

COMPLIANCE



FOCUS

PRO

**Uno strumento pratico
per l'aggiornamento
e la formazione continua
sui temi della compliance**



VOLUME 1



S O M M A R I O

INTRODUZIONE DEL SERVIZIO	
LA COMPLIANCE INTEGRATA	6
RESPONSABILITÀ AMMINISTRATIVA	8
WHISTLEBLOWING	10
I SISTEMI DI CERTIFICAZIONE	12
SOSTENIBILITÀ E FATTORI ESG	14
PRIVACY	16





Introduzione del servizio

COSA È COMPLIANCE FOCUS PRO?

LO STRUMENTO DI FORMAZIONE CHE DÀ DEL TU AI DIPENDENTI

PERCHÉ SERVE ALLA TUA AZIENDA?

Non una semplice rivista, ma un **percorso formativo** e coinvolgente per i dipendenti che vogliono essere **aggiornati** con le ultime novità in materia di **compliance aziendale integrata**.

Cari,

siamo lieti di presentarvi **Compliance Focus Pro**, una guida approfondita e specializzata nel campo della compliance aziendale integrata. L'abbonamento permette un accesso privilegiato a informazioni utili sui temi della compliance, per una gestione e organizzazione aziendale che sia orientata al rispetto delle norme e dei regolamenti applicabili in materia.

Perché Compliance Focus Pro?

Compliance Focus Pro è uno strumento prezioso per tutti i **dipendenti** che desiderano svolgere il proprio lavoro in modo conforme alle normative e contribuire al successo dell'azienda. In un contesto normativo sempre più complesso, è fondamentale rimanere aggiornati.

CFPro vi fornisce le conoscenze e gli strumenti necessari per:

- **gestire e controllare i rischi in modo efficace**, tutelando la reputazione e il patrimonio aziendale;
- assicurare una gestione e organizzazione aziendale orientata al **rispetto delle norme**;
- **rimanere aggiornati** sulle ultime novità in materia di compliance.



"Il coraggio è la capacità di resistere alla paura, di dominare la paura."
- Mark Twain

Ogni pubblicazione si concentra su un tema specifico con un'esplorazione dettagliata e analitica, includendo anche **casi studio concreti** e **l'analisi di provvedimenti** che influenzano significativamente lo scenario attuale.

Questo primo numero offre una panoramica generale dei temi principali della compliance aziendale integrata. Introdurremo, in termini sintetici e puramente normativi, la definizione di compliance integrata, gli argomenti della **responsabilità amministrativa degli enti**, della **sostenibilità** e **certificazioni**, del **whistleblowing** e della **privacy**, riservandoci di approfondire criticamente ciascun ambito nei numeri che seguiranno.

Buona lettura a tutti!

La parola whistleblower è un termine inglese che deriva dalla frase to blow the whistle, letteralmente «soffiare il fischiello»



+ La compliance integrata

Per prima cosa occorre definire il significato del termine “Compliance” applicato alle realtà aziendali. Con il **termine compliance** si fa riferimento alla conformità rispetto a una norma di legge, uno standard o a best practice; il concetto di compliance include anche la capacità dell’azienda di attuare un sistema di controllo interno volto alla valutazione della conformità di procedure e comportamenti rispetto ai contesti normativi in cui l’azienda opera.

La compliance ormai è centrale in un contesto aziendale e assume un ruolo anche strategico. Infatti, il **rischio di compliance** - ossia di non conformità alle norme imperative, di autoregolamentazione e di best practice - oltre che esporre le aziende al rischio di incorrere in sanzioni giudiziarie amministrative, perdite finanziarie rilevanti o danni reputazionali, risulta essere anche un elemento essenziale nell’ambito delle scelte strategiche di business e performance aziendale.

La compliance integrata permette di coniugare efficacemente obiettivi di compliance e obiettivi di performance, contenendo al contempo i costi.



Il passaggio ad una **compliance integrata**, infatti, potrebbe permettere alle aziende di:

- razionalizzare le attività (in termini di risorse, persone, sistemi, etc);
- migliorare l'efficienza dei processi;
- facilitare la condivisione delle informazioni attraverso una visione integrata delle diverse esigenze di compliance anche attraverso l'esecuzione di Risk Assessment congiunti e la manutenzione periodica di programmi di compliance.

Un sistema integrato permetterebbe la semplificazione e la sintesi dei processi interni coinvolti nel monitoraggio della compliance.

