

## Whistleblowing: le nuove regole privacy che ogni azienda o ente deve conoscere

Scopri le novità 2025 su whistleblowing e privacy: rischi, obblighi, DPIA e misure richieste dal Garante nelle nuove Linee guida ANAC.

(Fonte: <https://www.lavoroediritti.com/> 3 dicembre 2025)



### Indice:

- [Che cos'è il whistleblowing](#)
- [Perché il parere è così rilevante](#)
- [I principali punti di attenzione evidenziati dal Garante](#)
- [Indicazioni anche per i datori di lavoro privati](#)
- [Un sistema più robusto e coerente](#)
- [Conclusione](#)

Il Garante della Privacy interviene sulla disciplina del whistleblowing in Italia. Con il [provvedimento n. 581 del 9 ottobre 2025](#), il Garante per la protezione dei dati personali ha espresso un articolato parere sugli schemi di Linee guida ANAC dedicati sia ai **canali interni** di segnalazione sia all'aggiornamento delle Linee guida sul **canale esterno**. La newsletter del 27 novembre 2025 ne ha anticipato i punti essenziali, confermando l'importanza di una gestione delle segnalazioni più uniforme, sicura e rispettosa della privacy di tutte le persone coinvolte.

Il quadro che emerge è chiaro: i canali di whistleblowing diventano sempre più un vero e proprio presidio di tutela dei diritti, ma richiedono un salto di qualità nelle misure tecniche e organizzative adottate da enti pubblici e imprese private.

### **Che cos'è il whistleblowing**

Il **whistleblowing** è il processo attraverso il quale una persona - tipicamente un dipendente o collaboratore, pubblico o privato - segnala violazioni, irregolarità o comportamenti illeciti di cui è venuta a conoscenza nel proprio contesto lavorativo.

La finalità non è la denuncia anonima indiscriminata, ma la tutela dell'interesse pubblico e dell'integrità dell'organizzazione. La normativa vigente garantisce protezioni specifiche al segnalante, evitando ritorsioni e assicurando la massima riservatezza della sua identità e del contenuto della segnalazione.

**Leggi anche:** [Whistleblowing, gli adempimenti per evitare le sanzioni](#)

### **Perché il parere è così rilevante**

Nel parere ufficiale il Garante sottolinea che le Linee guida di ANAC hanno un impatto diretto sulla protezione dei dati personali trattati nei processi di segnalazione.

La normativa di riferimento - in particolare il D.lgs. 24/2023 - impone che **la riservatezza dell'identità del segnalante, delle persone menzionate e del contenuto della segnalazione sia garantita in ogni fase**. Il parere richiama numerosi punti tecnici del decreto, evidenziando gli obblighi degli enti e l'importanza di definire in modo chiaro ruoli, responsabilità, processi di gestione e misure di sicurezza.

### **I principali punti di attenzione evidenziati dal Garante**

#### **1. Posta elettronica? Un canale troppo rischioso**

Sia la newsletter sia il parere sottolineano che l'uso della semplice email come canale di segnalazione **espone a rischi significativi di tracciamento e perdita della riservatezza**. Le piattaforme dedicate, invece, consentono cifratura, separazione dei ruoli e riduzione delle impronte digitali riconducibili al segnalante, in linea con l'orientamento già espresso dal Garante.

#### **2. Obbligo di svolgere la valutazione di impatto (DPIA)**

Il parere ribadisce che i trattamenti connessi alla gestione delle segnalazioni rientrano tra quelli che richiedono **l'obbligo di una valutazione di impatto sulla protezione dei dati**. La DPIA deve essere svolta prima dell'attivazione del canale e coinvolgere anche eventuali responsabili del trattamento, come fornitori di piattaforme software.

### 3. Tempi di conservazione chiari e limitati

Le Linee guida ribadiscono i limiti già previsti dal D.lgs. 24/2023: **non oltre cinque anni dalla comunicazione dell'esito finale della procedura**. Una misura necessaria per evitare la conservazione ingiustificata di informazioni altamente sensibili.

### 4. Condivisione del canale: sì, ma con estrema cautela

Il decreto prevede che alcuni enti - ad esempio piccoli comuni o PMI sotto i 249 dipendenti - possano **condividere il canale di segnalazione interna**. Il Garante chiarisce che, in tali casi, devono essere adottate **misure tecniche e organizzative robuste** per impedire che un ente possa accedere alle segnalazioni destinate a un altro.

### 5. L'importanza delle piattaforme informatiche

Le Linee guida evidenziano che l'uso di piattaforme informatiche consente maggiori garanzie: cifratura, accessi segregati, documentazione dei processi, possibilità di mantenere un dialogo riservato con il segnalante.

Il parere ricorda che tali strumenti devono essere **affidabili, adeguatamente progettati e valutati attraverso la DPIA**.

### Indicazioni anche per i datori di lavoro privati

La newsletter chiarisce che le Linee guida sui canali interni non riguardano solo la pubblica amministrazione: *forniscono indicazioni e principi che i datori di lavoro potranno tenere in considerazione nell'attivazione dei propri canali*.

Tra le misure raccomandate rientrano:

- evitare la tracciabilità del segnalante che accede dalla rete interna,
- definire ruoli e autorizzazioni in modo rigoroso,
- adottare procedure formalizzate per la gestione delle segnalazioni,
- garantire che solo personale autorizzato tratti i dati.

Un approccio in linea con il principio di **accountability**, che richiede ai titolari del trattamento di dimostrare in modo documentato la conformità alla normativa.

### Un sistema più robusto e coerente

La collaborazione tra ANAC e Garante, evidente nel parere e richiamata nella newsletter, punta a creare un ecosistema di segnalazione più **sicuro, coerente e affidabile**.

Le nuove Linee guida, che recepiscono molti degli orientamenti espressi dal Garante, rappresentano un passo avanti nel bilanciamento tra:

- **efficacia dei canali di whistleblowing,**
- **protezione della riservatezza,**

- **correttezza del trattamento dei dati personali.**

La sfida per enti pubblici e aziende sarà ora **tradurre questi principi in procedure concrete**, investendo in piattaforme adeguate, formazione specializzata e governance dei processi.

## **Conclusione**

Il [parere del 9 ottobre 2025](#) e la successiva newsletter confermano che il whistleblowing non è solo uno strumento anticorruzione, ma un sistema complesso che richiede **tecnologia sicura, processi strutturati e profonda attenzione alla privacy.**

Per datori di lavoro pubblici e privati, il messaggio è inequivocabile:

***l'attivazione di un canale di segnalazione non può essere trattata come un adempimento formale, ma come un processo critico che richiede competenze, strumenti e responsabilità precise.***