MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO D. LGS 231/2001

APPENDICE 1

Integrazione di Novità Legislative e Migliori Prassi

Prima Emissione		**Del 02.07.2026**

Il presente rapporto ha lo scopo di delineare le modifiche e gli aggiornamenti necessari alla "Parte Generale" del Modello di Organizzazione, Gestione e Controllo (MOGC) di Sage Castelli S.R.L., in conformità con il Decreto Legislativo 231/2001. L'analisi si concentra sull'integrazione delle più recenti novità legislative e delle migliori prassi giurisprudenziali emesse nel primo semestre del 2026. Verranno evidenziate le aree critiche di aggiornamento, tra cui la normativa anticorruzione, i reati tributari, la disciplina del whistleblowing, la cybersicurezza, l'Intelligenza Artificiale, e i vincoli di indipendenza della tutela penale dell'ente.

1. Introduzione: Il Contesto Evolutivo della Compliance al D. Lgs. 231/2001

Il Modello di Organizzazione, Gestione e Controllo (MOGC) ai sensi del D. Lgs. 231/2001 rappresenta per un'azienda non un mero adempimento formale, bensì un sistema dinamico e strategico. La sua funzione principale è prevenire la commissione di reati presupposto, fornendo all'ente una difesa esimente da responsabilità amministrativa. Questo strumento si configura come un pilastro fondamentale per promuovere una cultura di legalitò ed etica all'interno dell'organizzazione. La necessità di un aggiornamento continuo del MOGC deriva dalla natura stessa del quadro normativo del D. Lgs. 231/2001, il quale è soggetto a una costante espansione legislativa e a un affinamento interpretativo da parte della giurisprudenza.

2. Aggiornamenti Legislativi Chiave e il Loro Impatto sul MOGC

Modifiche al Codice Penale

La Legge 190/2012 ha modificato l'Articolo 317 del Codice Penale (concussione), rimuovendo il riferimento all'induzione, che ora è disciplinata separatamente dall'Articolo 319-quater c.p.. Questo comporta che il privato che subisce l'induzione non è più considerato vittima, ma può essere soggetto a punibilità. È stato inoltre introdotto l'Articolo 346-bis c.p., che disciplina il reato di traffico di influenze illecite, punendo chi, sfruttando relazioni esistenti o asserite con un pubblico ufficiale, si fa dare o promettere denaro o altra utilità per fungere da mediatore illecito. La legge ha anche esteso i reati previsti dagli Articoli 318 e 319 c.p. (corruzione) agli incaricati di un pubblico servizio. Il Decreto P.I.F. (Direttiva UE 2017/1371) è intervenuto anche su alcune fattispecie di corruzione, estendendo la responsabilità dell'ente ai casi in cui denaro o utilità siano sottratti al bilancio

dell'Unione o ad altri suoi organismi.

Implicazioni per il MOGC di Sage Castelli S.r.l. S.R.L.
Sage Castelli S.r.l. S.R.L. deve rivedere e aggiornare la propria valutazione del rischio per le interazioni con la Pubblica Amministrazione, prestando particolare attenzione alle nuove definizioni dei reati di corruzione. I protocolli interni devono essere adeguati per affrontare l'ampliamento del campo di applicazione del "traffico di influenze illecite" e dell'"induzione indebita". È fondamentale assicurare linee guida interne chiare in merito a regali, ospitalità e interazioni con i funzionari pubblici, considerando l'interpretazione più ampia dell'influenza illecita.
L'attenzione legislativa all'indipendenza e alle responsabilità del RPCT, unitamente alla struttura del PTPC, indica un'evoluzione da una compliance meramente formale a un impegno anticorruzione sostanziale e monitorato. L'assorbimento del PTPC nel PIAO per gli enti pubblici suggerisce una spinta governativa più ampia verso la pianificazione e la trasparenza integrate, che potrebbe diventare una prassi o un'aspettativa futura anche per gli enti privati che adottano MOGC, specialmente quelli con significative interazioni pubbliche. Le modifiche al Codice Penale, in particolare l'introduzione del "traffico di influenze illecite", ampliano la portata della condotta punibile oltre la corruzione diretta. Ciò richiede a Sage Castelli S.r.l. di estendere la propria mappatura dei rischi per includere il traffico di influenze indiretto, le attività di lobbying e l'uso di intermediari, valutando non solo i pagamenti diretti ma anche lo sfruttamento delle relazioni per ottenere vantaggi illeciti. Questo rende necessarie procedure di due diligence più robuste per gli impegni con terze parti.

2.2. Introduzione dei Reati Tributari (D.L. 124/2019 conv. L. 157/2019 e Direttiva PIF)

I reati tributari sono stati introdotti tra i reati presupposto del D. Lgs. 231/2001 solo di recente, dopo diciotto anni dall'entrata in vigore del decreto, attraverso due successivi interventi normativi. Questa inclusione rappresenta un'espansione significativa della responsabilità amministrativa degli enti.

