

Whistleblowing e MOG 231: canali interni sotto esame ANAC

SINTESI OPERATIVA

Le indicazioni ANAC sul whistleblowing impongono a imprese ed enti di dimostrare che il canale interno funziona, non soltanto che esista. La procedura deve individuare gestore e sostituto, consentire segnalazioni scritte o orali, assicurare riservatezza, protezione dei dati, tracciabilità e riscontro nei tempi previsti. Il sistema va coordinato con il MOG 231, l'Organismo di vigilanza e il sistema disciplinare, prevenendo ritorsioni e gestendo segnalazioni anonime. Servono formazione, report e regole per gruppi: piattaforma e casella, da sole, non bastano.

[Articolo originale](#)

LEGGI ONLINE

Le nuove indicazioni ANAC sul whistleblowing costringono imprese, enti e consulenti a spostare l'attenzione dal documento alla sostanza. Non basta più avere una procedura interna, una piattaforma digitale o una casella riservata. Serve un sistema che funzioni davvero, con ruoli chiari, tempi presidiati, tracciabilità, protezione dei dati personali e collegamento effettivo con il modello organizzativo 231.

Il passaggio è meno formale di quanto sembri. Il canale interno di segnalazione entra nel cuore degli assetti organizzativi. Tocca la governance, il sistema disciplinare, i flussi verso l'Organismo di vigilanza, i rapporti con le organizzazioni sindacali e, nei gruppi, anche il modo in cui capogruppo e controllate si dividono compiti e responsabilità.

Il rischio, per molte imprese, è credere di essere già coperte perché nel 2023 è stata acquistata una piattaforma o approvata una policy. È una certezza fragile. Le nuove Linee Guida mostrano che la conformità non si misura solo sulla presenza del canale, ma sulla sua integrazione nei processi aziendali.

IL QUADRO NORMATIVO DI PARTENZA

La disciplina italiana del whistleblowing è contenuta nel d.lgs. 10 marzo 2023, n. 24, adottato in attuazione della direttiva UE 2019/1937. Il decreto ha riunito in un unico testo la protezione delle persone che segnalano violazioni del diritto dell'Unione e delle disposizioni normative nazionali.

Il sistema non riguarda soltanto il settore pubblico. Coinvolge anche il settore privato, con un impatto particolare sulle società che hanno adottato un modello di organizzazione e gestione ai sensi del d.lgs. 231/2001.

Le Linee Guida ANAC del 2025 si inseriscono in questo quadro. La delibera n. 478 del 26 novembre 2025 riguarda i canali interni di segnalazione. La delibera n. 479 dello stesso giorno interviene invece sulle segnalazioni esterne, modificando e integrando il precedente impianto della delibera n. 311 del 12 luglio 2023.

Il dato più rilevante è il cambio di prospettiva. Superata la prima fase di adeguamento, l'Autorità punta ora alla qualità del sistema. Il canale interno deve essere accessibile, sicuro, riservato e gestito da soggetti realmente autonomi.

Da qui nasce un effetto pratico. Le imprese che avevano già adottato una procedura devono chiedersi se quella procedura sia ancora coerente con le nuove indicazioni. Non sempre lo è.

CHI DEVE DOTARSI DEL CANALE INTERNO

Nel settore privato, l'obbligo di attivare un canale interno riguarda diversi soggetti. Rientrano, in primo luogo, le imprese che hanno impiegato nell'ultimo anno una media di almeno 50 lavoratori subordinati.

Vi rientrano poi gli enti che operano in specifici settori regolati dal diritto dell'Unione, anche sotto la soglia dei 50 lavoratori. Si pensi, ad esempio, a determinati ambiti finanziari, alla prevenzione del riciclaggio, alla sicurezza dei trasporti o alla tutela ambientale.

Un capitolo autonomo riguarda gli enti che adottano modelli 231. Anche le realtà di minori dimensioni devono coordinare il sistema di segnalazione con il modello organizzativo, perché il whistleblowing è ormai uno degli strumenti attraverso cui il modello intercetta violazioni, anomalie e comportamenti contrari ai presidi di controllo.

