



Management e Whistleblowing in ambito D.lgs231/2001

***Whistleblowing: applicazioni pratiche in azienda
Ostacoli, soluzioni e lezioni apprese***

Dott.ssa Annalisa Quintavalle

02 Luglio 2025



Indice degli argomenti:

- **Perché è un tema manageriale**
- **Come strutturare un processo efficace**
- **Soluzioni applicative**
- **Casi di studio**



Perché è un tema manageriale

- Un sistema per la gestione della normativa del Whistleblowing è un processo che attiene alla governance aziendale, non si può limitare a essere gestito come un semplice obbligo.
- Un'adeguata gestione delle informazioni sensibili è fondamentale per la prevenzione dei rischi.
- Gli ingegneri hanno un ruolo strategico all'interno delle aziende per governare l'evoluzione dei processi aziendali.



Come strutturare un processo efficace

- Accessibilità: canale semplice e raggiungibile.
- Chiarezza: policy chiara e comprensibile.
- Tempestività: tempi certi nella gestione.
- Riservatezza: tutela del segnalante.
- Integrazione: collegamento con MOG 231 e cultura aziendale.



Come strutturare un processo efficace

La parte più delicata **non è tecnologica, ma organizzativa** interna:

- Chi gestisce cosa?
- Come si evita il conflitto di interessi?
- Come si costruisce fiducia nel canale?



Come strutturare un processo efficace

E' importante prima di tutto fissare **chi gestisce cosa?**

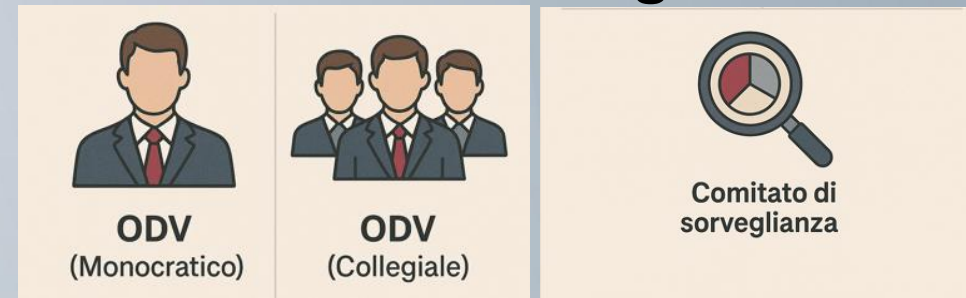
- Identificare ed elencare i canali di segnalazione
- Stabilire a chi sono destinatari delle segnalazione e le loro nomine
- Stabilire come devono essere gestite le segnalazioni
- Prevedere la gestione dei casi di conflitto di interesse
- Approfondire e prevedere specifica attribuzione delle responsabilità al trattamento dei dati, per i soggetti destinatari delle segnalazioni

Come strutturare un processo efficace

- **Canali di segnalazione:**



- **I destinatari delle segnalazione**



Nomine e Regolamento

- Dettagliare **come** devono essere **gestite le segnalazione** considerando anche i casi di conflitto di interesse

“In presenza di conflitto di interessi effettivo o potenziale, il soggetto designato deve astenersi e informare immediatamente l'organo di controllo, che provvederà alla nomina di un sostituto.”

