PROCEDURA WHISTLEBLOWING

Data approvazione 26 Gennaio 2024

La presente procedura, approvata dalla società, previa informativa alla rappresentanza sindacale aziendale e territoriale, è diretta a gestire le segnalazioni di illeciti effettuate ai sensi del Decreto Legislativo n. 24/2023 attuativo della Direttiva Europea n. 1937/2019.

Alcuni termini

Whistleblowers: sono tutti coloro che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea

Violazioni: qualsiasi comportamento, atto od omissione che lede l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato (a titolo esemplificativo ma non esaustivo: illeciti amministrativi, contabili, civili o penali)

Segnalazione: comunicazione scritta o orale di informazioni sulle violazioni

Segnalazione interna o esterna (esterna: tramite canale esterno ANAC)

Facilitatore: persona fisica che assiste il segnalante, nel processo di segnalazione, operante nello steso contesto lavorativo

Soggetti/persone che possono segnalare (c.d. Whistleblower)

Tutte le persone che operano nel contesto lavorativo di un soggetto pubblico o privato, sono legittimate ad effettuare segnalazioni

- **Lavoratori subordinati** di soggetti del settore privato
- **Lavoratori autonomi** che svolgono la propria attività lavorativa presso soggetti del settore privato
- **Collaboratori, liberi professionisti e consulenti** che prestano la propria attività preso soggetti del settore privato
- **Volontari e tirocinanti**, retribuiti e non retribuiti

- **Azionisti e persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza**, anche se le funzioni sono esercitate in via di mero fatto, presso soggetti del settore privato
- **Persone che lavorano sotto la supervisione e la direzione di appaltatori**
- **Subappaltatori e fornitori**

Le persone segnalanti beneficiano di protezione a condizione che abbiano avuto fondati motivi di ritenere che le informazioni segnalate fossero vere al momento della segnalazione e che tali informazioni rientrassero nell'ambito oggettivo di applicazione.

I soggetti segnalanti vengono tutelati, quando effettuano segnalazioni, se:

- Il rapporto giuridico è in corso
- Il rapporto giuridico non è ancora iniziato, ma le informazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali
- Durante il periodo di prova
- Successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite prima dello scioglimento del rapporto stesso (es.: pensionati)

Ambito oggettivo di applicazione – cosa si può segnalare

Possono essere segnalate violazioni aventi ad oggetto condotte che comportano gli estremi dei reati previsti nel D.Lgs. n. 231/2001 (c.d. reati presupposto).

La segnalazione può riguardare anche:

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

- . sospetti fondati, ossia irregolarità tali da far ritenere che potrebbe essere commessa una delle violazioni previste dal decreto.

Canale per la segnalazione – come segnalare

Canale interno

Mediante la pagina web ***klinicom.onwhistleblowing.com*** attraverso software Whistleblowing della piattaforma OmMyCompany che garantisce l'assoluto anonimato del segnalante. Per garantire la non tracciabilità è inserito nella pagina web il link per inviare la segnalazione mediante browser.

Le segnalazioni possono essere effettuate anche in forma orale: linee telefoniche, sistemi di messaggistica vocale, oppure su richiesta del segnalante, tramite incontro diretto fissato entro un termine ragionevole.

Canale esterno – gestito da ANAC

E' possibile ricorrere alla segnalazione all'ANAC quando il canale interno non è previsto o non è attivo; la segnalazione interna non ha avuto seguito; il segnalante ha fondati motivi di ritenere che la segnalazione interna possa determinare un rischio di ritorsione, il segnalante ha fondato motivo di ritenere che la violazione costituisca un pericolo imminente per il pubblico interesse.

Contenuto della segnalazione

La segnalazione deve contenere: la data, l'identità del segnalante, a meno che non voglia mantenere l'anonimato, il periodo ed il luogo fisico in cui si è verificato il fatto, soggetto/i che ha/hanno commesso il fatto (nome, cognome, qualifica), modalità con cui è venuto a conoscenza del fatto, eventuali altri soggetti che possono riferire sul

fatto (nome, cognome, qualifica, recapiti), area aziendale a cui è riferito il fatto, descrizione del fatto ed i motivi per cui la condotta è illecita.