Primo Intervento (Legge 157 del 19 dicembre 2019, che ha convertito il D.L. 124/2019)
Questo intervento ha comportato l'introduzione nel D. Lgs. 231/2001 del nuovo Articolo 25-quinquiesdecies , che estende la disciplina 231 ai seguenti reati in materia di IRES e IVA:

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (Art. 2, co. 1 e co. 2-bis, d. lgs. 74/2000).
- Dichiarazione fraudolenta mediante altri artifici (Art. 3, d. lgs. 74/2000).
- Emissione di fatture o altri documenti per operazioni inesistenti (Art. 8, commi 1 e 2-bis, d. lgs. 74/2000).

- Occultamento o distruzione di documenti contabili (Art. 10, d. lgs. 74/2000).
- Sottrazione fraudolenta al pagamento di imposte (Art. 11, d. lgs. 74/2000).

Secondo Intervento (Luglio 2020, Direttiva PIF - UE 2017/1371)

Con questo secondo intervento, le fattispecie tributarie rilevanti ai fini 231 sono state ulteriormente estese ai reati di:

- Dichiarazione infedele (Art. 4, d. lgs. 74/2000).
- Omessa dichiarazione (Art. 5, d. lgs. 74/2000).
- Indebita compensazione (Art. 10-quater, d. lgs. 74/2000).

Per queste ultime fattispecie, la configurabilità della responsabilità dell'ente è subordinata a condizioni specifiche: devono essere commessi nell'ambito di sistemi fraudolenti transfrontalieri, al fine di evadere l'IVA, e per un importo superiore a dieci milioni di euro. Il decreto PIF ha anche esteso la responsabilità degli enti per alcuni reati di corruzione che sottraggono denaro o utilità al bilancio dell'Unione o ad altri suoi organismi.

Implicazioni per i Controlli Finanziari e le Procedure Contabili

Il MOGC di Sage Castelli S.r.l. deve ora coprire esplicitamente questi nuovi reati tributari. Ciò richiede una mappatura approfondita dei processi e delle attività sensibili a rischio di commissione di tali illeciti , e l'implementazione di sistemi di controllo interno robusti, in particolare nei dipartimenti finanziari, contabili e fiscali. Particolare attenzione deve essere rivolta all'utilizzo di consulenti fiscali esterni, identificando potenziali comportamenti a rischio. La valutazione del rischio deve considerare il "doppio binario sanzionatorio" per i reati tributari (amministrativo e penale). È inoltre significativa la potenziale confisca del prezzo o del profitto del reato, che può avere effetti molto rilevanti per le violazioni fiscali. La giurisprudenza della Cassazione ha stabilito che non si possono applicare retroattivamente sanzioni per condotte che, al momento della commissione, non generavano responsabilità per l'ente , sottolineando l'importanza di aggiornamenti tempestivi del MOGC.

L'inclusione, seppur tardiva, dei reati tributari nel D. Lgs. 231/2001 indica una maturazione del quadro normativo, estendendone la portata all'integrità finanziaria. Le condizioni specifiche per la seconda ondata di reati tributari (transfrontalieri, IVA, soglia di 10 milioni di euro) indicano un approccio mirato alla frode finanziaria grave e organizzata, spesso con dimensioni internazionali. Questo è una diretta conseguenza delle direttive europee, che dimostrano come la politica dell'UE stia plasmando la responsabilità penale delle imprese a livello nazionale. Per Sage Castelli S.r.l., ciò implica che il MOGC deve non solo prevenire l'evasione fiscale interna, ma anche identificare e mitigare proattivamente i rischi associati a complesse operazioni finanziarie internazionali che potrebbero essere interpretate come frode transfrontaliera. La possibilità di confisca del profitto per i reati tributari rappresenta una conseguenza severa. Ciò significa che qualsiasi "risparmio" derivante da pratiche fiscali illecite, anche se esiguo, potrebbe portare

a significative sanzioni finanziarie per l'azienda, superando di gran lunga il "vantaggio" iniziale. Questo rafforza la necessità di un sistema di controllo interno estremamente robusto su tutti i flussi finanziari e le dichiarazioni fiscali, andando oltre la mera conformità verso una cultura di integrità fiscale assoluta. Il MOGC deve articolare chiaramente una tolleranza zero per qualsiasi forma di manipolazione fiscale, per quanto minore, poiché anche un risparmio "esiguo" può configurare un vantaggio.

