ANDERSEN

settembre 2025

&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**, **Fabio Cecilia**, **Elisa D'Arrigo**

ANDERSEN

settembre 2025

&Compliance Risk Management

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

D.Lgs. 231/2001

Il MOG 231 come fulcro del sistema di compliance integrato

Il Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001 (MOG 231) rappresenta oggi uno strumento centrale non solo per prevenire la responsabilità amministrativa dell'ente, ma anche come elemento cardine di un più ampio **sistema di compliance integrato**.

In un contesto normativo in continua evoluzione, le imprese sono chiamate a garantire **trasparenza, correttezza e sostenibilità** nelle proprie attività.
Il MOG 231, con la sua struttura di mappatura dei rischi, procedure di controllo e sistemi disciplinari, diventa la base su cui costruire un **approccio unitario alla gestione della conformità**: dalla tutela della salute e sicurezza sul lavoro alla protezione dei dati personali, dalla prevenzione della corruzione fino agli impegni ESG.

Integrare il Modello 231 con policy aziendali, codici etici, sistemi di gestione certificati e canali di whistleblowing significa creare un unico framework in grado di ridurre i rischi, migliorare la governance e rafforzare la fiducia di clienti, partner e istituzioni.

Il MOG 231 non è quindi un adempimento formale, ma il **fulcro di una cultura aziendale basata sull'etica e sulla responsabilità**, che trasforma la compliance da obbligo a opportunità strategica per la crescita sostenibile dell'impresa.

ANDERSEN

settembre 2025

&Compliance Risk Management

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

Privacy | AI | Cyber

NIS2 e IA: come rendere resiliente l'azienda in termini di privacy e cybersecurity

In un contesto dove l'intelligenza artificiale (IA) sta assumendo un ruolo sempre più centrale, l'adeguamento alla direttiva NIS2, recepita in Italia con il D.Lgs. 138/2024, costituisce un'opportunità concreta per aumentare la resilienza e garantire un livello elevato di **sicurezza informatica** all'interno dell'azienda.

Se da un lato la NIS2 impone **requisiti stringenti** in materia di risk management, risposta agli incidenti, business continuity e governance della cybersecurity, dall'altro l'adozione di sistemi di IA può supportare l'organizzazione, ottimizzando la capacità di prevedere le minacce e automatizzare le risposte. Tuttavia, è fondamentale che l'IA venga utilizzata in modo etico e responsabile, nonché in conformità alla normativa in materia di protezione dei dati personali.
Un'**integrazione consapevole tra NIS2, AI ACT e GDPR** consentirebbe di sviluppare sistemi di IA privacy compliant, capaci di garantire alti standard di sicurezza, riducendo i tempi di reazione agli attacchi. Per creare un sistema di compliance integrato, è però fondamentale adottare una strategia di governance efficace e un approccio risk based.

Questo si traduce nel valutare i **rischi cyber e privacy** derivanti dall'utilizzo di determinati sistemi (e strumenti) di IA, implementare delle procedure aziendali chiare e trasparenti, e **alfabetizzare le persone** attraverso una formazione specifica in ambito cyber.

Elemento imprescindibile rimane comunque l'apporto multidisciplinare delle funzioni aziendali interne che, se comunicano correttamente, possono davvero fare la differenza.

ANDERSEN

settembre 2025

&Compliance Risk Management

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

Risk Management

La norma UNI 11961: il ponte tra il MOG 231 e la ISO 37301

La norma UNI 11961:2024, "Linee guida per l'integrazione del sistema di gestione per la compliance UNI ISO 37301:2021 a supporto dei Modelli Organizzativi di Gestione e Controllo e degli Organismi di Vigilanza in conformità al D.Lgs.231/2001", rappresenta una svolta significativa nel contesto della compliance aziendale.

Questa norma, pubblicata il 17 dicembre 2024, fornisce **linee guida utili e pragmatiche per integrare i Modelli 231**, oltre che l'attività di verifica propria degli Organismi di Vigilanza, con **il Sistema di Gestione per la Compliance** secondo la UNI ISO 37301:2021.

L'obiettivo principale della UNI 11961 è guidare un **approccio strutturato, integrato e coerente nella gestione dei rischi di non conformità** e, di conseguenza, favorire controlli interni sistematici ed efficaci, oltre che opportunamente documentati. La norma si propone, pertanto, di efficientare sia l'attività di analisi dei rischi, che gli audit interni, riducendo le duplicazioni nelle attività ispettive e, al contempo, aumentando la tracciabilità e l'accountability delle azioni di prevenzione, in una prospettiva di miglioramento continuo.

In sintesi, la norma in esame propone specifiche **modalità operative per la costruzione, il mantenimento e l'implementazione** di Modelli Organizzativi solidi ed efficaci, oltre che idonei, in concreto, a prevenire la commissione di illeciti 231, con conseguente efficacia esimente del Modello per l'ente stesso.