Modalità di gestione della segnalazione

Soggetti incaricati della procedura (competenti a ricevere e a dare seguito alle segnalazioni

Sono gestite direttamente dall'Organismo di Vigilanza (di seguito: "O.d.V.").

Tutela della riservatezza

In ogni caso viene garantita la riservatezza del segnalante, la cui identità non sarà rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni.

Sono coperti da riservatezza, non solo il nome, ma tutti gli elementi da cui si possa ricavare, anche indirettamente, l'identificazione del segnalante.

Ogni informazione relativa a segnalazioni viene protetta con algoritmo asimmetrico RSA per la condivisione delle chiavi e algoritmo simmetrico AES per la criptazione finale dei file.

Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento.

Il sistema è installato su sistema operativo Windows dove è attiva la tecnologia Bitlocker.

Per quanto riguarda il sistema cloud, la VPN è crittografata (VPN IPSEC SSL); l'applicativo è esclusivamente HTTPS (il certificato è rilasciato da Let's Encrypt). E'stato scelto di implementare la soluzione TDE (Transparent Data Encryption): essa consiste nell'avere file DB, file di Log, di Backup e il Transaction log criptati ma i dati

all'interno del DB sono in chiaro. Solo il server DB che possiede il certificato è in grado di decriptare il DB.

Ogni informazione scambiata viene protetta in transito da protocollo HTTPS.

Le pagine HTML restituite al client sono impostate per non essere inserite in cache. Questo meccanismo, legato ad una sessione utente con durata limitata a 20 minuti di inattività, permette una congrua chiusura della sessione per rendere inaccessibile il contenuto aperto e non più presidiato.

Accesso ai dati politiche di sicurezza

L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali.
Il sistema implementa la seguente policy password sicura:

- Al primo accesso, per validare l'utente viene richiesto il passaggio tramite verifica della mail;
- L'utente al primo accesso sceglie in autonomia la propria password;
- Sono state definite delle regole di complessità della PSW (Alfanumerico, almeno 8 caratteri, e almeno un carattere speciale);
- La PSW può essere modificata in qualsiasi momento. Non risulta possibile riutilizzare le 4 PSW precedenti;
- Dopo 5 tentativi errati di inserimento PSW in 5 minuti, si blocca l'utenza. Solo un amministratore del sistema può sbloccare l'utenza.

Il sistema implementa protocollo di autenticazione a due fattori (MFA) con protocollo Oauth2.

Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.

I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent. I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati.

L'applicativo è periodicamente soggetto ad attività di Penetration test da parte della società che lo ha sviluppato, tramite personale professionalmente specializzato.

Il Back up viene eseguito dalla società che lo ha sviluppato, nel rispetto della Procedura interna Gestione backup e disaster recovery. Le operazioni di backup sono periodicamente verificate per garantire che soddisfino i requisiti dei piani di continuità gestionale in caso di emergenza. La procedura di Business Continuity inoltre garantisce continuità di trattamento dei dati, definendo a livello procedurale quali attività devono essere svolte dopo un evento imprevisto e negativo. In relazione al back up effettuato per l'applicazione whistleblowing fornita in modalità Saas, viene utilizzato lo strumento messo a disposizione dal cloud provider ArubaPEC Spa, Veeam; viene effettuato un back up delle intere virtual machine (DB compreso). La retention delle copie di back up è di 30 giorni dalla risoluzione del contratto

Sicurezza informatica delle informazioni

Tutte le connessioni sono protette tramite protocollo HTTPS

Il privilegio di amministratore, a qualsiasi livello, viene conferito solamente a risorse interne di Onit o qualora necessario temporaneamente, e sempre sotto la supervisione di personale Onit smart e/o Onit Sistemi, a consulenti esterni debitamente contrattualizzati con lettera di incarico e nomina a Responsabile di trattamento e amministratore di Sistema.

Tempistiche di gestione della segnalazione

- . avviso di ricevimento della segnalazione entro 7 giorni dalla ricezione;

- . riscontro alla segnalazione entro 3 mesi dalla data di avviso di ricevimento.

