

Regolamento
per la gestione delle
informazioni documentate,
delle registrazioni e del
sistema informativo
Allegato 4
Sistema di Whistleblowing

Sommario

0 - Premessa	3
1 – Scheda di sintesi	4
2 – Informativa (disposizioni per utenti e gestori)	5
2.1 – Soggetti legittimati ad effettuare le segnalazioni (ambito soggettivo)	5
2.2 – Soggetti che godono delle misure di protezione	5
2.3 – Le violazioni che possono essere segnalate (Ambito Oggettivo)	6
2.4 – Presupposti per l’effettuazione delle segnalazioni interne o esterne	6
2.5 – Canale di segnalazione ed istruzioni sul suo funzionamento	7
2.6 – Gestione della segnalazione	7
2.6.1 – I soggetti destinatari delle segnalazioni	7
2.6.2 – Ricezione della segnalazione	8
2.6.3 – La procedibilità della segnalazione	8
2.6.4 – L’ammissibilità della segnalazione	8
2.6.5 – Istruttoria ed accertamento della segnalazione	8
2.6.6 – Riscontro al segnalante	9
2.7 – Tutele riconosciute al segnalante	9
2.7.1 – La riservatezza dell’identità del segnalante	10
2.7.2 – Il Divieto e la protezione contro le ritorsioni	10
2.7.3 – Le limitazioni della responsabilità del segnalante	11
2.8 – Sistema sanzionatorio	12
2.9 – Segnalazione esterna e divulgazione pubblica	12
2.10 – Trattamento dei dati personali	13
2.11 – Modalità comunicazione e diffusione	14

0 - Premessa

Il presente regolamento intende fornire una informativa completa e una guida operativa a disposizione del segnalante in ordine alla disciplina normativa di cui al D. Lgs. 10 marzo 2023, che ha recepito nell'ordinamento nazionale la Direttiva UE 2019/1937 riguardante "la protezione delle persone che segnalano violazione del diritto dell'Unione" (cd. WHISTLEBLOWING), all'utilizzo del canale messo a disposizione dalla Moba Eurotubi Srl, alle procedure ed ai presupposti per l'inoltro di segnalazioni interne o esterne, in adempimento degli obblighi previsti dalla normativa suddetta.

Di seguito sono riportate:

una prima parte denominata SCHEDA DI SINTESI di come e con quale sistema informatico la Moba Eurotubi S.r.l. ha adempiuto alle disposizioni di legge per soddisfare i requisiti di WHISTLEBLOWING

una seconda parte dettagliata con tutte le disposizioni e le informazioni necessarie per una corretta gestione delle segnalazioni di eventuali violazioni del diritto dell'Unione inclusi obblighi e doveri delle parti (segnalante e soggetti destinatari delle segnalazioni)

1 – Scheda di sintesi

La Moba Eurotubi per consentire a tutti i LEGITTIMATI AD EFFETTUARE LE SEGNALAZIONI mette a disposizione accessibile da apposita sezione del proprio sito Web una piattaforma di whistleblowing funzionante come canale digitale sicuro e riservato per segnalare illeciti¹, per consentire al segnalante (*anche in forma anonima*) di inviare dettagli, gestire la comunicazione con il responsabile tramite messaggi criptati, e ricevere aggiornamenti sullo stato della pratica, il tutto garantendo la tutela del segnalante secondo le normative vigenti, con gestione centralizzata e tracciabile da parte dell'ente ricevente.

Come funziona per il segnalante (Utente)

- Accesso sicuro: *Si accede tramite credenziali univoche.*
- Invio segnalazione: *Si compila un form con dettagli, prove e si può allegare materiale; è possibile segnalare anche tramite messaggi vocali o richiedere un incontro orale.*
- Comunicazione protetta: *Si apre una chat sicura e crittografata per dialogare con il gestore, senza rivelare la propria identità se anonimi.*
- Monitoraggio: *Si ricevono notifiche (push o email) e si controlla lo stato della segnalazione (es. "In Corso di Esame", "Richieste Informazioni").*

Come funziona per l'ente (Moba Eurotubi)

- Pannello di controllo: *L'ente gestisce tutto da un pannello centrale, personalizzabile e sicuro.*
- Ricezione e gestione: *Le segnalazioni arrivano e vengono classificate, assegnate e gestite attraverso flussi di lavoro definiti.*
- Valutazione e follow-up: *L'ente può chiedere ulteriori informazioni, valutare la segnalazione e impostare lo stato finale (es. "Fondata", "Infondata").*
- Sicurezza e conformità: *La piattaforma, riconosciuta anche dall'ANAC², assicura privacy e rispetto del GDPR, con dati su cloud sicuro.*

Punti chiave della tecnologia

- Riservatezza: *Crittografia end-to-end e architettura sicura per proteggere i dati; No-log policy ovvero nessuna registrazione degli indirizzi IP o dei metadati dei dispositivi usati per segnalare; Gestione automatizzata dei periodi di conservazione dei dati e cancellazione sicura in conformità al GDPR.*
- Anonimato: *Possibilità di segnalare senza rivelare la propria identità³.*
- Tracciabilità: *Ogni fase della gestione è tracciata, garantendo trasparenza interna.*
- Conformità normativa: *Rispetta le direttive nazionali ed europee sulla tutela dei segnalanti.*
- Canali multipli: *Integra segnalazione scritta, vocale e richiesta di incontro.*

Le fasi principali del funzionamento della piattaforma sono:

1. Accesso e Invio della Segnalazione

Il segnalante accede al portale web nella sezione dedicata. Può scegliere di rimanere anonimo o fornire le proprie generalità; in entrambi i casi, la piattaforma cripta i dati per impedire accessi non autorizzati.

Contenuto: La segnalazione deve includere una descrizione chiara dei fatti e, se noti, gli autori dell'illecito.

La piattaforma, una volta effettuato l'accesso, presenterà al segnalante un modulo informatico con campi preimpostati da compilare con i dati e le informazioni descrittive la segnalazione

2. Gestione e Interazione Sicura

Una volta inviata la segnalazione, il sistema genera un codice identificativo unico.

Ricezione: La piattaforma rilascia un avviso di ricevimento entro 7 giorni.