Qui si apre un equivoco frequente. Alcune piccole società pensano che il tema whistleblowing non le riguardi se hanno meno di 50 dipendenti. Non è sempre così. Se hanno adottato un MOG 231, oppure operano in settori specifici, devono affrontare il problema in modo serio.

WHISTLEBLOWING E MOG 231

La keyword whistleblowing e MOG 231 intercetta il punto più delicato per le società già strutturate sul piano della compliance. Il canale interno non può restare una procedura separata, magari caricata sul sito e richiamata genericamente dal modello.

Il MOG 231 deve recepire la disciplina delle segnalazioni. Deve indicare il canale utilizzato, i soggetti competenti, le modalità di gestione e i rapporti con l'Organismo di vigilanza. Deve poi aggiornare il sistema disciplinare, includendo il divieto di ritorsione e il divieto di ostacolare la segnalazione.

Questa integrazione incide anche sull'efficacia del modello. Non perché ANAC possa sostituirsi al giudice nella valutazione dell'idoneità del MOG 231. Ma perché un modello che ignora o gestisce male il whistleblowing mostra una debolezza organizzativa evidente.

Si pensi a una società con codice etico, protocolli 231 e OdV nominato. Se la procedura whistleblowing non spiega come segnalare una violazione del codice etico, oppure non chiarisce quando l'OdV debba ricevere informazioni, il sistema rischia di frammentarsi.

Il modello deve quindi contenere almeno alcune informazioni essenziali: compiti del gestore, canali disponibili, tempi procedurali, criteri di ammissibilità, gestione dei conflitti, sostituzione del gestore, flussi verso l'OdV, conservazione dei dati e raccordo con il sistema disciplinare.

IL COINVOLGIMENTO DEI SINDACATI

L'art. 4, comma 1, del d.lgs. 24/2023 prevede che i soggetti obbligati attivino i canali di segnalazione dopo aver sentito le rappresentanze o le organizzazioni sindacali.

Non si tratta di una procedura di codecisione. L'impresa non deve ottenere un accordo. Deve però informare preventivamente i soggetti sindacali, consentendo loro di formulare osservazioni.

Secondo l'impostazione richiamata dalle Linee Guida, l'informativa deve precedere l'approvazione dell'atto organizzativo o dell'aggiornamento del MOG 231. Deve essere inviata in tempo utile, con un termine congruo per le eventuali osservazioni.

Quando in azienda sono presenti RSA o RSU, l'interlocuzione passa da tali rappresentanze. In assenza di rappresentanze interne, occorre rivolgersi alle organizzazioni territoriali delle associazioni sindacali più rappresentative sul piano nazionale.

Nella pratica, il passaggio andrebbe documentato con particolare attenzione. È opportuno conservare l'invio dell'informativa, il testo trasmesso, le eventuali osservazioni ricevute e il verbale di un incontro, se svolto. Non per burocrazia. Per dimostrare che il confronto è avvenuto prima della decisione aziendale.

SITUAZIONE AZIENDALE	SOGGETTO DA INFORMARE
Presenza di RSA	Rappresentanze sindacali aziendali presenti nell'ente.
Presenza di RSU	Rappresentanza sindacale unitaria, con eventuale coordinamento interno.
Assenza di RSA e RSU	Organizzazioni territoriali delle associazioni sindacali più rappresentative.

SITUAZIONE AZIENDALE	SOGGETTO DA INFORMARE
Aggiornamento del MOG 231	Informativa preventiva prima dell'approvazione della modifica.

CANALE SCRITTO E CANALE ORALE

Uno degli errori più frequenti riguarda la forma della segnalazione. Il decreto prevede che le segnalazioni possano essere effettuate in forma scritta, anche con modalità informatiche, oppure in forma orale.