Perché è un tema manageriale - Processo

Fase	Descrizione sintetica	Attori coinvolti	Finalità di governance
1. Accesso al canale	Il segnalante accede al canale interno (web, voce, cartaceo) e avvia la segnalazione, in forma anonima o identificata.	Dipendenti, terzi, stakeholder	Favorire la trasparenza e l'accessibilità del sistema
2. Presa in carico formale	La segnalazione è ricevuta da soggetti autorizzati (es. RPCT, ODV). Entro 7 giorni si invia ricevuta al segnalante.	Gestore segnalazioni, ODV, RPCT	Garantire tracciabilità, tempestività e responsabilità
3. Valutazione preliminare (ammissibilità)	Verifica di ricevibilità: competenza, coerenza, completezza delle informazioni.	Gestore segnalazioni	Evitare strumentalizzazioni, assicurare correttezza del processo
4. Istruttoria / approfondimento	Raccolta documenti, interviste, valutazione di merito. Eventuale attivazione audit interno.	RPCT, ODV, HR, Compliance, Internal Audit	Gestione imparziale, proporzionale e protetta della segnalazione
5. Feedback al segnalante	Entro 3 mesi dalla conferma di ricezione, si comunica l'esito (anche parziale) dell'istruttoria.	Gestore segnalazioni	Rafforzare fiducia nel sistema e accountability
6. Risoluzione e chiusura	Azioni correttive o disciplinari, segnalazione archiviata secondo GDPR. Tracciamento nel registro segnalazioni.	Direzione, HR, Audit, Legale	Prevenzione, monitoraggio e miglioramento continuo
7. Reporting e controllo	Redazione di report anonimi, statistiche per CDA/ODV/ANAC. Revisione periodica del canale.	CDA, ODV, RPCT, DPO	Misurare l'efficacia del sistema, prevenire rischi, garantire trasparenza



Perché è un tema manageriale – Aree di rischio

Area di rischio	Descrizione
Accessibilità del canale	Rischio che i potenziali segnalanti non conoscano o non si fidino del canale
Tutela dell'anonimato	Rischio di esposizione dell'identità del segnalante o del contenuto della segnalazione
Presa in carico ritardata	Rischio di non rispettare i tempi previsti (7 giorni ricevuta, 3 mesi feedback)
Mancata tracciabilità del processo	Rischio di gestione informale, con documenti non protetti o attività non registrate
Conflitto di interessi	Rischio che la segnalazione sia presa in carico da persone coinvolte o non indipendenti
Ritorsioni o percezione di ritorsioni	Rischio che il segnalante subisca o percepisca svantaggi dopo la segnalazione
Data breach / cybersecurity	Rischio di accessi non autorizzati alle informazioni raccolte
Inadeguatezza dei ruoli e delle competenze	Rischio che RPCT/ODV non siano formati o aggiornati sul trattamento delle segnalazioni

Perché è un tema manageriale – Conflitto di interesse

Situazione	Descrizione	Perché è un conflitto
Segnalazione contro un dirigente che fa parte dell'ODV	Il segnalato è membro dell'organismo che dovrebbe valutare la segnalazione	Coincidenza tra controllore e controllato
Responsabile del canale è in rapporto gerarchico con il segnalato	L'RPCT o il gestore della segnalazione è sovraordinato/subordinato al soggetto segnalato	Potenziale alterazione dell'obiettività
Coinvolgimento di familiari del gestore o del segnalato	Il segnalato è parente del valutatore o del referente	Rischio di favoritismo o accanimento
Segnalazione contro un soggetto con potere su budget/formazione del gestore	Il gestore teme ripercussioni future se agisce contro il segnalato	Pressione psicologica o auto-censura
Gestione delle segnalazioni affidata a chi ha interessi nel contratto in discussione	Un appalto è oggetto della segnalazione e il valutatore è coinvolto nel procedimento	Rischio di tutela di interessi propri o dell'ente

Prevedere un art. del regolamento del comitato di sorveglianza: "In presenza di conflitto di interessi effettivo o potenziale, il soggetto designato deve astenersi e informare immediatamente l'organo di controllo, che provvederà alla nomina di un sostituto."

Affidare la gestione ad **advisor esterni**, avvocati o consulenti, **nei casi di segnalazioni ad alta sensibilità interna**, come quelle verso top management o CDA



Come strutturare un processo efficace

Altra cosa molto importante è costruire la **fiducia nel canale**

- Comunicare e rendere disponibile la policy
- Comunicare e rendere disponibili procedure e/o note operative
- Informare / Formare il personale

E per la **parte tecnologica?**

- Identificare la soluzione applicative
- Prevedere una DPIA
- Descrivere, eseguire e documentare i casi di test
- Approfondire tutte le tematiche Privacy in relazione alla soluzione tecnologica e rivalutare le responsabilità al trattamento dei dati degli Amministratori di Sistema.