Dialogo Protetto: Il segnalante può monitorare lo stato della pratica e dialogare con il gestore (es. l'Organismo di Vigilanza o il Responsabile Anticorruzione) tramite una chat protetta, senza rivelare la propria identità reale.

3. Istruttoria e Riscontro

Il gestore valuta l'ammissibilità della segnalazione e avvia le verifiche interne.

Termini di Legge: L'azienda o l'ente pubblico è obbligato a fornire un riscontro finale sull'esito della segnalazione entro 3 mesi dalla data dell'avviso di ricevimento.

¹ In Italia, il funzionamento è regolato dal D.Lgs. 24/2023, che impone standard tecnologici elevati per proteggere l'identità del segnalante

² Autorità Nazionale Anti Corruzione

³ I dati identificativi sono segreti. Le segnalazioni eventualmente presentate in forma anonima sono trattate come segnalazioni ordinarie, non potendo essere equiparate a segnalazioni whistleblowing

2 – Informativa (disposizioni per utenti e gestori)

2.1 – Soggetti legittimati ad effettuare le segnalazioni (ambito soggettivo)

Le segnalazioni, intese come informazioni, compresi i fondati sospetti, su violazioni già commesse o non ancora commesse nonché su condotte volte ad occultarlo, di cui il segnalante sia venuto a conoscenza nell'ambito del contesto lavorativo della Moba Eurotubi.

Rispetto all'accezione da attribuire alla definizione del "contesto lavorativo", sia secondo il Decreto che le Linee Guide elaborate dall'ANAC, occorre fare riferimento ad un perimetro di applicazione ampio e non limitato a chi abbia un rapporto di lavoro in senso stretto con l'azienda.

Le segnalazioni possono essere pertanto effettuate anche da coloro che abbiano in corso con l'azienda altri tipi di rapporti giuridici diversi da quelli di lavoro in senso stretto; quindi, a titolo esemplificativo e non esaustivo l'elenco dei soggetti legittimati a presentare una segnalazione nell'ambito della disciplina del Whistleblowing include:

- lavoratori dipendenti ed autonomi;
- liberi professionisti e consulenti;
- collaboratori;
- volontari e tirocinanti;
- lavoratori e collaboratori che svolgono la propria attività presso soggetti pubblici o privati che forniscono beni o servizi;
- azionisti, intesi come "coloro che siano venuti a conoscenza di violazioni oggetto di segnalazione nell'esercizio di diritti di cui sono titolari in ragione del loro ruolo di azionisti rivestito nell'impresa".
- ai soggetti con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza;

La disciplina si applica anche nel caso di segnalazioni che intervengano nell'ambito di un rapporto di lavoro poi terminato, se le informazioni sono state acquisite durante il suo svolgimento, nonché qualora il rapporto non sia ancora iniziato e le informazioni sulle violazioni siano state acquisite durante la selezione o in altre fasi precontrattuali.

Ciò che rileva pertanto è l'esistenza di una relazione qualificata tra il segnalante e l'azienda nell'ambito della quale il primo opera, relazione che riguarda attività lavorative o professionali presenti o anche passate.

2.2 – Soggetti che godono delle misure di protezione

I soggetti che godono delle misure di protezione previste nell'ambito della disciplina normativa del Whistleblowing sono costituiti dal Segnalante ed ai soggetti ad esso assimilati, tra i quali:

- il facilitatore, ovvero la persona fisica che assiste il segnalante nel processo di segnalazione operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata; qualora il facilitatore, appartenente al medesimo contesto lavorativo, rivesta la qualifica di sindacalista ed assista il lavoratore utilizzando tale sigla non potrà rivestire il ruolo di facilitatore;
- persone del medesimo contesto lavorativo del segnalante, denunciante o di chi effettua una divulgazione pubblica, che sono legate a essi da uno stabile legame affettivo o di parentela entro il quarto grado; Tale espressione potrebbe fare riferimento a "coloro che hanno un rapporto di convivenza con il segnalante; in un'accezione di portata estensiva la nozione di stabile legame affettivo potrà intendersi non solo come convivenza in senso stretto, bensì come rapporto di natura affettiva caratterizzato da una certa stabilità sia sotto il profilo temporale e che sotto il profilo di condivisione di vita, un legame affettivo che coinvolge quindi una persona specifica";
- colleghi di lavoro del segnalante, denunciante o di chi effettua una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo del segnalante e che hanno con detta persona un rapporto abituale e corrente; più precisamente "coloro che al momento della segnalazione lavorano con il segnalante (esclusi quindi gli ex colleghi) e che abbiano con quest'ultimo un rapporto abituale e corrente, non occasionale o sporadico, episodico ed eccezionale, ma protratto nel tempo e connotato da una certa continuità tale da determinare un rapporto di comunanza ed amicizia";
- enti di proprietà in via esclusiva o in compartecipazione maggioritaria di terzi del segnalante, denunciante o di chi effettua una divulgazione pubblica;
- Enti presso i quali il segnalante denunciante o chi effettua una divulgazione pubblica, lavorano;

Per la corretta individuazione di tali soggetti sarebbe opportuno che gli estremi degli stessi fossero integrati dal segnalante nell'ambito del processo di istruttoria della segnalazione, dimostrando la sussistenza dei relativi presupposti.

2.3 – Le violazioni che possono essere segnalate (Ambito Oggettivo)

L'ambito di applicazione della disciplina è articolato e complesso e si poggia su un regime di obblighi e tutele a geometria variabile che muta in base: i) all'oggetto della violazione, ii) alla natura pubblica o privata del soggetto di appartenenza del segnalante; iii) alle dimensioni dell'ente privato ed all'applicabilità allo stesso della disciplina di cui al Decreto 231.

