NUMERO 01 – MARZO 2026 NEWSLETTER TRIMESTRALE

FOCUS COMPLIANCE

AGGIORNAMENTI NORMATIVI E INDICAZIONI OPERATIVE PER LA GESTIONE DEI RISCHI AZIENDALI

Nota informativa

La presente newsletter viene trasmessa esclusivamente a imprese e organizzazioni che collaborano con COMPLIANCE SRL o che hanno richiesto di ricevere questo servizio informativo.

La comunicazione non ha finalità promozionali o di marketing, ma esclusivamente tecniche e informative, con l'obiettivo di condividere aggiornamenti normativi e indicazioni operative utili per le aziende.

Per tali ragioni la presente comunicazione rientra nelle attività informative rivolte a soggetti professionali e non richiede un consenso esplicito, fermo restando che chiunque non desideri più riceverla potrà richiederne in qualsiasi momento la cancellazione.

In questo numero

DANIEL ZISA
FOUNDER, COMPLIANCE SRL

Mi chiamo Daniel Zisa e, insieme al team di COMPLIANCE SRL, ho il piacere di presentarvi il primo numero di Focus Compliance, una newsletter dedicata agli aggiornamenti normativi e alle principali evoluzioni in materia di governance, gestione dei rischi e compliance aziendale.

Negli ultimi anni il quadro normativo che riguarda imprese e organizzazioni è diventato sempre più articolato e dinamico. Temi come protezione dei dati personali, responsabilità amministrativa degli enti, whistleblowing, cybersecurity e gestione dei rischi organizzativi richiedono oggi un monitoraggio costante e un approccio strutturato alla compliance.

Con questa newsletter ci impegneremo, numero dopo numero, a tenervi aggiornati su ciò che accade nel panorama normativo italiano ed europeo, selezionando gli sviluppi più rilevanti e offrendo alcune indicazioni operative utili per comprenderne gli impatti sulle organizzazioni.

L'obiettivo di Focus Compliance è quello di fornire uno strumento informativo chiaro e sintetico, capace di aiutare imprese e professionisti a orientarsi in un contesto normativo in continua evoluzione.

In questo primo numero troverete alcuni approfondimenti dedicati, tra gli altri temi, alle nuove Linee guida ANAC in materia di whistleblowing, agli aggiornamenti relativi alla normativa 231/2001, alle implicazioni operative della Direttiva NIS2, nonché ad alcune opportunità per le imprese legate al Rating di Legalità.

Con l'auspicio che questo strumento possa risultare utile, vi auguriamo buona lettura.

Daniel Zisa

Videosorveglianza e geolocalizzazione dei lavoratori: limiti e obblighi per le aziende

L'utilizzo di sistemi tecnologici nei contesti lavorativi – come **telecamere di videosorveglianza o dispositivi di geolocalizzazione** installati sui veicoli aziendali – è sempre più diffuso nelle organizzazioni, spesso per finalità di sicurezza, tutela del patrimonio aziendale o gestione delle attività operative.

Il tema è stato oggetto, negli ultimi anni, di diversi interventi da parte del Garante per la protezione dei dati personali, che hanno ribadito la necessità di garantire un corretto equilibrio tra le esigenze organizzative dell'impresa e la tutela dei diritti dei lavoratori.

Tali strumenti possono infatti comportare una **raccolta sistematica di dati** relativi all'attività dei dipendenti, configurando in alcuni casi una forma di **controllo a distanza** dell'attività lavorativa.

Per questo motivo la normativa italiana prevede specifiche garanzie.

In particolare, ai sensi dell'art. 4 dello **Statuto dei Lavoratori**, l'installazione di strumenti dai quali possa derivare un controllo sull'attività lavorativa è consentita solo previo **accordo con le rappresentanze sindacali**, oppure in loro assenza, previa **autorizzazione dell' Ispettorato Territoriale del Lavoro.**

Oltre agli aspetti lavoristici, l'utilizzo di questi sistemi deve rispettare anche i principi previsti dal **Regolamento europeo sulla protezione dei dati (GDPR)**, tra cui trasparenza, minimizzazione dei dati e informazione chiara ai lavoratori.