Soluzioni applicative



Prodotto Opensource

Sviluppatore: Hermes Center for Transparency and Digital Human Rights (Italia)
Licenza: AGPLv3 (open source)

Descrizione: Piattaforma robusta per la raccolta di segnalazioni anonime e riservate. Supporta la crittografia end-to-end, l'invio sicuro via Tor e HTTPS.

Conformità: pienamente aderente alla Direttiva (UE) 2019/1937 e al D.Lgs. 24/2023.

Caratteristiche principali:

- Interfaccia web personalizzabile
- Protezione dell'identità del segnalante
- Supporto multilingua
- Gestione multi-canale e multi-ente

Adozione: utilizzato da ANAC per la piattaforma WhistleblowingPA.it

Sito ufficiale: <https://www.globaleaks.org>

Codice sorgente: <https://github.com/globaleaks/GlobaLeaks>

Soluzioni applicative



Prodotto Opensource

Sviluppatore: Freedom of the Press Foundation (USA)

Licenza: GNU GPLv3 **Descrizione:** Soluzione progettata per giornalismo investigativo e ONG, ma adattabile anche a contesti whistleblowing aziendali.

Caratteristiche:

- Crittografia forte (PGP)

- Anonimato garantito **tramite Tor**

- Flussi di comunicazione unidirezionali

Limitazioni: meno orientato alla gestione formale del workflow (assenza di pannelli gestionali avanzati). Non è presente un'interfaccia gestionale per assegnare ruoli (es. RPCT, ODV), tracciare lo stato o creare registri.

Sito ufficiale: <https://securedrop.org>

Codice sorgente:

<https://github.com/freedomofpress/securedrop>

Soluzioni applicative



Considerazioni normative e di sicurezza

I prodotti **GlobaLeaks** e **SecureDrop** sono gli unici prodotti **open source** effettivamente maturi e mantenuti con aggiornamenti regolari, e possono essere considerati affidabili per contesti corporate o pubblici.

In particolare, GlobaLeaks: è stato scelto da enti pubblici italiani (ANAC, Comuni, Università, Regioni) è **compliant al GDPR**, alla **Direttiva UE 2019/1937** e supporta l'integrazione con i flussi previsti dal **D.Lgs. 24/2023** consente anche integrazione con SPID/CIE e logica multi-tenant.

Punto di attenzione :

Infrastrutture Hardware
Infrastrutture di Rete
Responsabile DBA

Soluzioni applicative

ENIS Integrity Line


MY GOVERNANCE
ZUCCHETTI

Requisito

Anonimato facoltativo garantito
Gestione sicura dati personali (GDPR)
Crittografia dati e audit log
Canale interno + tracciamento stato segnalazione
Flussi separati RPCT / ODV
Accesso web sicuro
Hosting UE o su richiesta Italia
Configurazione ruoli e livelli di accesso
Reportistica / registri
Integrazione con policy aziendale

Conformità dichiarata



Soluzioni applicative

Caratteristica	GlobaLeaks (Open Source)	EQS Integrity Line	My Whistleblowing
Conformità D.Lgs. 24/2023	✓ Sì	✓ Sì	✓ Sì
Conformità Direttiva UE 2019/1937	✓ Sì	✓ Sì	✓ Sì
Conformità GDPR	✓ Alta	✓ Alta	✓ Alta
Anonimato segnalante (nativo)	✓ Totale (Tor, no log)	✓	✓
Ruoli personalizzabili (es. RPCT, ODV)	✓ Avanzato	✓ Avanzato	✓ Avanzato
Pannello gestione segnalazioni	✓ Base/Personalizzabile	✓ Avanzato	✓ Avanzato
Flusso workflow (presa in carico, indagine)	✓ Personalizzabile (ma manuale)	✓ Sì	✓ Sì
Audit log / tracciamento eventi	✓ Sì	✓ Sì	✓ Sì
Canali multipli (web, posta, voce, telefono)	✓ Web/Cartaceo	✓ Completo	✓ Completo
Integrazione SPID/CIE	✓ Opzionale	✓ (su richiesta)	✓ (su richiesta)
Lingue disponibili	✓ Multilingua	✓ > 40 lingue	✓ Multilingua
Dashboard e reportistica	⚠ Limitata	✓ Avanzata	✓ Avanzata
Hosting	On-premise / Cloud EU	Cloud UE / On-premise	Cloud IT/EU / On-premise
Certificazioni sicurezza (es. ISO 27001)	⚠ Nessuna nativa	✓ ISO 27001, 27017	✓ ISO 27001, 9001, 22301
Licenza	✓ AGPLv3	✗ Proprietaria	✗ Proprietaria
Costi licenza	✓ Nessuno	📁 Medio-alto	📁 Medio
Manutenzione / Supporto tecnico	⚠ Richiede IT interno	✓ Incluso	✓ Incluso
Target ideale	PA, ONG, PMI, grandi aziende	Multinazionali, enti PA	PMI, partecipate, PA