In quest'ottica, l'approccio integrato dovrebbe contemplare procedure comuni che garantiscano efficienza e snellezza e che non generino sovrapposizione di ruoli (o mancanza di presidi), duplicazioni di verifiche e di azioni correttive, in termini più ampi, di conformità rispetto alla copiosa normativa di riferimento, laddove tali ruoli rispettivamente incidano e insistano sui medesimi processi.

Per dare attuazione a una gestione integrata di questo tipo occorre quindi anche definire specifici e continui meccanismi di coordinamento e collaborazione tra i principali soggetti aziendali.



Responsabilità amministrativa degli enti ex D. LGS. 231/2001

Il Decreto Legislativo 8 giugno 2001 n. 231 (di seguito anche semplicemente il “**Decreto 231**”) ha introdotto nell’ordinamento giuridico italiano il principio della responsabilità amministrativa degli enti dipendente da reato. Gli enti (le società, innanzitutto) possono così essere sanzionati per reati commessi da amministratori, da dipendenti o da collaboratori.

Le **sanzioni** sono particolarmente pesanti per la società e possono minarne la continuità aziendale (ad esempio, tramite la confisca dei beni aziendali o sanzioni interdittive). Peraltro, il sequestro dei beni aziendali e le misure interdittive possono essere applicati - sussistendo i requisiti previsti dal Decreto - anche in sede cautelare, dunque appena aperte le indagini e ben prima di un accertamento di merito sulla responsabilità dell’ente.

Affinché l’ente venga sanzionato è necessario che sussistano i seguenti presupposti:

- la commissione di uno dei reati elencati dal Decreto 231 da parte di un soggetto apicale o sottoposto dell’ente (c.d. “reati pre supposto”);
- la circostanza che la commissione del reato realizzi un interesse e/o vantaggio dell’ente (da intendersi anche, secondo giurisprudenza autorevole e costante, come risparmio di spesa);
- l’assenza di un modello di organizzazione, gestione e controllo idoneo a prevenire i reati del tipo di quello effettivamente realizzati (c.d. Modello 231).



Come appena anticipato, elemento costitutivo della fattispecie è, innanzitutto, la commissione, da parte di un soggetto apicale o di un soggetto sottoposto dell'ente, di uno degli illeciti penali elencati dal Decreto 231 (ad esempio, il reato di corruzione o quello di c.d. 'falso in bilancio').

Per **soggetto apicale** si intende un "vertice" dell'organizzazione aziendale: una persona che riveste funzioni di rappresentanza, di amministrazione, o di direzione dell'ente. Si tratta, in altri termini, di persone che rappresentano la volontà dell'ente o che, comunque, esercitano - anche a prescindere dalla qualifica formale - una concreta e penetrante influenza nelle attività aziendali (ad esempio, il Consigliere di Amministrazione, il Direttore Generale, i soggetti dotati di deleghe/procure formali, i Responsabili di unità operative periferiche dotate di autonomia finanziaria e funzionale).

Ultimo, fondamentale, presupposto per la responsabilità dell'ente è la c.d. **colpa d'organizzazione**. L'ente può, infatti, essere 'incolpato' del reato esclusivamente se non ha fatto quanto in suo potere per evitare la realizzazione dell'illecito, ovvero non si è organizzato con procedure volte a ridurre - entro limiti ragionevoli - il rischio di commissione del reato.

Dunque, l'adozione e la concreta attuazione di un idoneo Modello di Organizzazione, Gestione e Controllo - quale insieme di procedure finalizzate al contenimento del rischio di commissione di illeciti - **esclude la sanzionabilità dell'ente** per l'illecito commesso al suo interno.





Whistleblowing

Avuto riguardo al tema **Whistleblowing**, le fonti alle quali bisogna fare riferimento sono il D. Lgs. 10 marzo 2023 n. 24 (“Decreto”) che ha recepito la Direttiva UE 2019/1937 sul Whistleblowing; la Delibera ANAC n. 469 del 9 giugno 2021; le Linee Guida ANAC (“LG ANAC”) approvate con delibera n. 311 del 12 luglio 2023; Guida operativa per gli enti privati di Confindustria.

Il Decreto disciplina i **canali** e le modalità per effettuare una segnalazione. In particolare, si distinguono tre fattispecie:

- a) la segnalazione attraverso un canale interno all'ente;
- b) la segnalazione mediante un canale esterno all'ente, istituito e gestito dall'ANAC;
- c) la divulgazione pubblica.