Una corretta progettazione dei sistemi di monitoraggio consente alle imprese di conciliare le esigenze organizzative con la tutela dei diritti dei dipendenti, riducendo il rischio di contestazioni e sanzioni.

Cosa verificare in azienda

- Verificare se gli impianti di videosorveglianza o geolocalizzazione possano comportare un controllo sull'attività lavorativa
- Accertare la presenza di accordo sindacale o autorizzazione dell'Ispettorato del Lavoro ove necessario
- Verificare che i lavoratori abbiano ricevuto informativa privacy aggiornata
- Verificare la corretta regolamentazione interna dell'utilizzo di tali strumenti (policy aziendali, regolamenti interni, procedure)

Whistleblowing: nuove Linee guida ANAC e centralità della formazione

Nel dicembre 2025 l'Autorità Nazionale Anticorruzione (**ANAC**) ha pubblicato **nuove Linee guida operative sui canali interni di segnalazione**, con l'obiettivo di supportare enti pubblici e imprese nell'applicazione del D.Lgs. 24/2023 in materia di whistleblowing.

Il documento integra le indicazioni già fornite nel 2023 e nasce dall'analisi delle principali criticità emerse nella fase iniziale di applicazione della normativa, tra cui difficoltà organizzative nella gestione delle segnalazioni e scarsa conoscenza degli strumenti da parte dei lavoratori.

Tra gli aspetti più rilevanti evidenziati dalle nuove linee guida vi sono:

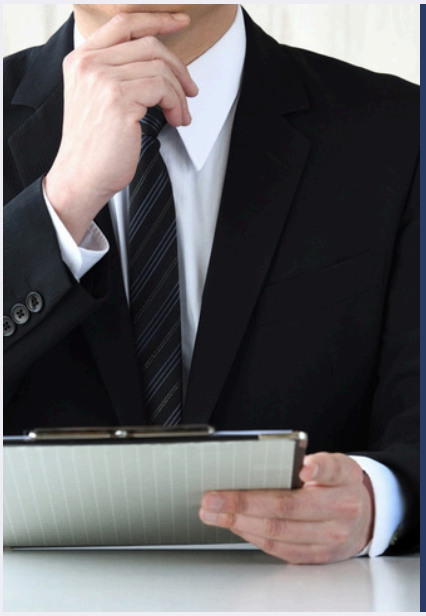
- la corretta **organizzazione del canale** interno di segnalazione;
- l'individuazione di un **gestore del canale** indipendente e adeguatamente formato;
- **l'integrazione del sistema whistleblowing** con codici etici, procedure interne e Modelli 231.

Particolare attenzione viene dedicata al tema della **formazione del personale**, considerata un elemento essenziale per garantire il corretto funzionamento del sistema di whistleblowing.

Secondo l'ANAC, infatti, non è sufficiente limitarsi a fornire una semplice informativa interna sull'esistenza dei canali di segnalazione, ma è necessario prevedere specifiche attività di formazione **a tutto il personale aziendale**, finalizzate a garantire che i lavoratori conoscano:

- l'**esistenza** dei canali di segnalazione messi a disposizione dall'azienda;
- le **modalità** corrette di utilizzo;
- le **tutele previste** per il segnalante, in particolare il divieto di atti ritorsivi.

Particolare rilievo assume inoltre la formazione dei soggetti incaricati della gestione del canale, che dovrebbe essere adeguata e periodicamente aggiornata, al fine di garantire una gestione corretta e riservata delle segnalazioni.



Cosa verificare in azienda

- Presenza di un canale interno di segnalazione conforme al D.Lgs. 24/2023
- Individuazione di un gestore del canale con adeguata autonomia e formazione
- Aggiornamento di codice etico, procedure interne e Modello 231
- Pianificazione di attività di formazione sul whistleblowing per tutto il personale aziendale

Normativa 231: la mappatura di rischi e reati nel Modello Organizzativo

Il sistema di responsabilità amministrativa degli enti previsto dal **D.Lgs. 231/2001** continua ad evolversi attraverso l'introduzione di nuove fattispecie di reato presupposto e l'ampliamento di quelle già esistenti.