Per quanto riguarda il settore privato, le segnalazioni possono avere ad oggetto violazioni della disciplina nazionale solo con riferimento ai reati previsti dal Decreto 231 o alle violazioni del Modello Organizzativo nonché quelle riguardanti il diritto europeo con riferimento:

- agli illeciti relativi ai seguenti settori: contratti pubblici, servizi, prodotti e mercati finanziari, prevenzione del riciclaggio e del terrorismo, sicurezza e conformità dei prodotti, sicurezza dei trasporti, tutela dell'ambiente, radioprotezione e sicurezza nucleare, sicurezza degli alimenti, 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. A titolo esemplificativo, reati ambientali
- atti ed omissioni che ledono gli interessi finanziari del UE come individuati nei regolamenti, direttive, decisioni raccomandazioni, pareri dell'UE come ad es. frodi, corruzione e qualsiasi altra attività illegale commessa ai danni dell'Unione;
- atti o omissioni legati al mercato interno che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali. Sono ricomprese le violazioni delle norme dell'UE in materia di concorrenza ed aiuti di Stato, di imposte sulle imprese, ed i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto e le finalità della normativa applicabile in materia di imposte sulle imprese;
- atti o comportamenti che vanificano l'oggetto e le finalità delle disposizioni dell'Unione europea nei settori di cui sopra, come ad esempio le pratiche abusive

Sono **escluse dall'ambito di applicazione** della disciplina "Whistleblowing" le segnalazioni:

- legate ad un interesse personale del segnalante che attengono ai propri rapporti individuali di lavoro, ovvero inerenti ai rapporti di lavoro con le figure gerarchicamente sovraordinate (es. vertenze di lavoro, discriminazioni, conflitti interpersonali tra colleghi, segnalazioni su trattamenti dei dati effettuati nel contesto del rapporto individuale di lavoro o in assenza di una lesione dell'interesse pubblico o dell'integrità dell'ente privato). Le segnalazioni delle violazioni NON rientranti nel campo di applicazione della normativa Whistleblowing, ma comunque rilevanti in quanto lesive di principi o prescrizioni richiamate nel Codice Etico adottato dall'azienda o nei regolamenti aziendali interni potranno essere fatte valere attraverso il ricorso diretto ai propri referenti diretti preposti o alle funzioni interne incaricate della responsabilità della gestione e dell'organizzazione del personale.
- in materia di sicurezza e difesa nazionale;
- relative a violazioni già regolamentate in via obbligatoria in alcuni settori speciali alle quali continua ad applicarsi la disciplina della segnalazione ad hoc (servizi finanziari, prevenzione riciclaggio, terrorismo, sicurezza nei trasporti, tutela dell'ambiente).

Fermo restando la normativa in materia di: i) informazioni classificate, ii) segreto medico e forense, iii) segretezza delle deliberazioni degli organi giurisdizionali; iv) norme di procedura penale sull'obbligo di segretezza delle indagini; v) disposizioni sull'autonomia e sull'indipendenza della magistratura; vi) difesa nazionale e di ordine e sicurezza pubblica; vii) esercizio del diritto dei lavoratori di consultare i propri rappresentanti o i sindacati.

2.4 – Presupposti per l'effettuazione delle segnalazioni interne o esterne

Le segnalazioni sono definite come le informazioni, compresi i fondati sospetti, su violazioni già commesse o non ancora commesse ma che alla base di elementi concreti potrebbero esserlo, nonché su condotte volte ad occultarle. Si deve altresì trattare di comportamenti, atti od omissioni, di cui il segnalante sia venuto a conoscenza nell'ambito del contesto lavorativo, inteso secondo un'eccezione più estensiva a tutti coloro che abbiano instaurato con l'azienda un rapporto giuridico diverso da quello del lavoro in senso stretto, come ad. Collaboratori, consulenti, tirocinanti, azionisti, ed alle persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza.

Quanto al contenuto le segnalazioni devono essere circostanziate al fine di consentire a valutazione dei fatti da parte dei soggetti competenti a ricevere e gestire le segnalazioni:

In particolare, è necessario che risultino chiari i seguenti elementi essenziali della segnalazione, anche ai fini de vaglio della sua ammissibilità:

- i dati identificativi della persona segnalante, nonché un recapito a cui comunicare i successivi aggiornamenti;

- le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione quindi una descrizione dei fatti, specificando i dettagli relativi alle notizie circostanziali e ove presenti anche le modalità con cui si è venuti a conoscenza dei fatti oggetto della segnalazione;
- le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati.

E' utile anche che alla segnalazione vengano allegati documenti che possano fornire elementi di fondatezza dei fatti oggetto di segnalazione nonché le indicazioni di altri soggetti potenzialmente a conoscenza dei fatti.

2.5 – Canale di segnalazione ed istruzioni sul suo funzionamento

Fermo restando la possibilità di effettuare denunce all'Autorità Giudiziaria e contabile nei casi di loro competenza, per l'effettuazione della segnalazione il soggetto segnalante potrà fare ricorso ai seguenti canali:

- 1) canale interno;
- 2) canale esterno;
- 3) divulgazione pubblica

I canali di segnalazione interni è idoneo ad assicurare la riservatezza circa l'identità del segnalante e delle persone coinvolte, compreso il cd facilitare, del contenuto della segnalazione e della documentazione ad essa relativa.

Per quanto attiene agli strumenti con cui attivare il canale di segnalazione interno, la normativa prevede che le segnalazioni possano essere effettuate con differenti modalità:

- in forma SCRITTA anche mediante modalità informatica;
- in forma ORALE attraverso appositi servizi vocali di messaggistica vocale, fruibili attraverso la piattaforma;

Per il proprio sistema di whistleblowing Moba Eurotubi ha deciso di ricorrere alla piattaforma informatica on line, riconosciuta anche dall'ANAC quale strumento informatico adeguato a garantire la riservatezza, a differenza degli strumenti costituiti dalla posta elettronica ordinaria e PEC che non assicurano standard di sicurezza adeguati.

2.6 – Gestione della segnalazione

2.6.1 – I soggetti destinatari delle segnalazioni

La figura responsabile della ricezione e della gestione della segnalazione viene individuata all'interno dell'organigramma funzionale adottato dalla Moba Eurotubi nella figura del **Responsabile della funzione Amministrazione, contabilità e controllo di gestione**, dotata degli strumenti delle risorse e delle competenze e della formazione necessarie e ciò, pertanto, in grado di gestire in maniera appropriata e diligente, autonoma le segnalazioni eventualmente pervenute.