Al riguardo, pur non indicando espressamente un ordine di priorità tra le diverse modalità di segnalazione, il Decreto fissa condizioni specifiche - sebbene con formule talvolta eccessivamente generiche - per accedere sia alla procedura esterna, sia alla divulgazione pubblica, al fine di incentivare gli enti a dotarsi di sistemi organizzativi efficienti integrati nei propri sistemi di controllo interno e di realizzare un corretto bilanciamento tra la tutela del whistleblower e la salvaguardia della reputazione dell'ente.

Su tale aspetto, anche le LG ANAC ribadiscono una gradualità nella scelta del canale di segnalazione più idoneo al caso concreto, da un lato, ribadendo la priorità del ricorso al canale interno e, dall'altro, chiarendo, in modo più puntuale rispetto alla disciplina normativa, le condizioni per il ricorso alla segnalazione esterna e alla divulgazione pubblica.



Con riferimento invece alle tipologie e alle modalità per effettuare le segnalazioni, la disciplina cambia in base alle dimensioni e alla natura pubblica o privata del soggetto di appartenenza del segnalante. In particolare, negli **enti privati** che:

- non hanno raggiunto la media di 50 lavoratori e hanno adottato il Modello Organizzativo 231, le segnalazioni possono riguardare solo condotte illecite rilevanti per la disciplina 231 o violazioni del modello 231 ed essere effettuate unicamente attraverso il canale interno;
- hanno impiegato la media di almeno 50 lavoratori e hanno adottato il Modello Organizzativo 231, le segnalazioni possono:
 1. Avere a oggetto condotte illecite o violazione del Modello Organizzativo 231 ed essere effettuate solo attraverso canale interno;
 2. Avere a oggetto violazioni del diritto UE ed essere effettuate attraverso canale interno, esterno, divulgazione pubblica o denuncia.
- hanno impiegato la media almeno di 50 lavoratori e non hanno il Modello Organizzativo 231 oppure rientrano nell'ambito di applicazione degli atti dell'Unione di cui alle parti I.B e II dell'Allegato (servizi, prodotti e mercati finanziari, prevenzione del riciclaggio e del finanziamento del terrorismo, nonché sicurezza dei trasporti e tutela dell'ambiente) anche se non hanno raggiunto la media di 50 lavoratori subordinati, le segnalazioni possono riguardare violazioni del diritto UE ed essere effettuate attraverso canale interno, esterno, divulgazione pubblica o denuncia.

Quando ai **soggetti legittimati a presentare la segnalazione**, nell'ambito degli enti pubblici e privati destinatari della disciplina in esame, le segnalazioni possono essere fatte da: lavoratori dipendenti e autonomi, liberi professionisti e consulenti, lavoratori e collaboratori che svolgono la propria attività presso soggetti pubblici o privati che forniscono beni o servizi presso soggetti pubblici e privati, i volontari, i tirocinanti, gli azionisti, e le persone con funzione di direzione amministrazione e controllo.

L'azienda, tenuta ad adeguarsi alla normativa, deve adottare un protocollo che contenga gli elementi essenziali previsti dal Decreto e dalla prassi di settore e deve darne informativa a tutti i soggetti coinvolti. Inoltre, la stessa deve nominare un **gestore del canale**, che può essere un soggetto/ufficio interno all'azienda ovvero un soggetto esterno. In ogni caso, è fondamentale che tali soggetti siano dotati di autonomia e specificamente e adeguatamente formati alla gestione delle segnalazioni.

La prima tutela posta della normativa in esame è la **tutela della riservatezza del segnalante**, della sua identità e di ogni altra informazione, inclusa l'eventuale documentazione allegata, dalla quale possa direttamente o indirettamente risalire all'identità del whistleblower. In quest'ottica la normativa vieta ogni forma di ritorsione nei confronti del segnalante, intesa come qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, che si verifichi nel contesto lavorativo e che determini – in via diretta o indiretta – un danno ingiusto ai soggetti tutelati.



I SISTEMI DI CERTIFICAZIONE



La **certificazione di sistema di gestione** è il riconoscimento delle capacità imprenditoriali di un'organizzazione che ha saputo ottimizzare la propria struttura dotandosi di una gestione efficiente, di competenze adeguate e di processi e strumenti interni idonei.

