MY GOVERNANCE
WE DIGITIZE YOUR COMPANY

ZUCCHETTI

GUIDA OPERATIVA — WHISTLEBLOWING

Open source vs software commerciale

Vantaggi e criticità alla luce della normativa italiana

Aggiornato a **maggio 2026**

D.Lgs. 24/2023 · Delibera ANAC 478/2025

Perché questo documento

Quando si valuta uno strumento per il whistleblowing, prima o poi emerge la domanda: perché non usare una soluzione open source? La domanda è legittima, e merita una risposta altrettanto diretta.

La distinzione che conta non è tra open source e software commerciale. È tra soluzione **autogestita** e soluzione **gestita da un fornitore**, con tutto ciò che questo implica sul piano della responsabilità, degli aggiornamenti normativi e del presidio tecnico.

Cosa funziona nell'open source

GlobaLeaks, il software open source di riferimento per il whistleblowing, implementa alcuni requisiti tecnici fondamentali: cifratura dei dati, gestione dei conflitti di interesse nel flusso delle segnalazioni, audit trail delle operazioni. Il codice è pubblicamente verificabile, il che è un vantaggio reale in termini di trasparenza.

L'open source come tecnologia funziona. **L'autogestione dell'open source è un'altra cosa**.

Le quattro criticità dell'autogestione

1. IL CANALE ORALE NON È INCLUSO NELLA VERSIONE STANDARD

Le Linee Guida ANAC n. 1/2025 prevedono che le organizzazioni soggette al D.Lgs. 24/2023 debbano mettere a disposizione almeno una modalità di segnalazione orale. GlobaLeaks ha sviluppato questa funzionalità, ma non è inclusa nella versione gratuita né nelle versioni standard: è disponibile solo nelle versioni personalizzate a pagamento, gestite da un fornitore.

Chi installa GlobaLeaks in autonomia deve risolvere il canale orale con strumenti esterni, una linea telefonica dedicata, una casella vocale separata, e inserire manualmente nella piattaforma quanto emerge dalla segnalazione orale. È un carico organizzativo aggiuntivo che aumenta il rischio di gestione non conforme.

2. IL RESPONSABILE DEL TRATTAMENTO EX ART. 28 GDPR NON ESISTE

Con un software commerciale, il fornitore viene nominato responsabile del trattamento ai sensi dell'art. 28 GDPR: c'è un contratto, ci sono obblighi definiti in caso di data breach, c'è una catena di responsabilità formalizzata.

Con l'autogestione open source, questo fornitore non esiste. La responsabilità tecnica ricade sull'IT interno, che gestisce dati personali sensibili senza le garanzie contrattuali richieste dalla normativa.

> **ATTENZIONE**
>
> Nel 2022 il Garante Privacy ha sanzionato un'azienda e il suo fornitore software per mancata regolamentazione dei rapporti tra responsabili del trattamento nella gestione delle segnalazioni whistleblowing. Non basta che il software funzioni: la catena di responsabilità deve essere formalizzata.

3. GLI AGGIORNAMENTI NORMATIVI SONO A CARICO DELL'ORGANIZZAZIONE

Con un software commerciale, l'adeguamento agli aggiornamenti normativi è un obbligo contrattuale del fornitore. Con l'autogestione open source, il monitoraggio normativo, la valutazione dell'impatto tecnico e l'implementazione delle modifiche sono tutti a carico dell'organizzazione, con competenze giuridiche e tecniche che raramente convivono nella stessa funzione interna.

Il rischio concreto è la **deriva silente**: la normativa cambia, la piattaforma rimane ferma, e l'organizzazione non se ne accorge fino a un controllo esterno.

4. IL SUPPORTO ALLA DPIA È ASSENTE

Per condurre la valutazione d'impatto sulla protezione dei dati, il DPO ha bisogno della documentazione tecnica dell'infrastruttura. Con un software commerciale questa documentazione è prodotta dal fornitore. Con l'autogestione open source deve essere costruita internamente, spesso ricostruendo a posteriori un'installazione non documentata.

IN SINTESI

Le criticità dell'open source autogestito non riguardano la qualità del software. Riguardano la catena di responsabilità, il presidio degli aggiornamenti normativi e la capacità di documentare gli adempimenti privacy. Sono criticità organizzative, non tecniche.

Il confronto in sintesi

Aspetto	Open source autogestito	Software commerciale
Canale orale integrato	Solo versioni personalizzate (a pagamento)	Incluso
Responsabile del trattamento art. 28 GDPR	Assente — ricade sull'IT interno	Fornitore nominato con contratto
Aggiornamenti normativi	A carico dell'organizzazione	Obbligo contrattuale del fornitore
Documentazione per la DPIA	Da costruire internamente	Fornita dal vendor su richiesta
SLA di disponibilità del canale	Nessuna garanzia formale	Definita contrattualmente
Costo iniziale	Basso o nullo	Canone periodico
Costo di presidio nel tempo	Elevato (risorse IT e legali interne)	Incluso nel servizio

La domanda giusta prima di decidere

La domanda non è "quanto costa la licenza?", ma: **chi si assume la responsabilità di tenere il sistema conforme nel tempo?**

Se la risposta è chiara, documentata e sostenibile con le risorse disponibili, la scelta può andare in qualsiasi direzione. Se la risposta è vaga, il risparmio sul canone iniziale si trasforma in un costo nascosto, operativo e sanzionatorio.

> § **RIFERIMENTO NORMATIVO**
>
> D.Lgs. 24/2023, art. 4 (requisiti del canale interno) e art. 14 (protezione dei dati personali). Delibera ANAC 478/2025, requisiti tecnici del canale. GDPR, art. 28 (responsabile del trattamento) e art. 35 (valutazione d'impatto).

maggio 2026

My Governance - Zucchetti

Soluzioni Legal Tech per la compliance aziendale

www.mygovernance.it