Nel caso in cui il gestore della segnalazione, così come sopra individuato, coincida con il segnalante, con il segnalato o sia comunque una persona coinvolta o interessata dalla segnalazione, la segnalazione sarà indirizzata al Responsabile della Divisione Affari Generali, pro tempore, fermo restando la necessità che siano assicurati i requisiti richiesti ai fini di una gestione efficace, indipendente ed autonoma della segnalazione, nel rispetto degli obblighi di riservatezza previsti dalla normativa.

Contestualmente all'adozione del Modello Organizzativo 231 ed alla eventuale nomina dell'Organo di Vigilanza 231 (OdV), monocratico o collegiale, Moba Eurotubi si riserva di valutare l'affidamento a quest'ultimo del ruolo di gestore delle segnalazioni, in considerazione del fatto che l'OdV già possiede i requisiti richiesti dalla normativa per l'assolvimento dell'incarico (competenze tecniche, autonomia ed indipendenza funzionali e gerarchiche) e che la disciplina del Whistleblowing costituisce parte integrante del Modello Organizzativo 231, sulla cui osservanza l'OdV è chiamato a vigilare.

Quanto sopra, fermo restando che anche qualora l'OdV non venga investito del relativo incarico, lo stesso verrà comunque coinvolto nel processo di gestione delle segnalazioni whistleblowing, nel rispetto degli obblighi di riservatezza alla luce della rilevanza anche ai fini 231 delle violazioni segnalabili ai sensi della relativa normativa.

In particolare, l'OdV dovrà ricevere:

- immediata informativa sulle segnalazioni rilevanti in termini 231 affinché nell'esercizio della sua attività di vigilanza, possa condividere le proprie eventuali osservazioni e partecipare all'istruttoria o comunque seguirne l'andamento;
- un aggiornamento periodico sull'attività complessiva di gestione delle segnalazioni, anche non 231, al fine di verificare il funzionamento del sistema di whistleblowing e proporre eventuali necessità di suo miglioramento.

A tal fine, il Modello Organizzativo 231 dovrà disciplinare i predetti flussi informativi.

2.6.2 – Ricezione della segnalazione

La piattaforma rilascia al segnalante l'avviso di ricevimento entro sette giorni della presentazione della segnalazione.

Tale riscontro non implica per il gestore alcuna valutazione dei contenuti oggetto della segnalazione ma è unicamente volto ad informare il segnalante dell'avvenuta corretta ricezione della stessa.

Tale avviso viene inoltrato al recapito indicato dal segnalante nella segnalazione. In assenza di tale indicazione e dunque della possibilità di interagire con il segnalante per i seguiti è possibile considerare la segnalazione come non gestibile ai sensi della disciplina del whistleblowing,

Il sistema consentirà la ricezione di segnalazione anonime, anche alla luce delle indicazioni fornite dall'ANAC, qualora le stesse risultino puntuali, circostanziate e supportate da idonea documentazione, trattate come segnalazioni ordinarie trattate ai sensi dei regolamenti interni laddove eventualmente implementati.

La documentazione relativa alle segnalazioni anonime verrà comunque registrata dalla piattaforma al fine di consentire che laddove il segnalante anonimo venga successivamente identificato abbia subito ritorsioni, allo stesso debbano essere garantite le tutele previste per il whistleblower.

Completata la fase relativa alla trasmissione dell'avviso di ricevimento, gli uffici o la persona deputati possono procedere all'esame preliminare della segnalazione ricevuta.

Durante tale fase, il gestore della segnalazione esaminerà la procedibilità e l'ammissibilità della stessa.

2.6.3 – La procedibilità della segnalazione

La disciplina normativa definisce i presupposti soggettivi e oggettivi per effettuare una segnalazione interna.

Il gestore della segnalazione verificherà pertanto la sussistenza di tali presupposti:

- che il segnalante sia un soggetto legittimato ad effettuare la segnalazione;
- che l'oggetto della segnalazione rientri tra gli ambiti di applicazione della disciplina;

Nel caso in cui la segnalazione riguardi una materia esclusa dall'ambito oggettivo di applicazione, la stessa potrà essere trattata come ordinaria e quindi gestita secondo le eventuali procedure già in precedenza adottate dall'azienda per tali violazioni dandone comunicazione al segnalante.

2.6.4 – L'ammissibilità della segnalazione

Verificato che la segnalazione possieda i requisiti soggettivi ed oggettivi previsti dalla normativa, il gestore della segnalazione dovrà valutarne l'ammissibilità come segnalazione whistleblowing.

Ai fini della ammissibilità, è necessario che nella segnalazione risultino chiaramente indicate:

- Le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione e quindi, una descrizione che contenga i dettagli relativi alle notizie circostanziali e ove presenti, anche rispetto alle modalità attraverso cui il segnalante è venuto a conoscenza dei fatti;
- Le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati;

Alla luce di queste indicazioni, la segnalazione potrà quindi essere ritenuta inammissibile per:

- Mancanza dei dati che costituiscono gli elementi essenziali della segnalazione;
- Manifesta infondatezza degli elementi di fatto riconducibili alle violazioni previste espressamente dalla normativa;
- Esposizione dei fatti di contenuto generico tali da non consentirne la comprensione al gestore della segnalazione;
- Produzione di sola documentazione senza la segnalazione vera e propria di violazioni;

Nel caso in cui la segnalazione risulti improcedibile o inammissibile, il gestore della segnalazione potrà procedere alla sua archiviazione, garantendo comunque la tracciabilità delle motivazioni a supporto della decisione.

Durante la verifica preliminare il gestore della segnalazione potrà comunque richiedere al segnalante ulteriori elementi necessari per effettuare approfondimenti relativi alla segnalazione, di cui una volta verificata la procedibilità ed ammissibilità, procederà con l'avvio dell'istruttoria interna sui fatti e sulle condotte segnalate al fine di valutarne la fondatezza,

2.6.5 – Istruttoria ed accertamento della segnalazione

Il gestore della segnalazione assicura che siano effettuate tutte le opportune verifiche sui fatti segnalati, garantendo tempestività e rispetto dei principi di obiettività, competenza e diligenza professionale.

