel caso in cui il *whistleblower* debba effettuare la segnalazione.

L'iscrizione alla piattaforma è, altresì, indispensabile per tutelare il dipendente che decida di effettuare una segnalazione in quanto l'iscrizione permette la creazione di una "banca dati" dei dipendenti e degli altri soggetti tutelati, per essere sicuri che a chi utilizzerà il servizio saranno garantite le tutele previste dall'art. 54-bis del D.Lgs. 165/2001. Infatti, ove uno dei soggetti abilitati dovesse inviare una segnalazione, i suoi dati identificativi saranno separati dalla segnalazione e mantenuti riservati dal software.

Più è alto il numero di iscritti alla Banca Dati, maggiore sarà la riservatezza garantita ad un futuro segnalante.

Il software è facilmente accessibile e utilizzabile; assicura la ricezione confidenziale di ogni segnalazione; garantisce il monitoraggio e la gestione delle segnalazioni; permette la creazione della reportistica necessaria alle funzioni e agli organi preposti; fornisce visibilità in tempo reale sulle segnalazioni, sui provvedimenti e sulle azioni correttive.

A seguito dell'iscrizione, il *whistleblower* segnala al RPCT la situazione irregolare: l'unico soggetto che può ricevere le segnalazioni di *whistleblowing*, con le connesse garanzie di protezione del segnalante, è il RPCT. Nel caso di segnalazioni destinate unicamente al superiore gerarchico, il segnalante non sarà tutelato ai sensi dell'art. 54-bis. I dati del segnalante restano sconosciuti con il solo limite dei casi previsti dalla legge.

Dopo la segnalazione, il RPCT si fa carico, grazie alla segnalazione, di fronteggiare il rischio che quella situazione possa ripetersi in futuro, intervenendo dunque affinché l'amministrazione interessata adotti le giuste misure per prevenire la corruzione. La tutela della riservatezza si estende - oltre che all'identità del segnalante, al contenuto della segnalazione, della documentazione ad essa allegata e degli atti formati nel corso dell'attività istruttoria - anche all'identità del segnalato.

Quando il *whistleblower* perfeziona l'iscrizione, l'amministratore (il RPCT) riceve la richiesta di registrazione, verifica in maniera riservata che si è effettivamente un dipendente o uno dei soggetti tutelati, e consente l'abilitazione al sistema.

Questa preventiva verifica è necessaria poiché essendo il software raggiungibile online dal sito istituzionale, chiunque potrebbe registrarsi ed effettuare una

segnalazione, senza però avere il diritto di farla e di essere, di conseguenza, tutelato. Fino alla verifica da parte dell'amministratore, non si potrà, pertanto, effettuare alcuna segnalazione.

Si rammenta brevemente la differenza tra la segnalazione anonima e quella riservata: la segnalazione anonima proviene da un soggetto qualsiasi, non identificato e non identificabile perché non ha mai comunicato i suoi dati ed a cui non è possibile garantire tutela; la segnalazione riservata, invece, proviene da un soggetto che ha fornito i suoi dati, consentendo di ricomprenderlo tra i soggetti abilitati e, dunque, tra i soggetti da tutelare. L'identità del segnalante va, poi, mantenuta riservata dal RPCT che non deve rivelare a nessuno (tranne nei casi previsti dalla legge) il nome del *whistleblower,* anche al fine di evitare l'applicazione di misure ritorsive nei suoi confronti.

Terminata la procedura di registrazione ed ottenuta l'abilitazione, ove uno dei soggetti abilitati dovesse inviare una segnalazione, i suoi dati identificativi saranno separati dalla segnalazione e mantenuti riservati dal software.

Infatti, l'unico abilitato a ricevere la segnalazione è l'amministratore ovvero l' RPCT: questi, appena riceverà la segnalazione, vedrà i dati del segnalante oscurati, mentre potrà leggere solo il contenuto della segnalazione.

La segnalazione dovrà essere gestita solo in base agli elementi contenuti nella stessa senza conoscere i dati personali del segnalante.

Il RPCT dovrà gestirla e avviare le procedure necessarie: non saprà, quindi, chi, tra tutti i registrati alla piattaforma, ha inviato la segnalazione. Per questo, si ribadisce, più è alto il numero delle registrazioni, maggiori saranno le garanzie di riservatezza.