L'alternativa è una facoltà del segnalante. Non dell'ente. Di conseguenza, una procedura che consenta solo l'invio tramite piattaforma informatica può risultare incompleta, se non prevede anche una modalità orale.

La forma scritta può essere gestita tramite piattaforma, posta cartacea riservata, doppia busta o posta elettronica con misure adeguate. La forma orale può avvenire tramite linea telefonica, messaggistica vocale o incontro diretto.

L'incontro diretto deve essere richiesto dal segnalante. Può svolgersi anche presso l'ente, purché siano garantite riservatezza e protezione dell'identità. Non serve creare un luogo simbolicamente esterno. Serve evitare che l'accesso al colloquio renda riconoscibile il segnalante.

Qui il dettaglio operativo pesa molto. Se l'incontro avviene in una stanza vicina all'ufficio del personale, in orari visibili a tutti, la riservatezza è solo teorica. La procedura deve quindi prevedere modalità concrete di appuntamento, verbalizzazione e custodia degli atti.

PIATTAFORMA INFORMATICA E DOPPIA BUSTA

ANAC conferma una preferenza per le piattaforme informatiche. La ragione è comprensibile. Una piattaforma ben progettata protegge meglio l'identità del segnalante, consente dialoghi riservati e riduce la circolazione incontrollata di documenti.

La piattaforma, però, non è obbligatoria in assoluto. L'ente può adottare strumenti diversi, purché idonei a garantire la riservatezza dell'identità del segnalante, della persona coinvolta, dei soggetti menzionati e del contenuto della segnalazione.

Se si sceglie una piattaforma, occorre valutare seriamente il fornitore. Non basta una scheda commerciale. Servono verifiche sulle misure di sicurezza, sulla gestione degli accessi, sulle certificazioni, sulla localizzazione dei dati, sui tempi di conservazione e sulle modalità di cancellazione.

La doppia busta resta praticabile. In questo caso la procedura dovrebbe spiegare come comporre l'invio, chi riceve fisicamente la busta, dove viene protocollata e chi può aprirla. Le Linee Guida valorizzano anche il principio di minimizzazione: non va richiesta automaticamente copia del documento di identità.

La posta elettronica ordinaria o certificata merita prudenza. Può essere usata, ma solo con misure di contenimento del rischio. Una PEC aziendale accessibile a più persone, magari usata anche per altre comunicazioni, non appare coerente con la logica del canale riservato.

PRIVACY E VALUTAZIONE DEL RISCHIO

Il whistleblowing è anche un trattamento di dati personali ad alto impatto organizzativo. Le segnalazioni possono contenere dati comuni, dati particolari, informazioni giudiziarie, valutazioni soggettive e documenti aziendali sensibili.

Per questo la procedura non deve essere scritta solo dal consulente 231. Deve dialogare con la documentazione privacy. Occorre verificare informativa, registro dei trattamenti, ruoli del fornitore, autorizzazioni interne, misure tecniche e tempi di conservazione.

Quando la piattaforma o il gestore esterno trattano dati per conto dell'ente, il rapporto deve essere regolato ai sensi dell'art. 28 GDPR. Devono essere disciplinati oggetto, durata, natura del trattamento, categorie di dati, misure di sicurezza e istruzioni del titolare.



Nei casi più delicati, la DPIA diventa uno strumento quasi inevitabile. Non perché ogni canale richieda automaticamente una valutazione d'impatto. Ma perché il rischio sulla riservatezza del segnalante e dei soggetti coinvolti è elevato, soprattutto in strutture piccole.

Una procedura formalmente corretta ma priva di presidi privacy rischia di collassare alla prima segnalazione complessa. Basta un inoltro improprio, un accesso non autorizzato o un allegato salvato in una cartella condivisa.

IL GESTORE DELLA SEGNALEZIONE

Il gestore non è il destinatario passivo di un modulo. È il soggetto che prende in carico la segnalazione, verifica i presupposti, interloquisce con il segnalante, svolge l'istruttoria e fornisce riscontro.