Nel corso degli ultimi anni il catalogo dei reati rilevanti ai fini della responsabilità dell'ente si è progressivamente ampliato, includendo ambiti sempre più rilevanti per la vita delle imprese, tra cui **reati tributari, ambientali, informatici e fattispecie legate alla sicurezza sul lavoro e alla corruzione**.

Più recentemente, interventi normativi tra il 2025 e l'inizio del **2026** hanno introdotto ulteriori fattispecie, tra cui i reati legati alla **violazione delle misure restrittive dell'Unione europea** (sanzioni internazionali), che possono incidere in particolare sulle imprese che operano con partner o mercati esteri.

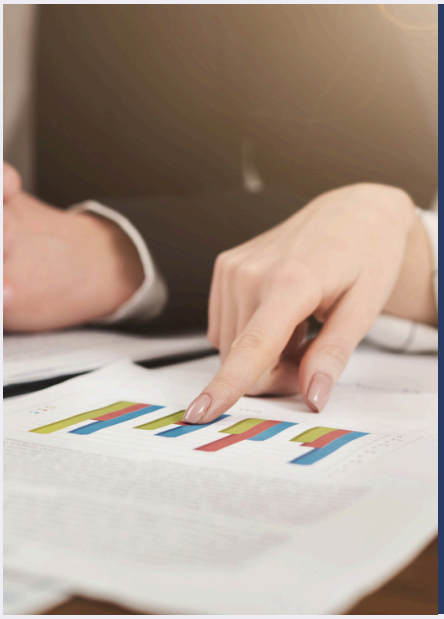
In questo contesto, il **Modello di Organizzazione, Gestione e Controllo** rappresenta lo strumento principale attraverso il quale l'ente può dimostrare di aver adottato misure idonee a prevenire la commissione di reati nel proprio ambito organizzativo.

Per questa ragione il Modello 231 non può essere considerato un **documento statico**, ma deve essere aggiornato alla luce:

- delle modifiche normative;
- dell'evoluzione della giurisprudenza e delle prassi applicative;
- di cambiamenti interni (attività, mercati, modifiche della struttura societaria).

L'introduzione o l'estensione di nuove fattispecie di reato presupposto può rendere necessario procedere a una **revisione della mappatura dei rischi** aziendali, all'aggiornamento dei protocolli interni e alla verifica dell'efficacia dei sistemi di controllo previsti dal Modello.

Un Modello organizzativo aggiornato non rappresenta soltanto uno strumento di tutela rispetto al rischio di responsabilità dell'ente, ma contribuisce anche a **rafforzare i sistemi di controllo interno e la cultura della compliance** all'interno dell'organizzazione.



Cosa verificare in azienda

- Verificare quando è stato adottato o aggiornato l'ultima volta il Modello 231
- Valutare se le recenti evoluzioni normative richiedono un aggiornamento della mappatura dei rischi
- Verificare la presenza di protocolli e procedure interne coerenti con le attività aziendali
- Accertare che l'Organismo di Vigilanza svolga attività di monitoraggio periodico e reporting

Direttiva NIS2: aggiornamenti sul portale ACN e percorso verso la piena conformità

La normativa europea in materia di cybersecurity ha introdotto nuovi obblighi per numerose organizzazioni attraverso la **Direttiva NIS2**, recepita nell'ordinamento italiano con l'obiettivo di rafforzare la **sicurezza delle infrastrutture digitali** e dei servizi essenziali.

Le imprese rientranti nel perimetro della normativa – tra cui operatori di servizi essenziali e soggetti considerati "importanti" – sono tenute ad adottare un approccio strutturato alla **gestione dei rischi informatici** e alla sicurezza delle proprie infrastrutture digitali.

Tra gli adempimenti previsti dalla disciplina rientra anche la registrazione e l'aggiornamento delle informazioni sul portale dell'Agenzia per la Cybersicurezza Nazionale (**ACN**), attraverso il quale le organizzazioni interessate devono comunicare alcuni dati rilevanti, come i punti di contatto per la sicurezza informatica e le informazioni relative ai servizi erogati.

Parallelamente, le organizzazioni coinvolte stanno affrontando il percorso verso la **piena conformità ai requisiti previsti dalla NIS2**, che richiede l'adozione di misure tecniche e organizzative adeguate alla gestione dei rischi cyber.