Tabella 1: Nuovi Reati Tributari Presupposto ai sensi del D. Lgs. 231/2001

Reato	Articolo di riferimento (D. Lgs. 74/2000)	Legislazione introduttiva	Condizioni specifiche per la responsabilità 231 (se applicabile)
Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti	Art. 2, co. 1 e 2-bis	D.L. 124/2019 conv. L. 157/2019	Nessuna condizione specifica
Dichiarazione fraudolenta mediante altri artifici	Art. 3	D.L. 124/2019 conv. L. 157/2019	Nessuna condizione specifica
Emissione di fatture o altri documenti per operazioni inesistenti	Art. 8, commi 1 e 2-bis	D.L. 124/2019 conv. L. 157/2019	Nessuna condizione specifica
Occultamento o distruzione di documenti contabili	Art. 10	D.L. 124/2019 conv. L. 157/2019	Nessuna condizione specifica
Sottrazione fraudolenta al pagamento di imposte	Art. 11	D.L. 124/2019 conv. L. 157/2019	Nessuna condizione specifica
Dichiarazione infedele	Art. 4	Direttiva PIF (UE 2017/1371)	Commesso nell'ambito di sistemi fraudolenti transfrontalieri, al fine di evadere l'IVA, per un importo superiore a dieci milioni di euro
Omessa dichiarazione	Art. 5	Direttiva PIF (UE 2017/1371)	Commesso nell'ambito di sistemi fraudolenti transfrontalieri, al fine di evadere l'IVA, per un importo superiore a dieci milioni di euro
Indebita compensazione	Art. 10-quater	Direttiva PIF (UE	Commesso nell'ambito di

Reato	Articolo di riferimento (D. Lgs. 74/2000)	Legislazione introduttiva	Condizioni specifiche per la responsabilità 231 (se applicabile)
		2017/1371)	sistemi fraudolenti transfrontalieri, al fine di evadere l'IVA, per un importo superiore a dieci milioni di euro

2.3. La Disciplina del Whistleblowing (D.Lgs. 24/2023)

Il Decreto Legislativo 24 del 10 marzo 2023, pubblicato in Gazzetta Ufficiale il 15 marzo 2023, recepisce la Direttiva UE 2019/1937, unificando la normativa sul whistleblowing per il settore pubblico e privato. Questo aggiornamento è di fondamentale importanza per i MOGC, in quanto incide direttamente sui sistemi di controllo interno e sulla condotta etica.

Requisiti per i Canali di Segnalazione Interni ed Esterni

Il decreto impone l'istituzione di canali di segnalazione interni obbligatori per gli enti che rientrano nel suo ambito di applicazione. Tali canali devono garantire la riservatezza dei dati personali del segnalante e della segnalazione stessa, prevedendo sistemi di crittografia. I canali di segnalazione esterni sono invece gestiti dall'ANAC. Sono previste tempistiche specifiche per la gestione delle segnalazioni.

Ambito di Applicazione

La nuova disciplina si applica a tutti i soggetti del settore pubblico (inclusi quelli di proprietà o sotto il controllo di tali soggetti, e i Comuni con più di 10.000 abitanti). Nel settore privato, l'applicazione è scaglionata: dal 15 luglio 2023 per le aziende con più di 250 dipendenti (indipendentemente dall'adozione di un MOGC), e dal 17 dicembre 2023 per quelle con una media di 50-249 lavoratori subordinati nell'ultimo anno (anch'esse indipendentemente dall'adozione di un MOGC). È cruciale per Sage Castelli S.r.l. che le entità che adottano un MOGC ai sensi del D. Lgs. 231/2001 sono soggette al decreto, a prescindere dal numero di dipendenti. L'oggetto delle segnalazioni comprende comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, incluse le violazioni di disposizioni normative nazionali e del diritto dell'Unione.

Soggetti Protetti e Ritorsioni Proibite

Il D. Lgs. 24/2023 tutela un'ampia gamma di soggetti, tra cui dipendenti, collaboratori, lavoratori subordinati e autonomi, liberi professionisti, tirocinanti

(anche non retribuiti), azionisti e persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza. Una novità significativa è la protezione estesa ai cosiddetti "facilitatori" (colleghi, parenti o affetti stabili di chi ha segnalato). Le misure di protezione mirano a prevenire ritorsioni, la cui lista (non esaustiva) include: licenziamento, sospensione, retrocessione di grado, mancata promozione, modifica dell'orario di lavoro, sospensione della formazione, note di merito negative, misure disciplinari, coercizione, intimidazione, molestie, ostracismo, discriminazione, trattamento sfavorevole, mancata conversione di contratti a termine, danni (anche alla reputazione, inclusi i social media), pregiudizi economici o finanziari, annullamento di licenze o permessi, e la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

Ruolo dell'ANAC e Sanzioni Applicabili

L'ANAC è l'Autorità competente a ricevere le segnalazioni esterne, sia per il settore pubblico che per quello privato. Sono previste sanzioni pecuniarie da 10.000 a 50.000 euro per gli enti che non istituiscono canali di segnalazione, non adottano procedure per la gestione delle segnalazioni o se tali procedure non sono conformi. Sanzioni da 500 a 2.500 euro sono previste per i segnalanti in caso di accertata responsabilità penale per i reati di diffamazione o calunnia.