Nel caso in cui la segnalazione riguardasse il gestore della segnalazione dovranno essere garantite inoltre le opportune misure per la gestione del conflitto di interessi potenziale.

L'obiettivo di questa fase è di procedere con le verifiche, analisi e valutazioni specifiche circa la fondatezza o meno dei fatti segnalati, anche al fine di formulare eventuali raccomandazioni in merito all'adozione delle necessarie azioni correttive sulle aree e sui processi aziendali interessati nell'ottica di rafforzare il sistema di controllo interno.

Il gestore deve assicurare pertanto lo svolgimento delle adeguate verifiche necessarie, a titolo esemplificativo:

- Direttamente acquisendo gli elementi informativi necessari alle valutazioni attraverso l'analisi della documentazione / informazioni ricevute;
- Attraverso il coinvolgimento di altre funzioni aziendali o anche di soggetti specializzati esterni (es. tecnici IT) in considerazione delle specifiche competenze tecniche e professionali richieste;
- Audizione di eventuali soggetti interni / esterni;

Nel caso in cui risulti necessario avvalersi dell'assistenza tecnica di professionisti terzi, nonché del supporto specialistico del personale di altre funzioni/direzioni aziendali, si renderà necessario – al fine di garantire gli obblighi di riservatezza richiesti dalla normativa – oscurare ogni tipologia di dato che possa consentire l'identificazione della persona segnalante o di ogni altra persona coinvolta, incluso l'eventuale facilitatore o altre persone menzionate nella segnalazione:

Nel caso in cui si renda necessario il coinvolgimento di altri soggetti interni diversi dal Gestore anche ad essi andranno estesi gli obblighi di riservatezza espressamente previsti nella presente informativa Whistleblowing e nel Modello Organizzativo 231, sanzionati dal sistema disciplinare interno.

Qualora tali dati siano necessari all'indagine condotta da soggetti esterni (eventualmente coinvolti dal Gestore) tali doveri di confidenzialità e riservatezza saranno estesi anche a tali soggetti esterni nell'ambito di specifiche clausole contrattuali da inserire negli accordi stipulati con il soggetto esterno e nell'ambito del relativo conferimento di incarico ai fini della privacy,

Completata l'attività di accertamento della segnalazione, il gestore potrà:

- Archiviare la segnalazione perché infondata, motivandone le ragioni;
- Dichiarare fondata la segnalazione, rivolgersi agli organi / funzioni interne competenti per i relativi seguiti. Al gestore della segnalazione non compete alcuna valutazione in ordine alle responsabilità individuali ed agli eventuali successivi provvedimenti o procedimenti conseguenti.

Tutte le fasi di accertamento saranno completamente tracciate e correttamente archiviate al fine di dimostrare la corretta diligenza tenuta nel dare seguito alla segnalazione.,

Durante la fase di istruttoria e di accertamento della segnalazione è tutelata la riservatezza dell'identità della persona segnalante, del segnalato, e di tutte le persone coinvolte e/o menzionate nella segnalazione.

2.6.6 – Riscontro al segnalante

Il Gestore della segnalazione fornisce riscontro al segnalante entro 3 mesi dalla data di avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni per tale avviso.

Si precisa che non è necessario concludere l'attività di accertamento entro i 3 mesi, in considerazione del fatto che potrebbero sussistere fattispecie che richiedono, ai fini delle verifiche, un tempo maggiore.

Pertanto, alla scadenza dei 3 mesi, il gestore della comunicazione potrà comunicare al segnalante:

- l'avvenuta archiviazione della segnalazione, motivandone le ragioni;
- l'avvenuto accertamento della fondatezza della segnalazione e la sua trasmissione agli organi interni competenti;
- l'attività svolta fino a quel momento e/o l'attività che intende svolgere.

In tale ultimo caso, comunicherà anche il successivo esito finale dell'istruttoria della segnalazione (archiviazione o accertamento della fondatezza della segnalazione con trasmissione agli organi competenti).

2.7 – Tutele riconosciute al segnalante

La tutela riconosciuta al segnalante è assicurata attraverso:

- l'obbligo di riservatezza della sua identità;
- il divieto di atti ritorsivi nei suoi confronti;
- la limitazione della sua responsabilità per la rivelazione o diffusione di alcune tipologie di informazioni protette.

Tali misure di protezione si applicano non solo nei confronti del soggetto segnalante ma anche ad altri soggetti che potrebbero essere destinatari di ritorsioni, in ragione del ruolo assunto o della particolare vicinanza o rapporto, con il segnalante.

2.7.1 – La riservatezza dell'identità del segnalante

La principale tutela a favore del segnalante è costituita dall'obbligo di riservatezza della sua identità e di ogni altra informazione inclusa l'eventuale documentazione allegata dalla quale possa direttamente o indirettamente risalire all'identità del whistleblower, a cui sono tenuti:

- i soggetti competenti a ricevere e gestire le segnalazioni;
- l'ANAC
- le autorità amministrative cui l'Anac trasmette per competenza le segnalazioni esterne ricevute.

Nell'istituzione e regolamentazione del canale interno devono essere predisposte adeguate misure che consentano di mantenere riservata l'identità del segnalante, il contenuto della segnalazione e la relativa documentazione.

La riservatezza è garantita rispetto ad ogni modalità di segnalazione e quindi anche quando avvenga in forma orale.

Nell'ambito del procedimento disciplinare attivato dall'azienda nei confronti del presunto autore della condotta segnalata, l'identità del segnalante non può essere rivelata, ove la contestazione dell'addebito sia fondata, su accertamenti distinti ed ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa.

Qualora invece la contestazione sia fondata in tutto o in parte sulla segnalazione e l'identità del segnalante risulti indispensabile alla difesa del soggetto cui è stato contestato l'addebito disciplinare, quest'ultima sarà utilizzabile ai fini del procedimento disciplinare, solo previo consenso espresso della persona segnalante alla rivelazione della propria identità, cui è dato preventivo avviso mediante comunicazione scritta delle ragioni che rendono necessaria la rivelazione dei dati riservati.