Caso 1: Azienda industriale

Contesto: impresa con oltre 800 dipendenti, attiva nel settore manifatturiero avanzato.

Problema: l'azienda aveva avviato un canale di segnalazione interno, gestito dal Comitato Etico.

Tuttavia, nei primi mesi non era arrivata alcuna segnalazione



Caso 1: Azienda industriale

Accessibilità: canale presente ma scarsamente pubblicizzato.

Chiarezza: le policy erano disponibili ma poco conosciute dai dipendenti.

Tempestività: assente, in quanto il processo non era ancora testato.

Riservatezza: percezione di rischio personale elevata.

Integrazione: il canale non era legato stato operativamente al Modello .



Caso 1: Azienda industriale

Soluzione:

- Campagna informativa interna a firma dell'Amministratore Delegato
- Workshop con HR e tecnici per spiegare le garanzie di anonimato
- Simulazione di segnalazione per testare il canale

Risultato: nei sei mesi successivi, cinque segnalazioni pertinenti, di cui due legate a carenze operative rilevanti.



Caso 2: Data breach sistema Whistleblowing

Ecco i dettagli accertati dal Garante per la protezione dei dati sul data breach legato alla segnalazione whistleblowing presso l'Aeroporto Guglielmo Marconi di Bologna:

Violazioni riscontrate: Mancanza di crittografia

Il canale di segnalazione operava ancora in HTTP, senza protezione TLS/SSL, sia in transito sia a riposo.

Ciò ha compromesso l'integrità e la riservatezza dei dati sensibili dei segnalanti

Logging non autorizzato

Il sistema tracciava indirizzi IP, username e attività di navigazione, contravvenendo ai principi di “privacy by design” e “privacy by default” del GDPR.



Caso 2: Data breach sistema Whistleblowing

Assenza di DPIA (Data Protection Impact Assessment)

Non è stata condotta alcuna valutazione d'impatto per identificare e mitigare i rischi legati al trattamento dei dati sensibili raccolti tramite la piattaforma whistleblowing.

Sanzioni comminate

€ 40.000 all'Aeroporto Guglielmo Marconi di Bologna (titolare del trattamento)

€ 20.000 al fornitore software responsabile (ex art. 28 GDPR)

Lezioni e requisiti da adottare

Per garantire la conformità normativa e la sicurezza del whistleblowing, le organizzazioni devono:

- Utilizzare HTTPS/TLS e crittografia a riposo sui dati raccolti.
- Limitare i log ai dati strettamente necessari, escludendo IP e navigation logs
- Effettuare la DPIA obbligatoria per piattaforme di segnalazione dati
- Stabilire accordi chiari con i fornitori, garantendo misure tecniche e organizzative adeguate come richiesto dall'art. 28 del GDPR .

Q&A



GRAZIE PER L'ATTENZIONE

Dott.ssa Annalisa Quintavalle

*Senior Consultant
Governance, Compliance e Sistemi*

Annalisa.quintavalle@gmail.com

mob.: +39 34834999082

LinkedIn www.linkedin.com/in/annalisa-quintavalle