La NIS2 segna quindi un passaggio importante: la cybersecurity diventa sempre più un tema di **governance aziendale**, non solo tecnologico ma anche organizzativo e gestionale.

Ambiti maggiormente rilevanti

- **Rischi informatici**
  Gestione e analisi dei rischi informatici
- **Gestione incidenti**
  Procedure per la gestione degli incidenti di sicurezza
- **Catena di fornitura**
  Sicurezza della catena di fornitura digitale
- **Continuità operativa**
  Misure di continuità operativa e gestione delle crisi
- **Formazione**
  Attività di formazione e sensibilizzazione del personale

Cosa verificare in azienda

- Verificare se l'organizzazione rientra tra i soggetti interessati dalla normativa NIS2
- Controllare l'aggiornamento delle informazioni e dei contatti sul portale ACN
- Valutare l'adozione di un sistema strutturato di gestione dei rischi cyber
- Pianificare attività di formazione e sensibilizzazione sulla sicurezza informatica

Rating di Legalità: un'opportunità per valorizzare la compliance aziendale

Il **Rating di Legalità**, rilasciato dall'Autorità Garante della Concorrenza e del Mercato (AGCM), è uno strumento pensato per premiare le imprese che adottano comportamenti improntati a legalità, trasparenza e corretta gestione aziendale.

Il rating viene attribuito su richiesta dell'impresa ed è espresso attraverso un punteggio **da una a tre "stelle"**, che può essere utilizzato come elemento qualificante nei rapporti con banche, pubbliche amministrazioni e partner commerciali, ad esempio nell'accesso al credito o nella partecipazione a bandi pubblici.

Per ottenere il rating è necessario innanzitutto soddisfare alcuni **requisiti base**, legati principalmente all'assenza di condanne o violazioni rilevanti in ambito penale, fiscale o amministrativo.

Il punteggio può poi aumentare attraverso l'adozione di specifici **requisiti premiali**, che valorizzano la presenza di strumenti organizzativi e sistemi di controllo all'interno dell'azienda.

Tra gli elementi che possono contribuire ad aumentare il punteggio rientrano, ad esempio:

- **Modello 231**
  Adozione di un Modello di Organizzazione e Gestione ai sensi del D.Lgs. 231/2001
- **Anticorruzione**
  Adozione di sistemi di prevenzione della corruzione
- **Certificazioni**
  Possesso di certificazioni ambientali o sociali
- **Tracciabilità**
  Utilizzo di sistemi di tracciabilità dei pagamenti
- **White List**
  Iscrizione nelle White List prefettizie

AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO
AGCM
RATING DELLA LEGALITÀ ★++

Cosa verificare in azienda

- Verificare se l'impresa possiede i requisiti base per richiedere il Rating di Legalità
- Valutare la presenza di requisiti premiali (Modello 231, certificazioni, sistemi anticorruzione, ecc.)
- Analizzare se i presidi organizzativi già presenti possono contribuire ad aumentare il punteggio
- Verificare la possibilità di presentare o aggiornare la domanda presso l'AGCM

In molti casi le imprese **possiedono già diversi di questi presidi** organizzativi senza essere consapevoli della possibilità di ottenere il rating o di migliorarne il punteggio.

Il Rating di Legalità rappresenta quindi uno strumento che consente di **valorizzare gli investimenti** in compliance già effettuati, rafforzando al tempo stesso **la reputazione e l'affidabilità** dell'azienda sul mercato.

CONTATTI

info@compliance-srl.it
daniel.zisa@compliance-srl.it

www.compliance-srl.it

Nel prossimo numero

Nel prossimo numero di **Focus Compliance** continueremo a condividere aggiornamenti normativi e indicazioni operative sui principali temi di interesse per le imprese in materia di compliance, governance e gestione dei rischi aziendali.

Progressivamente, attraverso questa newsletter, avremo inoltre il piacere di **presentare i professionisti e i collaboratori che fanno parte del team di COMPLIANCE SRL**, illustrando le diverse competenze che contribuiscono alle attività di consulenza e supporto alle organizzazioni.

Compliance®
Smart Solutions