Qualora il soggetto segnalante neghi il proprio consenso, la segnalazione non potrà essere utilizzata nel procedimento disciplinare che quindi non potrà essere avviato o proseguito in assenza di elementi ulteriori sui quali fondare la contestazione. Resta ferma in ogni caso, sussistendone i presupposti, la facoltà dell'ente di procedere con la denuncia all'Autorità Giudiziaria.

2.7.2 – Il Divieto e la protezione contro le ritorsioni

È fatto divieto di qualsiasi forma di ritorsione nei confronti del segnalante, inteso come qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato che si verifichi nel contesto lavorativo e che determini – in via diretta o indiretta – un danno ingiusto ai soggetti tutelati. Gli atti ritorsivi adottati in violazione di tale divieto sono nulli.

L'ANAC è l'Autorità preposta a ricevere dal segnalante e gestire le comunicazioni su presunte ritorsioni dallo stesso subite. Affinché sia riconosciuta tale forma di tutela è necessario che:

- il segnalante/denunciante al momento della segnalazione o della denuncia all'A.G. o contabile o della divulgazione pubblica avesse fondato motivo di ritenere le informazioni veritiere e rientranti nel perimetro di applicazione della relativa disciplina;
- la segnalazione/denuncia/divulgazione sia stata effettuata secondo la disciplina prevista dalla normativa vigente.

A titolo esemplificativo, non esaustivo e non tassativo, viene riportato un elenco delle possibili fattispecie ritorsive:

- a) il licenziamento, la sospensione o misure equivalenti;
- b) la retrocessione di grado o mancata promozione;
- c) il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- d) la sospensione della formazione o qualsiasi restrizione all'accesso della stessa;
- e) note di merito o referenze negative;
- f) l'adozione di misure disciplinari o di altra sanzione;
- g) la coercizione, l'intimidazione, le molestie, l'ostracismo;
- h) la discriminazione o l'applicazione di trattamenti più sfavorevoli;
- i) il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
- j) la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
- k) l'annullamento di un permesso;
- l) la richiesta di sottoposizione ad accertamenti psichiatrici o medici;

Qualora l'Autorità consideri inammissibile la comunicazione provvederà ad archivarla; se invece dovesse accertarne la fondatezza ed il nesso causale tra segnalazione e ritorsione avvierà il procedimento sanzionatorio.

Nel caso di provvedimento sanzionatorio, in caso di ritorsioni commesse nel contesto lavorativo di un soggetto del settore privato, l'ufficio preposto informa l'Ispettorato Nazionale del Lavoro per i provvedimenti di competenza.

Rimane di competenza dell'autorità giudiziaria disporre le misure necessarie ad assicurare la tutela del segnalante.

Nei procedimenti dinanzi all'ANAC l'intento ritorsivo si presume, determinando un'inversione dell'onere probatorio a carico della persona che ha posto in essere la presunta ritorsione che dovrà quindi fornire concreta ed effettiva dimostrazione che la presunta tale non è connessa alla segnalazione/denuncia ma dipende da ragioni estranee. Questa presunzione opera esclusivamente a favore del segnalante e non anche del facilitatore e dei soggetti ad esso assimilati,

Il segnalante perde la protezione, qualora i) sia accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante per i reati di diffamazione o di calunnia o nel caso in cui tali reati siano commessi con la denuncia all'autorità giudiziaria o contabile, ii) in caso di responsabilità civile per lo stesso titolo per dolo o colpa grave. In entrambe le ipotesi alla persona denunciante o segnalante verrà irrogata una sanzione disciplinare.

A fronte di segnalazione anonima, la tutela è assicurata anche qualora la persona segnalante sia stata successivamente identificata o la sua identità si sia palesata solamente in un secondo momento.

2.7.3 – Le limitazioni della responsabilità del segnalante

In conformità a quanto previsto dalla disciplina normativa vigente è riconosciuta una limitazione della responsabilità del segnalante rispetto alla rivelazione ed alla diffusione di alcune categorie di informazioni che altrimenti lo esporrebbero a responsabilità penali, civili ed amministrative.

In particolare, il segnalante non sarà chiamato a rispondere né penalmente né in sede civile ed amministrativa:

- di rivelazione ed utilizzazione del segreto d'ufficio (art. 326 c.p.);
- di rivelazione del segreto professionale (art. 622 c.p.);
- di rivelazione dei segreti scientifici ed industriali (art. 623 c.p.);
- di violazione del dovere di fedeltà e di lealtà (art. 2105 c.c.);
- di violazione delle disposizioni relative alla tutela del diritto d'autore;
- di violazione delle disposizioni relative alla protezione dei dati personali;
- di rivelazione o di diffusione di informazioni sulle violazioni che offendono la reputazione della persona coinvolta;

a condizione che:

- al momento della rivelazione o della diffusione vi siano fondati motivi per ritenere che le informazioni siano necessarie per svelare la violazione oggetto di segnalazione;
- la segnalazione sia effettuata nel rispetto delle condizioni previste dalla normativa per beneficiare della tutela contro le ritorsioni (fondati motivi per ritenere veritieri i fatti segnalati, la violazione rientri tra quelle segnalabili e siano rispettate le modalità e le condizioni di accesso alla segnalazione).

La limitazione della responsabilità opera, pertanto, se le ragioni alla base della rivelazione o diffusioni non sono fondate su semplici illazioni, gossip, fini vendicativi, opportunistici o scandalistici.

Non viene invece esclusa la responsabilità del segnalante per condotte che:

- non siano collegate alla segnalazione;
- non siano strettamente necessarie a rivelare la violazione;
- configurino un'acquisizione di informazioni o l'accesso modo illecito.

Ove l'acquisizione si configuri come un reato, si pensi all'accesso abusivo ad un sistema informatico o ad un atto di pirateria informatica, resta ferma la responsabilità penale ed ogni altra responsabilità civile, amministrativa e disciplinare della persona segnalante.

La normativa consente altresì al segnalante ed altri soggetti tutelati di poter rinunciare ai propri diritti e mezzi di tutela o farne oggetto di transazione, la cui rinuncia è generalmente vietata, solo se ciò avviene nelle sedi protette e quindi dinanzi ad un giudice a seguito del tentativo obbligatorio di conciliazione o di accordi di mediazione e conciliazione predisposti in sede sindacale o davanti agli organi di certificazione.