I **benefici** connessi alle certificazioni possono ricondursi a tre concetti principali:

- **Coesione aziendale:** l'evidenza di una cultura lavorativa condivisa da tutta l'azienda, improntata alla professionalità;
- **Affidabilità:** la conferma di una realtà affidabile che garantisce la riproducibilità delle sue performance e il miglioramento del suo standard qualitativo nel tempo;
- **Trasparenza:** una garanzia per clienti, fornitori, dipendenti e collaboratori, tanto più valida tanto più è prestigioso l'organismo che ha rilasciato la certificazione.

Si menzionano, a titolo esemplificativo e non esaustivo, le **certificazioni** secondo le norme:

- ISO 9000 per i sistemi di gestione della qualità;
- ISO 14000 per i sistemi di gestione ambientale;
- ISO 45001 per i sistemi di gestione della sicurezza e della salute nei luoghi di lavoro;
- SA 8000 impatto sull'etica e sul sociale (emessa dal SAI)
- UNI/PDR 125:2022 sulla parità di genere;
- ISO 30415 sulla gestione delle risorse umane Diversità e Inclusione;
- ISO 27000 per i sistemi di gestione della sicurezza delle informazioni.

L'adesione a tali norme è volontaria, salvo che non siano citate come testi cogenti in atti legislativi specifici. I certificati vengono rilasciati dagli organismi accreditati a seguito di verifiche ispettive condotte, secondo precisi regolamenti concordati, presso l'organizzazione richiedente.

I sistemi di certificazione **mirano a migliorare l'immagine e la visibilità** delle imprese che li adottano, consolidando il consenso che esse riscuotono sul mercato presso investitori e clienti. Implementare un sistema certificato di misure organizzative e preventive, infatti, è segno di un'inclinazione dell'ente alla cultura del rispetto delle regole, che può costituire anche la base per la costruzione di modelli tesi alla prevenzione di reati-presupposto (Modelli 231).

Bisogna tuttavia distinguere tale funzione delle certificazioni da quella propria dei Modelli 231, i quali invece servono a prevenire i reati nell'ambito dell'attività dell'ente o comunque a metterlo al riparo da responsabilità per i casi in cui, nonostante l'adozione e l'efficace attuazione del modello, tali reati si siano comunque verificati.

Coerentemente, i **requisiti di idoneità** dei modelli non sono del tutto corrispondenti a quelli richiesti per ottenere le certificazioni dei sistemi di gestione, ad esempio della qualità, dell'ambiente o della salute e sicurezza sul lavoro. L'articolo 6 del D.lgs. 231/2001 prevede, infatti, l'istituzione di un **Organismo di Vigilanza** e la predisposizione di un sistema di controlli più elaborato di quelli previsti per il conseguimento o mantenimento di certificazione dei sistemi aziendali.

Dato questo quadro, in un'ottica di compliance integrata, sarà importante valorizzare la sinergia del Modello 231 con la documentazione dei sistemi di gestione aziendali sottostanti alle certificazioni, al fine migliorare e valorizzare l'efficienza dei vari strumenti di compliance adottati.





Sostenibilità e fattori ESG

Strettamente collegato al contesto delle certificazioni è il tema della sostenibilità, dei fattori ESG e, più nello specifico, dei **reporting ESG**.

Nel dettaglio l'acronimo ESG indica:

- E: "Environmental" (Ambientale) che riguarda le politiche e le performance di un'azienda in termini di impatto ambientale (es. l'emissione di gas serra, la gestione dei rifiuti, l'uso delle risorse naturali e la conservazione della biodiversità);
- S: "Social" (Sociale) che interessa le relazioni dell'azienda con i suoi dipendenti e la comunità più ampia (può includere questioni come le condizioni di lavoro, la salute e la sicurezza, i diritti umani e le relazioni con la comunità locale);
- G: "Governance" (Governance) che riguarda la struttura di gestione dell'azienda, compresi i diritti degli azionisti, la remunerazione degli executive, le pratiche di business etiche e la trasparenza.

I vari strumenti di reportistica ESG hanno avuto ampia diffusione negli ultimi anni.

Molte aziende, difatti, anche quelle non obbligate, includono i criteri ESG nelle proprie relazioni annuali, per dimostrare ai propri stakeholder che la sostenibilità è parte integrante della loro attività. Nel tempo queste tematiche hanno acquisito sempre più importanza in quanto gli investitori e le altre parti interessate richiedono maggiore trasparenza sulle performance non finanziarie delle aziende.