L'art. 4, comma 2, del d.lgs. 24/2023 consente di affidare la gestione a una persona interna, a un ufficio autonomo dedicato o a un soggetto esterno. In ogni caso servono autonomia, imparzialità e formazione specifica.

La formazione non può ridursi a una breve sessione introduttiva. Il gestore deve conoscere la disciplina whistleblowing, i principi privacy, le tecniche minime di istruttoria, i limiti della propria funzione e la struttura aziendale.

La conoscenza dell'ente è centrale. Un gestore esterno che non sa come funzionano reparti, deleghe, procure, flussi approvativi e processi sensibili può ricevere la segnalazione, ma faticherà a capirla.

Per questo, nei contratti di affidamento esterno, è utile prevedere incontri periodici, accesso all'organigramma, elenco dei referenti interni e procedure di escalation. Senza questi elementi, l'esternalizzazione diventa un outsourcing cieco.

ORGANO DI INDIRIZZO E REPORT AGGREGATI

Le Linee Guida chiariscono il rapporto tra gestore e organo di indirizzo. Il gestore deve restare autonomo nella gestione della segnalazione e nell'istruttoria. L'organo di indirizzo non deve interferire con il singolo procedimento.

Questo non significa assenza totale di flussi. L'organo amministrativo deve poter monitorare il funzionamento complessivo del sistema. Può quindi ricevere report periodici, aggregati e, quando opportuno, anonimizzati.

Il report non dovrebbe contenere dettagli inutili. Dovrebbe indicare numero delle segnalazioni, canali utilizzati, tempi medi di gestione, esiti, aree aziendali coinvolte in forma non identificativa e criticità procedurali.

Un flusso annuale può essere sufficiente nelle realtà più piccole. In contesti più complessi, soprattutto nei gruppi o nelle società vigilate, può essere opportuno un monitoraggio semestrale.

La logica è semplice: l'organo di indirizzo deve sapere se il sistema funziona, non chi ha segnalato cosa. Confondere questi due piani è pericoloso.

CONFLITTO DI INTERESSI E SOSTITUTO

Il conflitto di interessi è uno dei punti più sottovalutati. Può accadere che il gestore sia coinvolto nella segnalazione, sia vicino alla persona segnalata o abbia un interesse nella vicenda.

La procedura deve prevedere cosa succede in questi casi. Non può deciderlo dopo, quando la segnalazione è già arrivata. Occorre individuare a monte un sostituto, oppure una modalità alternativa di gestione.

Se il gestore è un organo collegiale, può essere sufficiente l'astensione del solo componente in conflitto. Se invece il gestore è monocratico, la presenza del sostituto diventa essenziale.

Le Linee Guida richiamano anche l'ipotesi dell'assenza prolungata del gestore, superiore a 7 giorni. Il sistema deve continuare a funzionare. Il termine di 7 giorni per l'avviso di ricevimento non aspetta il rientro dalle ferie.

Per le piccole imprese il tema è più complicato. Se non è possibile nominare un sostituto per carenza di personale, occorre almeno spiegare la soluzione adottata. In alcuni casi la segnalazione potrà essere indirizzata al canale esterno ANAC.



I DPO E GESTORE

La coincidenza tra DPO e gestore non è vietata in modo assoluto. Ma non può essere scelta per comodità.

Negli enti grandi o complessi, la sovrapposizione rischia di compromettere il pieno esercizio di entrambe le funzioni. Il DPO vigila, consiglia e controlla la conformità privacy. Il gestore conduce l'istruttoria sulla segnalazione.

La distinzione dei ruoli evita equivoci. Se il DPO diventa anche gestore, può trovarsi a valutare un trattamento che egli stesso contribuisce a realizzare operativamente. Il rischio non è sempre insuperabile, ma va misurato.

Nelle imprese piccole, invece, la stessa persona può ricoprire entrambi i ruoli se la scelta è motivata. La motivazione dovrebbe considerare dimensione aziendale, carenza di personale, carico di lavoro, misure di segregazione e assenza di conflitti.