Si sottolinea, in ogni caso, che è necessario utilizzare questo strumento in maniera corretta: le segnalazioni devono avvenire nell'interesse dell'integrità della pubblica amministrazione, non devono riguardare questioni personali né condotte illecite che prevedono già altri tipi di tutela (es.: violazione delle norme sulla sicurezza nei luoghi di lavoro, violazione della disciplina sulla privacy, mancata pubblicazione dei dati su "Amministrazione trasparente"), ma devono riguardare delitti contro la PA (ossia le ipotesi di corruzione per l'esercizio della funzione, corruzione per atto contrario ai doveri d'ufficio e corruzione in atti giudiziari) oppure situazioni di abuso di potere al fine di ottenere vantaggi privati o situazioni che comportino un mal funzionamento dell'amministrazione (sprechi, nepotismo, ripetuto mancato rispetto dei tempi procedimentali, irregolarità contabili, false dichiarazioni). Sono escluse le informazioni acquisite in violazione di legge.

I fatti illeciti oggetto delle segnalazioni '*whistleblowing*' comprendono non solo le fattispecie riconducibili all'elemento oggettivo dell'intera gamma dei delitti contro la pubblica amministrazione (di cui al Libro II, Titolo II, Capo I, del codice penale) ma anche tutte le situazioni in cui, nel corso dell'attività amministrativa, si riscontrino comportamenti impropri di un funzionario pubblico che, anche al fine di curare un interesse proprio o di terzi, assuma o concorra all'adozione di una decisione che devia dalla cura imparziale dell'interesse pubblico. Ciò a condizione che si possa configurare un illecito. Non è necessario che il dipendente sia certo dell'effettivo accadimento dei fatti denunciati e/o dell'identità dell'autore degli stessi: è sufficiente che il dipendente, in base alle proprie conoscenze, ritenga ragionevolmente che un fatto illecito si sia verificato. Non sono invece meritevoli di tutela le segnalazioni fondate su meri sospetti, voci, o contenenti informazioni che il segnalante sa essere false.

Nelle ipotesi in cui le segnalazioni di cui all'art. 54-bis siano connotate da un interesse personale del segnalante che concorre con quello generale alla salvaguardia

dell'integrità della pubblica amministrazione, la presenza di detto interesse personale privato concorrente deve essere dichiarato dal segnalante al RPCT.

Non possono generalmente essere considerate segnalazioni di *whistleblowers* quelle prive dell'interesse generale all'integrità della pubblica amministrazione, quali, ad esempio, lamentele di carattere personale del segnalante come contestazioni, rivendicazioni o richieste che attengono alla disciplina del rapporto di lavoro o ai rapporti con superiori gerarchici o colleghi che rilevano la mera presenza di un interesse personale del segnalante.

Elementi costituitivi della segnalazione sono:

- le circostanze di tempo e di luogo in cui si è verificato il fatto antigiuridico oggetto della segnalazione;
- la descrizione del medesimo fatto;
- la generalità degli autori della condotta illecita o, comunque, altre indicazioni che consentano di identificare il soggetto cui attribuire i fatti segnalati;
- l'allegazione di documentazione a corredo che possa fornire elementi di fondatezza dei fatti oggetto di segnalazione

Con riguardo alla tutela relativa alla identità del segnalante, vige il divieto di rivelare l'identità del segnalante l'illecito oltre che nel procedimento disciplinare, anche in quello penale e contabile:

- nel procedimento penale, la segretezza dell'identità del denunciante è coperta in relazione e nei limiti del principio di segretezza degli atti d'indagine di cui all'articolo 329 c.p.p.;
- nel processo contabile, l'identità non può essere rivelata fino alla fine della fase istruttoria;
- nel procedimento disciplinare l'identità del segnalante non può essere rivelata senza il suo consenso (sempre che la contestazione disciplinare sia basata su elementi diversi da quelli su cui si basa la segnalazione). Tuttavia, se la contestazione disciplinare è fondata, anche solo parzialmente, sulla segnalazione, l'identità può essere rivelata dietro consenso del segnalante, diversamente rimanendo inutilizzabile la segnalazione ai fini del procedimento disciplinare (comma 3).

La procedura di gestione delle segnalazioni di *whistleblowing* effettuate direttamente al RPCT segue le modalità indicate nel manuale operativo già noto e che si riallega alla presente circolare e si articola, sostanzialmente, in una attività "di verifica e di analisi" della segnalazione da parte del RPCT cui segue l'adozione dei seguenti, alternativi, provvedimenti: archiviazione, adeguatamente motivata, in caso di manifesta infondatezza della segnalazione; istruttoria della segnalazione, se fondata.

Nel rappresentare nuovamente la necessità di avere un numero più alto possibile di iscrizioni al fine di garantire la riservatezza del segnalante, sono certa che le SSLL saranno sensibili e attenti rispetto al nuovo sollecito.

Alla presente si riallega il manuale operativo per l'iscrizione al software in materia di whistleblowing.

Cordiali saluti.

Il RPCT
Avv. Ersilia Amatruda