

## **WHISTLEBLOWING: GLI ADEMPIMENTI NECESSARI ALL'ADEGUAMENTO**

A partire dal 17 dicembre 2023, per tutte le aziende con un numero di dipendenti superiore a 50, entrano in vigore nuovi adempimenti obbligatori per i datori di lavoro privati per il rispetto della normativa in tema di protezione dei dipendenti che denunciano illeciti di cui sono testimoni sul proprio posto di lavoro.

Si tratta del cosiddetto “**whistleblowing**”, regolamentato dal recente **D.Lgs. n. 24/2023** che ha recepito l'ultima Direttiva Europea (Dir. UE 2019/1937), in tema.

### **Cos'è il “Whistleblowing”?**

La definizione letterale è “soffiare nel fischietto”, ma consiste in uno strumento di compliance aziendale che permette ai dipendenti di un'azienda e agli stakeholder, come ad esempio fornitori o clienti, di segnalare, in modo riservato e con le opportune garanzie in termini di tutele, eventuali illeciti riscontrati in ambito aziendale.

Il D.Lgs. 24/2023, reca disposizioni volte a fornire ai segnalanti (o *whistleblowers*) una tutela introducendo regole che impongano l'adozione di canali di segnalazione efficaci, riservati e sicuri e, al tempo stesso, garantiscano una protezione degli informatori da possibili ritorsioni.

### **Ma quali misure specifiche devono adottare le aziende per essere conformi alla normativa?**

La normativa è molto complessa e prevede sanzioni elevate in caso di mancata conformità.

Per questo, di seguito, vengono indicati gli adempimenti essenziali che le aziende devono adottare al fine di garantire la compliance del processo.

Fondamentale è la scelta di un canale telematico idoneo allo scopo e in grado di garantire da un lato fruibilità gestionale e dall'altro, l'applicazione di principi di *security* e *privacy by design*.

Tali principi vengono rispettati mediante la **crittografia dei dati** che ne garantisce l'integrità (i dati non possono essere corrotti o modificati), la privacy (i dati non possono essere intercettati da terze parti) e l'autenticità (l'utente finale deve essere certo che il canale in cui sta effettuando la segnalazione sia quello realmente implementato dall'azienda).

Il sistema deve poi garantire **la riservatezza dell'identità del segnalante** (nonché di facilitatori, colleghi, parenti ed enti collegati), **del segnalato e del contenuto della segnalazione**.

L'ANAC, nelle sue Linee Guida, ritiene che, strumenti quali la posta elettronica ordinaria o la PEC non siano adeguati a garantire la riservatezza.

Il canale/sistema deve inoltre rendere disponibile anche **l'anonimizzazione** che deve essere soddisfatta in tutte le fasi di gestione del “procedimento” stesso, se il *whistleblower* lo richiede.

Il sistema non deve memorizzare informazioni che non siano state fornite in modo esplicito dal segnalante.

Particolare importanza rivestono inoltre i metadati (ora e luogo di creazione del file, autore, attributi di formattazione, ecc...): questi potrebbero infatti rivelare l'identità dell'informatore in modo indiretto. Il sistema deve quindi garantire che i metadati vengano rimossi automaticamente prima che la segnalazione venga inviata.

Un canale di segnalazione che rispetti tutte le possibili modalità di segnalazione indicate dalla normativa, prevede inoltre segnalazioni da effettuarsi tramite registrazione vocale. In tal caso, per garantire l'anonimizzazione, dovrà essere presente un meccanismo di alterazione della voce del *whistleblower*.

L'azienda dovrà poi occuparsi di strutturare un sistema documentale adeguato, tra cui: un'ideale **informativa privacy**, una **procedura** di riferimento per la gestione delle segnalazioni da pubblicare rendere nota anche alle rappresentanze sindacali. L'azienda deve dotarsi anche di strumenti di *compliance* per la protezione dei dati, quali una **Valutazione d'impatto ex art. 35 GDPR** e un accordo per il trattamento dei dati con i soggetti preposti a ricevere le segnalazioni e/o con i fornitori del sistema/canale.

Responsabilità della direzione aziendale è poi pianificare e attuare periodicamente la **formazione dei dipendenti** in materia.

Un'ulteriore area di attenzione deve essere **la scelta corretta del soggetto preposto a ricevere e gestire le segnalazioni**. Non può essere individuato un soggetto che, a causa del ruolo esercitato presso l'Ente/Azienda, non abbia le caratteristiche di autonomia operativa, imparzialità e indipendenza, né tanto meno un soggetto esterno non in possesso delle necessarie competenze in materia per gestire correttamente le segnalazioni ricevute e veicolarle alla funzione interna deputata (es. OdV, DPO, RSPP, CdA, Collegio Sindacale, ecc.). Da tenere in considerazione anche la tempestività della presa in carico delle segnalazioni: la presa in carico della segnalazione dovrà essere comunicata al segnalante entro 7 giorni.

**La normativa prevede sanzioni da 10.000 a 50.000 euro, al verificarsi delle seguenti ipotesi:**

- mancata istituzione dei canali di segnalazione;
- mancata adozione delle procedure per effettuare e gestire le segnalazioni;
- adozione di procedure non conformi a quelle previste agli artt. 4 e 5 del D.Lgs. n. 24/2023;
- violazione dell'obbligo di riservatezza circa l'identità del segnalante;
- mancato svolgimento dell'attività di verifica e dell'analisi delle segnalazioni ricevute;
- ostacoli alla segnalazione o tentativi di ostacolarla;
- comportamenti ritorsivi.

L'istituzione di un canale Whistleblowing conforme alla normativa richiede quindi un'attenzione particolare, sia sulle tematiche tecnologiche ma anche organizzative e di presidio, nonché competenze diversificate ed una gestione in grado di garantire autonomia e indipendenza.

A cura di De Pieri Sara

**Praolini srl – New Consulting**



[www.new-consulting.it](http://www.new-consulting.it)

Tel/Fax: 0297297995