Una soluzione intermedia può essere utile: DPO e gestore appartengono allo stesso studio o società di consulenza, ma sono persone diverse. In tal caso non vi è coincidenza soggettiva. Resta però da verificare l'autonomia effettiva.

I LE FASI DELLA PROCEDURA

L'art. 5 del d.lgs. 24/2023 scandisce la gestione della segnalazione con tempi precisi. Il gestore deve rilasciare avviso di ricevimento entro 7 giorni. Deve mantenere le interlocuzioni con il segnalante. Deve dare diligente seguito. Deve fornire riscontro entro 3 mesi.

La sequenza operativa può essere letta in cinque passaggi: ricezione, avviso, verifica preliminare, istruttoria, riscontro finale o intermedio.

L'avviso di ricevimento non implica alcuna valutazione sul merito. Serve solo a comunicare che la segnalazione è stata ricevuta e presa in carico.

La verifica preliminare serve invece a capire se la segnalazione rientra nel perimetro del whistleblowing. Occorre valutare soggetto segnalante, contesto lavorativo, oggetto della violazione e sufficiente circostanziazione dei fatti.

Se i presupposti mancano, la segnalazione può essere trattata come ordinaria e trasmessa all'ufficio competente, se previsto dalla procedura. Il segnalante va informato di questo passaggio.

L'istruttoria deve essere proporzionata. Non tutte le segnalazioni richiedono un'indagine complessa. Alcune possono essere archiviate perché manifestamente infondate. Altre richiedono acquisizione di documenti, colloqui, analisi di procedure interne e coinvolgimento di funzioni specialistiche.

FASE	ATTENZIONE OPERATIVA
Ricezione	Garantire riservatezza del segnalante, del segnalato e del contenuto.
Avviso entro 7 giorni	Confermare la presa in carico senza anticipare valutazioni di merito.
Esame preliminare	Verificare presupposti soggettivi, oggettivi e sufficiente precisione dei fatti.
Istruttoria	Svolgere verifiche proporzionate, documentate e coerenti con la procedura.
Riscontro entro 3 mesi	Comunicare archiviazione, trasmissione interna o valutazione del fumus.
Conservazione	Cancellare segnalazione e documentazione entro il termine massimo di 5 anni.

I RISCONTRO AL SEGNALANTE

Il riscontro entro 3 mesi è spesso frainteso. Non sempre coincide con la chiusura definitiva di ogni accertamento interno. Può anche rappresentare un aggiornamento sull'esito della valutazione svolta fino a quel momento.

Il gestore deve però dire qualcosa di utile. Non basta una formula generica del tipo "la segnalazione è in corso di valutazione", ripetuta senza contenuto.



Il riscontro può indicare l'archiviazione, la trasmissione agli organi competenti, l'avvio di ulteriori verifiche o una valutazione preliminare di plausibilità. Va sempre evitata la comunicazione di dettagli che possano violare la riservatezza di altri soggetti.

È opportuno che la procedura preveda modelli di comunicazione. Non per rendere tutto automatico. Piuttosto per evitare risposte improvvisate, eccessive o troppo povere.

■ SEGNALAZIONI ANONIME

Le segnalazioni anonime rappresentano un terreno delicato. ANAC lascia spazio alla scelta dell'ente. La procedura può stabilire che siano trattate come whistleblowing, se sufficientemente circostanziate, oppure come segnalazioni ordinarie.

La scelta va esplicitata. Non può essere affidata alla valutazione caso per caso senza criteri.

Una segnalazione anonima circostanziata può contenere elementi utili: date, nomi, documenti, riferimenti a contratti, ordini, pagamenti o procedure violate. In tal caso ignorarla sarebbe poco prudente.

Una segnalazione anonima generica, invece, non diventa rilevante solo perché passa dal canale whistleblowing. Se mancano fatti verificabili, il gestore non ha una base istruttoria seria.

