ANDERSEN

giugno 2026

&Compliance Risk Management

Novità normative e pratiche di governance dei dati e di gestione di rischi d'impresa

Paola Finetto
Partner
paola.finetto@it.andersen.com

Luca Rigotti
Partner
luca.rigotti@it.andersen.com

Hanno collaborato: **Nicolò Bottura**, **Elisa D'Arrigo** e **Edoardo Vittorio Lazzaro**

D.Lgs. 231/2001

ODV e IA: controlli integrati e sempre più stringenti

A quasi tre anni dall'entrata in vigore del D.Lgs. 24/2023, molte organizzazioni continuano a sottovalutare gli obblighi introdotti dalla disciplina whistleblowing.
Tuttavia, l'istituzione di **canali di segnalazione conformi** e l'adozione di procedure adeguate non costituiscono meri adempimenti formali, bensì strumenti essenziali per la prevenzione degli illeciti e la tutela dell'integrità aziendale.

Le imprese tenute all'applicazione della normativa devono garantire la presenza di canali interni che assicurino la **riservatezza** dell'identità del segnalante, delle persone coinvolte e del contenuto della segnalazione, nonché definire un **processo** di gestione **chiaro**, **tracciabile** e **conforme** alla disciplina in materia di protezione dei dati personali.

Il mancato adeguamento può esporre l'ente a rilevanti conseguenze.
Il D.Lgs. 24/2023 attribuisce infatti all'ANAC il potere di irrogare **sanzioni amministrative pecuniarie** nei confronti delle organizzazioni che **omettano** di attivare i canali di segnalazione obbligatori o che adottino procedure non conformi ai requisiti di legge. Analoghe sanzioni possono essere applicate in presenza di comportamenti volti a ostacolare le segnalazioni o di misure ritorsive nei confronti dei whistleblower.

Accanto al rischio sanzionatorio, non devono essere trascurati gli **impatti reputazionali e organizzativi**.
L'assenza di un sistema efficace di segnalazione può infatti compromettere la capacità dell'ente di intercettare tempestivamente condotte illecite, irregolarità operative o violazioni normative, con possibili ricadute economiche e reputazionali.

Per le società dotate di Modello 231, inoltre, la conformità alla disciplina whistleblowing rappresenta un elemento essenziale del **sistema di controllo interno**.
Una verifica periodica dell'adeguatezza dei canali e delle procedure adottate costituisce pertanto una buona prassi di governance e compliance, oltre che un presidio fondamentale per la prevenzione dei rischi.

Privacy | AI | Cyber

Gestione delle segnalazioni e trattamento dei dati personali: il rischio di data breach è sempre più concreto!

La gestione delle segnalazioni (**whistleblowing**) comporta nuove e complesse sfide per la sicurezza aziendale, posizionando la protezione dei dati personali in cima alle priorità.

In questo scenario, il rischio di un data breach non è più un'ipotesi remota, ma una minaccia concreta. Le segnalazioni, infatti, possono contenere, oltre ai dati personali comuni (dati identificativi del segnalante e del segnalato), anche **categorie particolari di dati personali** (c.d. "dati sensibili") come dettagli su presunti illeciti, nomi di soggetti coinvolti, prove documentali, dati relativi alla salute nonché, a titolo esemplificativo, dati relativi a orientamenti sessuali, opinioni politiche, filosofiche, religiose. Se questi dati vengono sottratti a causa di **accessi non autorizzati, attacchi informatici o banalmente per un errore umano**, le conseguenze per l'organizzazione sono rilevanti.

Un data breach può comportare non solo pesanti **sanzioni pecuniarie** da parte dell'Autorità Garante per la privacy, ma anche **danni reputazionali** che minano la fiducia dei dipendenti e degli stakeholder. Resta inteso che nessun lavoratore utilizzerà i canali di segnalazione se teme che la propria identità possa essere esposta. Per mitigare questo rischio, le aziende devono adottare un approccio basato sulla "privacy by design e by default". È fondamentale implementare **canali di comunicazione criptati**, limitare l'accesso ai soli soggetti formalmente autorizzati e formare costantemente il personale addetto alla gestione delle segnalazioni.

Occorre altresì ricordare che in caso di violazione dei dati, il Regolamento Europeo (GDPR) impone l'obbligo di notifica all'Autorità di controllo **entro 72 ore dal momento in cui si viene a conoscenza dell'evento** se il rischio per i diritti e le libertà delle persone è elevato. Solo attraverso una **governance** rigorosa, sistemi IT criptati e una cultura aziendale orientata alla **sicurezza** dei dati e delle informazioni è possibile trasformare la gestione delle segnalazioni in un valore sicuro, riducendo così il rischio di violazioni dei dati.

Risk Management

Segnalazioni infondate: i rischi per il segnalante

Il sistema di **whistleblowing** rappresenta uno strumento fondamentale per favorire la trasparenza e prevenire illeciti all'interno delle organizzazioni.

La tutela riconosciuta al segnalante non è però illimitata: le protezioni previste dalla legge non si applicano a chi effettua una segnalazione infondata con **dolo o colpa grave**.

Sul piano interno, l'azienda può avviare un **procedimento disciplinare** per l'utilizzo scorretto del canale di segnalazione, fino all'applicazione delle sanzioni previste dal sistema disciplinare aziendale.

Sul piano civile, il soggetto segnalato potrebbe agire per ottenere il **risarcimento dei danni** provocati dalla segnalazione infondata.

Le segnalazioni infondate, inoltre, potrebbero integrare le fattispecie penali di **diffamazione** o **calunnia**.

Per i delitti sopra indicati, in caso di **condanna** in sede penale o di accertamento della sua responsabilità in sede civile, il segnalante **perde le tutele** previste dalla normativa whistleblowing e viene altresì irrogata una sanzione disciplinare.

Il canale di segnalazione non richiede la certezza dell'illecito, ma presuppone che il segnalante agisca in **buona fede**, sulla base di informazioni attendibili e verificabili.

Utilizzare il canale whistleblowing per finalità ritorsive, personali o strumentali significa esporsi a **rischi** che possono essere ben più gravi dei benefici che la normativa riconosce a chi segnala correttamente.