Svolgimento dell'istruttoria

L'O.d.V.:

- . svolge l'istruttoria necessaria a dare seguito alla segnalazione, anche mediante audizioni e acquisizioni di documenti;
- . mantiene le interlocuzioni con la persona segnalante e richiede a quest'ultima, se necessario, integrazioni;
- . redige la relazione finale, in cui sono indicate le attività svolte, i relativi esiti e la valutazione dei fatti segnalati alla luce delle procedure vigenti ed eventuali suggerimenti per impedire il reiterarsi dei comportamenti oggetto di segnalazione;
- . se ravvisa profili di reato, trasmette la comunicazione al Presidente della società cui compete la valutazione della trasmissione della comunicazione alle forze dell'ordine;
- . comunica alla persona segnalante l'esito finale della istruttoria, e adotta ogni conseguenziale provvedimento.

Conservazione della documentazione inerente alle segnalazioni

Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e, comunque, non oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

Misure di protezione

Protezione dalle ritorsioni

E' vietata ogni forma di ritorsione anche solo tentata o minacciata.

Sono considerate ritorsioni: *"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 denuncia, in via diretta o indiretta, un danno ingiusto".*

Alcune fattispecie di ritorsioni:

- licenziamento, sospensione o misure equivalenti;

- retrocessione di grado o la mancata promozione;

- mutamento di funzioni, cambiamento del luogo di lavoro, riduzione dello stipendio, modifica dell'orario di lavoro;

- sospensione della formazione o qualsiasi restrizione di accesso alla stessa;

- note di merito negative o referenze negative;

- adozione di misure disciplinari o altra sanzione anche pecuniaria;

- coercizione, intimidazione, molestie o ostracismo;

- discriminazione o trattamento sfavorevole;

- mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, nel caso il lavoratore avesse una legittima aspettativa a detta conversione;

- mancato rinnovo o la risoluzione anticipata di un contratto do lavoro a termine;

- danni, anche alla reputazione della persona, in particolare sui social media, o pregiudizi economici o finanziari, compresa la perdita di opportunità economiche e la perita di redditi;

- conclusione anticipata o annullamento del contratto di fornitura di beni o servizi;

- annullamento di una licenza o permesso

- richiesta di sottoposizione ad accertamenti psichiatrici o medici

Misure di sostegno

E' istituito presso l'ANAC ed è pubblicato sul sito l'elenco degli enti del terzo settore che forniscono alle persone segnalanti misure di sostegno.

Tali misure consistono in informazioni, assistenza e consulenza a titolo gratuito sulle modalità di segnalazione, sulle protezioni dalle ritorsioni e sui diritti della persona coinvolta.

Le misure di protezione si applicano anche:

- al **facilitatore** (persona che assiste il segnalante nel processo di segnalazione, operante nel medesimo contesto lavorativo e la cui assistenza deve rimanere riservata)

- alle **persone legate al segnalante** da uno stabile legame affettivo o di parentela entro il quarto grado, che appartengono allo stesso contesto lavorativo di colui che ha segnalato, sporto denuncia o di colui che ha effettuato una divulgazione pubblica;

- ai **colleghi di lavoro** della persona segnalante o della persona che ha sporto denuncia o effettuato una divulgazione pubblica e che hanno con questa persona un rapporto abituale e corrente;

- agli **enti di proprietà** della persona segnalante o per i quali le stesse persone lavorano nonché gli **enti che operano nel medesimo contesto lavorativo** delle predette persone

Inversione dell'onere della prova

Nei procedimenti giudiziari o amministrativi relativi a comportamenti ritorsivi, si presume che gli stessi siano posti in essere a causa della segnalazione. L'onere di provare l'estraneità alla segnalazione, incombe su colui che le ha poste in essere.

Limitazioni della responsabilità

Non è punibile chi riveli o diffonda informazioni coperte da obbligo di segreto o relative alla tutela del diritto di autore o alla protezione dei dati personali, quando vi è fondato motivo che tali rivelazioni siano necessarie per svelare la violazione e la rivelazione sia effettuata nelle modalità richieste.

La seguente procedura verrà esposta nelle bacheche aziendali e pubblicata mediante il seguente link https://klinicomsrl-my.sharepoint.com/:f:/g/personal/klinicom_klinicom_it/EmSzpz7ZQpRPs2-W4nsV0LYBIMzVuLCpzRG88XPe2TNS0w?e=20AQNG

Il Legale Rappresentante

Firma