La regola pratica dovrebbe essere questa: l'anonimato non basta a escludere la valutazione, ma la genericità sì.

■ SEGNALAZIONI INVIATE A PIÙ SOGGETTI

Un altro caso frequente riguarda la segnalazione inviata a più destinatari. Può accadere che il segnalante scriva al gestore, all'amministratore delegato, al responsabile HR e magari anche a un dirigente.

Se i destinatari sono tutti interni all'ente, la segnalazione ricevuta da soggetti non competenti deve essere inoltrata al gestore entro 7 giorni. Il segnalante deve esserne informato.

La segnalazione sarà trattata come whistleblowing se il segnalante dichiara di voler beneficiare delle relative tutele, oppure se tale volontà emerge chiaramente dal contenuto.

Più complesso è il caso dell'invio anche a soggetti esterni. Qui si pone il dubbio della divulgazione pubblica. Le Linee Guida indicano di chiedere chiarimenti al segnalante.

Questo punto resta fragile. Da un lato, è corretto evitare automatismi penalizzanti. Dall'altro, l'invio esterno può rompere la gradualità dei canali. La procedura dovrebbe quindi trattare espressamente questa ipotesi.

■ UNICITÀ DEL CANALE E ODV

ANAC raccomanda un canale unico idoneo a ricevere tutte le segnalazioni rientranti nel decreto, comprese quelle relative a condotte illecite rilevanti ai sensi del d.lgs. 231/2001 o a violazioni del MOG 231.

La raccomandazione ha senso. Due canali separati possono creare confusione. Il segnalante potrebbe non sapere se una condotta vada inviata al canale 231 o al canale whistleblowing.

Il doppio canale non è vietato in modo assoluto. Ma deve essere molto ben spiegato. Altrimenti genera incertezza, duplicazioni e problemi di riservatezza.

Se l'OdV è nominato gestore, riceve le segnalazioni e le tratta secondo la procedura whistleblowing. Se invece il gestore è un soggetto diverso, il MOG 231 deve regolare i flussi informativi tra gestore e OdV.

Il flusso deve essere calibrato. L'OdV ha bisogno delle informazioni necessarie a vigilare sul modello, non necessariamente dell'intero fascicolo. In molti casi possono bastare informazioni aggregate, anonimizzate o selezionate.

Il rischio opposto è svuotare l'OdV. Se il gestore trattiene ogni informazione su violazioni del modello, l'organismo non può svolgere la propria funzione. Serve equilibrio, non sovrapposizione.



SISTEMA DISCIPLINARE E RITORSIONI

L'aggiornamento del sistema disciplinare è uno degli snodi più concreti. Il modello 231 deve prevedere conseguenze per chi viola la procedura, ostacola la segnalazione, compie ritorsioni o viola gli obblighi di riservatezza.

Le ritorsioni possono assumere forme diverse. Licenziamento, demansionamento, trasferimento, esclusione da progetti, valutazioni negative immotivate, pressioni indirette. A volte non si presentano come ritorsioni. Sembrano normali decisioni organizzative.

Per questo la procedura dovrebbe prevedere un presidio anche successivo alla segnalazione. Non basta proteggere l'identità nel momento dell'invio. Occorre monitorare eventuali effetti negativi sul segnalante e sui soggetti protetti.

La tutela si estende, in determinate condizioni, anche a facilitatori, colleghi, parenti e soggetti collegati. Questo aspetto deve essere compreso dalle funzioni HR e dai responsabili di linea.

Un sistema disciplinare generico, limitato alla violazione del codice etico, non è sufficiente. Deve parlare il linguaggio della disciplina whistleblowing.

COMUNICAZIONE INTERNA ED ESTERNA

La procedura deve essere conosciuta. Non basta approvarla in consiglio di amministrazione o allegarla al MOG 231.