2.8 – Sistema sanzionatorio

Le linee guida ANAC distinguono per le varie fattispecie tra persona fisica e giuridica ritenute responsabili e quindi destinatarie della sanzione.

Oltre alle ipotesi di mancata istituzione del canale di segnalazione, di mancata adozione delle procedure o di adozione di procedure non conformi, a carico dell'organo di indirizzo amministrativo della Società e di quelle applicabili per l'ipotesi invece in cui non sia stata svolta l'attività di verifica ed analisi delle segnalazioni ricevute, nonché laddove sia stato violato l'obbligo di riservatezza, la cui responsabilità è individuata nel gestore delle segnalazioni, da valutare nell'ambito delle prerogative riconducibili allo svolgimento dell'attività lavorativa del soggetto incaricato della gestione delle segnalazioni,

la normativa prevede delle sanzioni amministrative pecuniarie anche verso chi abbia posto in essere un atto ritorsivo, per cui risulta sanzionabile direttamente la persona fisica individuata come responsabile delle ritorsioni, ed una sanzione amministrativa pecuniaria da 500 a 2.500 euro quando fosse accertata anche con sentenza di primo grado la responsabilità civile della persona segnalante per diffamazione o calunnia, nei casi di solo o colpa grave, salvo che la medesima sia già stata condannata anche in primo grado, per i reati di diffamazione o di calunnia o comunque per i medesimi reati già commessi con la denuncia all'autorità giudiziaria.

2.9 – Segnalazione esterna e divulgazione pubblica

La normativa attribuisce all'ANAC il compito di istituire un canale di segnalazione accessibile non solo ai soggetti appartenenti al settore pubblico ma anche al settore privato che sia idoneo ad assicurare la riservatezza dell'identità segnalante e di coloro che sono coinvolti nella segnalazione, del contenuto della segnalazione stessa e della relativa documentazione.

Il segnalante può ricorrere al canale della segnalazione esterna istituito dall'ANAC soltanto se ricorre una delle seguenti condizioni:

- i) Nel suo contesto lavorativo non è prevista l'attivazione del canale interno come obbligatoria, o se prevista, non è stata attivata;
- ii) La segnalazione non ha avuto seguito nel senso che non sia stata intrapresa entro i termini previsti alcuna attività circa l'ammissibilità della segnalazione, la verifica circa la sussistenza dei fatti segnalati o la comunicazione dell'esito dell'attività svolta;
- iii) Ha fondati motivi di ritenere che, se effettuasse la segnalazione interna, questa non avrebbe seguito - ad esempio per il rischio che le prove di condotte illecite possano essere occultate o distrutte o vi sia il timore di un accordo tra chi riceve la segnalazione e la persona coinvolta nella segnalazione, o ancora all'ipotesi in cui il gestore della comunicazione risulti in conflitto di interesse - oppure che andrebbe incontro a ritorsioni sulla base di circostanze concrete che devono essere allegare alla segnalazione e su informazioni acquisibili;
- iv) Ha fondati motivi per ritenere che la violazione possa costituire un pericolo immediato o palese per il pubblico interesse, per esempio quando la violazione richieda un intervento urgente da parte di un'autorità pubblica per salvaguardare un interesse collettivo quale ad esempio la salute, la sicurezza o la protezione dell'ambiente.

ANAC ha disciplinato nelle sue Linee Guida e nel Regolamento apposito, le modalità di presentazione e gestione delle segnalazioni esterne, prevedendo che le stesse possano essere gestite soltanto dalle persone fisiche legittimate ai sensi del Decreto (esclusa la possibilità di ricorrervi per rappresentanti delle organizzazioni sindacali).

Riguardo alle modalità di presentazione, le segnalazioni possono essere effettuate:

- a) Tramite piattaforma informatica con crittografia dei dati del segnalante e della segnalazione, individuata come canale prioritario, accessibile solo al Custode delle Identità che per garantire la massima riservatezza consente al Dirigente dell'Ufficio Whistleblowing dell'ANAC di accedere all'identità del segnalante solo dopo esplicita e motivata richiesta.
- b) Oralmente attraverso un servizio telefonico con operatore, rappresentato da un componente dell'ufficio ANAC competente che acquisisce la segnalazione telefonica e la inserisce nella piattaforma unitamente al file audio e alla registrazione;
- c) Tramite incontri diretti fissati entro un termine ragionevole, cui consegue l'inserimento della segnalazione in piattaforma da parte dell'operatore, dietro richiesta motivata.

Per essere considerata ammissibile nella segnalazione devono essere indicati denominazione e recapiti del whistleblower, i fatti oggetto di segnalazione e l'amministrazione o l'ente in cui sono avvenuti, l'ente o l'amministrazione nel cui contesto operativa opera il whistleblower ed il suo profilo professionale oltre che una descrizione sintetica delle modalità in cui il whistleblower è venuto a conoscenza dei fatti segnalati,

La segnalazione esterna è considerata inammissibile per i) manifesta infondatezza per l'assenza di elementi di fatto riconducibili alle violazioni tipizzate ii) manifesta infondatezza dei presupposti di legge per l'esercizio dei poteri di vigilanza iii) manifesta incompetenza dell'Autorità sulle questioni segnalate iv) contenuto eccessivamente generico della segnalazione esterna corredata da documentazione non appropriata v) produzione di documentazione in assenza di segnalazione esterna, vi) mancanza dei dati che costituiscono elementi essenziali della segnalazione esterna, vii) violazioni di lieve entità.

L'Anac può valutare la sussistenza dei requisiti di ammissibilità prevedendo la possibilità di integrazione istruttoria. Se le segnalazioni riguardano violazioni che non rientrano nella competenza dell'ANAC, l'Ufficio istruttore può provvedere ad inviare la relativa segnalazione all'autorità amministrativa competente oppure all'autorità giudiziaria.