Per il tramite del reporting ESG le aziende hanno modo di dimostrare concretamente il proprio impegno nei confronti degli stakeholder, rappresentando la certificazione ESG una sorta di "**bollino di qualità**" con cui viene attestata l'aderenza dell'azienda ai principi ESG.



Diversi possono essere i motivi che attribuiscono importanza al reporting ESG e tra questi vi sono:

- **Trasparenza:** il reporting ESG fornisce una visione chiara delle pratiche ambientali, sociali e di governance di un'azienda. Questo aiuta gli stakeholder, inclusi investitori, clienti e dipendenti, a comprendere meglio l'impegno dell'azienda verso la sostenibilità e la responsabilità sociale;
- **Decisioni di investimento:** sempre più investitori stanno considerando i fattori ESG nelle loro decisioni di investimento. Un buon reporting ESG può attrarre investitori che cercano di allineare i loro portafogli con obiettivi di sostenibilità;
- **Gestione del rischio:** il reporting ESG può aiutare le aziende a identificare e gestire i rischi legati a questioni ambientali, sociali e di governance. Questo può includere rischi legati ai cambiamenti climatici, ai diritti umani, alla diversità e inclusione, e alla governance aziendale;
- **Reputazione:** un buon reporting ESG può migliorare la reputazione di un'azienda, rendendola più attraente per i clienti, i dipendenti e gli investitori;
- **Conformità normativa:** in molte giurisdizioni, le aziende sono tenute a fornire determinate informazioni ESG. Un buon reporting ESG può aiutare le aziende a soddisfare questi requisiti normativi;
- **Miglioramento delle performance:** il reporting ESG può aiutare le aziende a identificare opportunità per migliorare le loro performance ambientali, sociali e di governance, contribuendo a creare valore a lungo termine.



+ Privacy

La tutela della privacy è un diritto fondamentale della persona. La tradizionale nozione di privacy, definita come il diritto ad essere lasciati indisturbati e fondata sul criterio dell'esclusione degli altri dalla propria sfera privata, si è evoluta nel diritto di controllare come gli altri trattino i propri dati.

Con l'introduzione del Regolamento UE 2016/679, si cerca di coniugare l'evoluzione tecnologica e la globalizzazione tipiche della società dell'informazione con il diritto alla privacy, imponendo ai titolari del trattamento dei dati personali livelli di sicurezza adeguati alle diverse tipologie di trattamento.

Il regolamento UE n. 2016/679 costruisce gli architravi della privacy sui seguenti punti:

- Rispetto dei principi e dei diritti delle persone;
- Analisi del rischio e valutazione di impatto;
- Predisposizione del registro dei trattamenti;
- Sicurezza dei dati;
- Responsabile della protezione dei dati (DPO).

A seguito dell'attuazione del Regolamento UE 2016/679, il legislatore italiano ha dovuto adeguare le previsioni normative del D.lgs. 196/2003 (c.d. Codice Privacy) alle disposizioni del Regolamento succitato.

A tal fine, ha emanato il D.lgs. 101 del 2018 che ha dovuto tenere in considerazione la circostanza che il D.lgs. n. 196/2003 e il Regolamento UE 2016/679 hanno un approccio completamente differente al tema della privacy, a partire dal **concetto di accountability**. Ne consegue che, per effetto del D.lgs. n. 101 del 2018, il nuovo Codice della Privacy, così come modificato, ha perso la sua centralità, dovendosi leggere le sue norme in combinato disposto con quelle del regolamento europeo.



GRAZIE PER AVER LETTO
IL NOSTRO APPROFONDIMENTO SULLA COMPLIANCE.

**NOVERIM È IL TUO PARTNER IDEALE
SCRIVICI SE VUOI SAPERE DI PIÙ
SUI NOSTRI SERVIZI COMPLIANCE :**

- ▶ Compliance e ESG Box
- ▶ Privacy
- ▶ Modello 231
- ▶ Bilancio di sostenibilità
- ▶ Parità di genere
- ▶ Whistleblowing

COMPLIANCE FOCUS PRO

I nostri approfondimenti si impegnano a fornire ai lettori informazioni accurate su temi di attualità.

Certi che la nostra offerta vi mantenga aggiornati sulle ultime normative e competitivi nel vostro mercato di riferimento, ci rivediamo ad aprile con il prossimo volume.

RIMANI AGGIORNATO