Le informazioni sul canale devono essere esposte e facilmente accessibili nei luoghi di lavoro, sul sito internet e, se presente, sulla intranet aziendale. Devono essere comprensibili anche a consulenti, fornitori, collaboratori e partner commerciali.

Per gli enti dotati di MOG 231, la pubblicazione sul sito è utile ma non sempre sufficiente. Le Linee Guida valorizzano anche la trasmissione a fornitori, consulenti, collaboratori e partner. Nella prassi, questo passaggio può essere gestito con clausole contrattuali, allegati o informative dedicate.

Il linguaggio deve essere chiaro. Una procedura scritta solo per specialisti scoraggia la segnalazione e aumenta gli errori di indirizzamento.

Una buona comunicazione dovrebbe spiegare cosa si può segnalare, cosa non rientra nel canale, quali tutele esistono, quali sono i tempi e chi gestisce la procedura.

GRUPPI SOCIETARI

Nei gruppi di imprese, la questione diventa più tecnica. Il decreto consente ai soggetti privati che hanno impiegato una media di lavoratori subordinati non superiore a 249 di condividere il canale interno e la relativa gestione.

Il calcolo della soglia va effettuato a livello di singola impresa. Non si deve sommare automaticamente il personale dell'intero gruppo per stabilire se la singola società possa condividere il canale.

La condivisione del canale richiede una piattaforma unica ma ramificata. In pratica, devono esistere sotto-canali autonomi per ciascuna società. Ogni ente resta responsabile della propria segnalazione e deve avere il proprio gestore.

Per le imprese sopra i 249 dipendenti, la condivisione non è ammessa. Resta però possibile l'esternalizzazione della gestione. In questo caso il gestore può essere la capogruppo, una controllata o un soggetto terzo.

La differenza non è solo nominale. Condivisione significa piattaforma comune con articolazioni autonome. Esternalizzazione significa affidamento della gestione a un soggetto esterno all'ente, attraverso un contratto.

SOLUZIONE	CARATTERISTICHE PRINCIPALI
Condivisione del canale	Ammessa per imprese fino a 249 dipendenti, con piattaforma ramificata e sotto-canali autonomi.
Esternalizzazione	Ammessa anche per imprese sopra 249 dipendenti, con affidamento della gestione a un soggetto terzo.



SOLUZIONE	CARATTERISTICHE PRINCIPALI
Capogruppo come gestore	Possibile mediante contratto di servizio o affidamento, con ruoli e responsabilità definiti.
Privacy	Il soggetto che gestisce per conto dell'ente opera di regola come responsabile del trattamento.

CONTRATTO CON IL GESTORE ESTERNO

L'esternalizzazione richiede un contratto. Non basta una delibera del consiglio, una lettera di incarico generica o una procedura di gruppo.

Il contratto deve indicare attività affidate, poteri del gestore, obblighi di riservatezza, tempi di gestione, flussi informativi, misure di sicurezza, responsabilità privacy e modalità di restituzione o cancellazione dei dati.

Se il gestore esterno è la capogruppo, il contratto resta necessario. Il rapporto infragruppo non elimina l'esigenza di disciplinare ruoli e responsabilità.

ANAC può valutare anche l'idoneità della scelta. Se l'ente affida la gestione a un soggetto manifestamente privo di competenze, autonomia o misure adeguate, la responsabilità dell'ente non viene meno.

È un passaggio che merita attenzione. L'outsourcing non trasferisce la responsabilità organizzativa. La rende solo più complessa da presidiare.

ESEMPIO PRATICO SU UNA PMI CON MOG 231

Si consideri una società manifatturiera con 85 dipendenti, MOG 231 adottato nel 2021 e OdV monocratico. Nel 2023 la società ha acquistato una piattaforma whistleblowing e ha pubblicato una procedura sul sito.

A prima vista il sistema sembra adeguato. Poi emergono i problemi. La procedura prevede solo la segnalazione scritta tramite piattaforma. Non disciplina il canale orale. L'informativa sindacale non è stata inviata prima dell'approvazione. Il gestore coincide con il responsabile HR, che potrebbe essere coinvolto in segnalazioni su personale e ritorsioni.