In ogni caso l'Ufficio entro tre mesi, o se ricorrono giustificate ragioni sei mesi dalla data di avviso di ricevimento della segnalazione esterna, in mancanza di detto avviso dalla scadenza di sette giorni dal ricevimento, comunica al segnalante i) l'archiviazione predisposta o che intende effettuare ii) la trasmissione all'autorità competente già effettuata o che intende effettuare, iii) l'attività già svolta dall'ufficio di vigilanza competente interno all'Autorità o l'attività che quest'ultimo intende svolgere, l'esito finale della segnalazione che può consistere nell'archiviazione, nelle risultanze istruttorie dell'Ufficio di vigilanza competente o nella trasmissione alle autorità competenti,

La normativa introduce anche per il segnalante la possibilità di effettuare una divulgazione pubblica beneficiando della protezione. Si tratta di una novità estremamente delicata in ragione delle potenzialità lesive per l'ente di una denuncia effettuata in assenza di giustificati motivi o di fondati elementi di prova. Ciò rende necessario circoscrivere il più possibile, anche in via interpretativa, il ricorso a tale istituto.

Per ricorrere a tale procedura deve ricorrere almeno una delle seguenti condizioni:

che sia stato previamente utilizzato il canale interno e/o esterno, ma non vi sia stato alcun riscontro o non vi sia stato seguito entro i termini previsti dalla normativa;

che il segnalante ritenga sussistere fondati motivi di un pericolo imminente e palese per il pubblico interesse, considerato come una situazione di emergenza o di rischio di danno irreversibile, anche all'incolumità fisica di una o più persone, che richieda che la violazione sia tempestivamente svelata con ampia risonanza per impedirne gli effetti;

oppure fondati motivi per ritenere che la segnalazione esterna possa comportare un rischio di ritorsione oppure non avere un efficace seguito perché per esempio potrebbe ricorrere un pericolo di distruzione delle prove o di collusione tra l'autorità preposta e ricevere la segnalazione e l'autore della violazione. Anche in questo caso i fondati motivi che legittimano il ricorso alla segnalazione esterna devono essere fondati sulla base di circostanze concrete che devono essere allegate alla segnalazione e su informazioni effettivamente acquisibili.

Ove il soggetto che effettui una divulgazione pubblica riveli la propria identità non si pone un problema di tutela della riservatezza, fermo restando la garanzia delle altre tutele. Se lo stesso ricorre a pseudonimo o nickname, la segnalazione verrà trattata alla stregua di una segnalazione anonima pur avendo cura di registrarla.

2.10 – Trattamento dei dati personali

La ricezione e la gestione delle segnalazioni interne determinano in capo alla Società il trattamento dei dati personali delle persone a vario titolo coinvolte nei fatti segnalati.

Tale trattamento dovrà essere attuato in conformità alla normativa vigente in materia di protezione dei dati personali (Regolamento UE n. 679/2016 cd. GDPR ed il D.Lgs. n. 196/2003 cd. Codice della Privacy).

Qualora la gestione del canale di segnalazione sia affidata in tutto o in parte ad un soggetto esterno alla sua organizzazione (es. fornitore della piattaforma) quest'ultimo tratta i dati in qualità di responsabile del trattamento ed in quanto tale deve presentare garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche ed organizzative che garantiscano la protezione dei dati.

L'esecuzione dei trattamenti da parte dei responsabili di trattamento dovrà essere disciplinata nell'ambito di un atto giuridico che stabilisca: a) le caratteristiche del trattamento affidato al responsabile, con particolare riguardo alla natura, alla finalità e alla durata del trattamento, al tipo di dati personali e alle categorie di interessati; b) gli obblighi e diritti del titolare del trattamento; c) le istruzioni per il trattamento dei dati da parte del responsabile.

Le persone fisiche preposte alla ricezione e/o alla gestione della segnalazione trattano i dati in qualità di soggetti autorizzati al trattamento, in quanto espressamente autorizzati ed istruiti in tal senso dal titolare o dal responsabile.

Nella fase di acquisizione della segnalazione e della eventuale successiva istruttoria non devono essere fornite informative specifiche ai soggetti diversi dal segnalante.

Ai fini della impostazione dei canali di segnalazione la normativa in materia di whistleblowing richiede espressamente sia data attuazione ai principi di:

- Trasparenza (art. 5, par. 1, lett. a) GDPR, da attuarsi mediante apposita idonea informativa sul trattamento dei dati personali da rendere ex ante ai possibili soggetti interessati recante informazioni sul i) titolare del trattamento e relativi dati di contatto; ii) la finalità del trattamento, iii) la base giuridica del trattamento, iv) le modalità del trattamento, v) l'ambito ed i soggetti cui sono comunicati i dati; vi) il periodo di conservazione dei dati. Tale informativa potrà essere allegata all'informativa "whistleblowing", in apposita sezione del sito web o dell'applicativo informatico,

- Limitazione delle finalità (art. 5, par. 1, lett. b) GDPR): i dati personali sono raccolti per finalità determinate, esplicite, legittime e successivamente trattati in modo che non sia incompatibile con tali finalità, prevedendo che le segnalazioni non possano essere utilizzate oltre quanto necessario per dare adeguato riscontro alle stesse;
- Minimizzazione dei dati (art. 5, par. 1, lett. c) GDPR): i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- Limitazione della conservazione (art. 5, par. 1, lett. e) GDPR); i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati e comunque non oltre 5 anni dalla comunicazione dell'esito finale della procedura;
- Integrità e riservatezza (art. 5, par. 1, lett. f) GDPR); i dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali compresa la protezione mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o da danni accidentali;

2.11 – Modalità comunicazione e diffusione

Al fine di mettere a disposizione del segnalante (a titolo esemplificativo personale interno, consulenti esterni, partner commerciali, fornitori, ecc.) informazioni chiare circa il canale, le procedure ed i presupposti per effettuare le segnalazioni interne ed esterne, come richiesto dall'art. 5, co. 1 del Decreto, la presente informativa è pubblicata in forma integrale presso apposita sezione del sito istituzionale dell'azienda (www.gruppomoba.com), accessibile quindi a tutti i soggetti legittimati a presentare delle segnalazioni di whistleblowing, nella medesima sezione in cui è presente il link per l'accesso alla piattaforma informatica per l'effettuazione delle segnalazioni, nonché disponibile per la consultazione nei luoghi di lavoro.