Il MOG 231 contiene un rinvio generico al whistleblowing. Non aggiorna il sistema disciplinare. Non chiarisce il rapporto tra gestore e OdV. Non prevede un sostituto del gestore in caso di conflitto o assenza.

In questo scenario non occorre demolire l'impianto. Occorre correggerlo. La società dovrebbe integrare il canale orale, rivedere la nomina del gestore, introdurre un sostituto, aggiornare il MOG 231 e documentare il coinvolgimento sindacale.

Dovrebbe anche regolare i flussi verso l'OdV. Ad esempio, trasmissione immediata delle segnalazioni 231 rilevanti, report periodico aggregato e accesso controllato agli atti solo quando necessario.

ESEMPIO PRATICO SU UN GRUPPO SOCIETARIO

Si immagini un gruppo composto da una capogruppo con 310 dipendenti e tre controllate, ciascuna sotto i 120 dipendenti. La capogruppo vorrebbe usare un'unica piattaforma e gestire tutte le segnalazioni centralmente.

La soluzione va costruita con cautela. Le controllate sotto soglia possono condividere il canale, con sotto-canali autonomi. La capogruppo, avendo più di 249 dipendenti, non può semplicemente condividere il canale nello stesso modo.

Può però assumere il ruolo di gestore esterno per le controllate, se vi è un contratto di affidamento. Oppure può esternalizzare essa stessa la gestione a un soggetto terzo. In ogni caso, ogni società deve mantenere consapevolezza delle segnalazioni di propria competenza.

Sul piano privacy, le autorizzazioni devono impedire accessi trasversali non necessari. Il gestore non deve vedere tutto per abitudine. Deve vedere ciò che serve per gestire la segnalazione dell'ente interessato.

Il punto critico, nei gruppi, è la falsa centralizzazione. Semplifica sulla carta. Ma può violare prossimità, autonomia e riservatezza.



CHECKLIST DI ADEGUAMENTO

AREA	DOMANDA DI CONTROLLO
Perimetro soggettivo	L'ente rientra tra i soggetti obbligati per dipendenti, settore regolato o MOG 231?
Informativa sindacale	È stata inviata prima dell'approvazione della procedura o dell'aggiornamento del modello?
Canale scritto	La modalità scritta garantisce riservatezza, tracciabilità e accessi limitati?
Canale orale	Sono previste linea telefonica, messaggistica vocale o incontro diretto?
Piattaforma	È stata svolta una due diligence sul fornitore e sulle misure di sicurezza?
Gestore	Autonomia, imparzialità, formazione e conoscenza dell'ente sono documentate?
Conflitti	La procedura prevede astensione, sostituto e gestione dell'assenza oltre 7 giorni?
DPO	L'eventuale cumulo con il ruolo di gestore è motivato e sostenibile?
OdV	I flussi tra gestore e OdV sono definiti senza violare la riservatezza?
Sistema disciplinare	Sono previste sanzioni per ritorsioni, ostacoli e violazioni della riservatezza?
Privacy	Informativa, registro, nomine, DPIA e tempi di conservazione sono coerenti?
Gruppi	È chiara la differenza tra condivisione del canale ed esternalizzazione?



STUDIO PIZZANO
COMMERCIALISTA E REVISORE LEGALE

STUDIO SABATINO PIZZANO

Sede: via Sant'Alessio, 5, 83030 Venticano (AV)
Contatti: info@studiopizzano.it • dev.studiopizzano.it

***Nota informativa:** Il presente approfondimento ha scopo puramente informativo e divulgativo alla data di redazione (12/05/2026). Per la trattazione di casistiche specifiche si raccomanda il ricorso a una consulenza professionale personalizzata.*



Studio
Sabatino
Pizzano
2022
via
Sant'Alessio,
5,
83030
Venticano

STUDIO PIZZANO