Implicazioni per il MOGC di Sage Castelli S.r.l. S.R.L.

Il MOGC di Sage Castelli S.r.l. deve integrare i nuovi requisiti del D. Lgs. 24/2023 sia nella sua "Parte Generale" che nei protocolli specifici. È imperativo stabilire canali di segnalazione interni chiari, sicuri e confidenziali, conformi ai nuovi requisiti tecnici (es. crittografia). Occorre sviluppare procedure dettagliate per la gestione delle segnalazioni, incluse le tempistiche e i protocolli di indagine. È essenziale una formazione completa per tutto il personale sulla nuova politica di whistleblowing, sui soggetti protetti e sulle ritorsioni proibite. I sistemi disciplinari interni devono essere rivisti e aggiornati per assicurare che nessuna misura ritorsiva sia adottata contro i segnalanti o i facilitatori. L'Organismo di Vigilanza (OdV) deve supervisionare l'efficacia del sistema di whistleblowing.

Il D. Lgs. 24/2023 non è un semplice aggiornamento procedurale, ma un cambiamento fondamentale verso l'istituzionalizzazione della trasparenza e della responsabilità interna. L'ampia portata dei soggetti protetti, inclusi i "facilitatori", e l'esteso elenco di ritorsioni proibite riflettono una forte volontà legislativa di creare un ambiente veramente sicuro per le segnalazioni, superando la compliance formalistica per giungere a una protezione sostanziale dei whistleblower. L'esplicita inclusione delle aziende che adottano un MOGC 231 significa che la conformità al whistleblowing è ora direttamente legata all'efficacia del MOGC stesso. Una mancata implementazione o gestione corretta dei canali di whistleblowing può portare a sanzioni ANAC, che a loro volta potrebbero essere interpretate da un tribunale come un difetto nella progettazione o nell'attuazione

effettiva del MOGC, indebolendone il potere esimente in un procedimento 231. Questo crea una nuova via per la responsabilità o per contestare l'idoneità del MOGC. La protezione dei "facilitatori" e l'ampia definizione di ritorsione richiedono un profondo cambiamento culturale all'interno di Sage Castelli S.r.l.. Non si tratta più solo di proteggere il segnalante diretto, ma di promuovere un ambiente in cui chiunque sia associato a una segnalazione si senta al sicuro da qualsiasi forma di trattamento avverso. Ciò richiede non solo modifiche politiche, ma anche formazione attiva, comunicazione e un impegno visibile da parte della direzione per garantire una cultura del "parlare apertamente", essenziale per l'efficacia complessiva del MOGC nell'identificazione dei rischi. Il codice etico del MOGC deve essere aggiornato per riflettere questa protezione estesa.

Di seguito una tabella riassuntiva della disciplina del whistleblowing:

Tabella 2: Riepilogo della Disciplina Whistleblowing (D. Lgs. 24/2023)

Categoria	Descrizione/Requisiti	Riferimento Normativo	Data di Entrata in Vigore per il Settore Privato
Canali di Segnalazione	Canali interni obbligatori, sicuri e riservati (con crittografia). Canali esterni gestiti da ANAC.	D. Lgs. 24/2023	Dal 15 luglio 2023 (>250 dipendenti); Dal 17 dicembre 2023 (50-249 dipendenti); Immediato per enti con MOGC 231
Soggetti Protetti	Dipendenti, collaboratori, lavoratori subordinati e autonomi, liberi professionisti, tirocinanti, azionisti, persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza. Inclusi i "facilitatori" (colleghi, parenti, affetti stabili).	D. Lgs. 24/2023, Art. 2, 3, 4	Immediato
Ritorsioni Proibite	Licenziamento, sospensione, retrocessione, mancata promozione, modifica orario, sospensione formazione, note di merito negative, misure	D. Lgs. 24/2023, Art. 17	Immediato

Categoria	Descrizione/Requisiti	Riferimento Normativo	Data di Entrata in Vigore per il Settore Privato
	disciplinari, coercizione, intimidazione, molestie, ostracismo, discriminazione, trattamenti sfavorevoli, mancata conversione contratto, danni reputazionali/economici, annullamento licenze, richiesta accertamenti medici.		
Ruolo di ANAC	Autorità competente a ricevere segnalazioni esterne e a imporre sanzioni per inadempienze.	D. Lgs. 24/2023, Art. 7, 10	Immediato
Sanzioni	Da €10.000 a €50.000 per mancata istituzione/adozione/conformità dei canali/procedure. Da €500 a €2.500 per segnalanti responsabili di diffamazione o calunnia.	D. Lgs. 24/2023	Immediato

2.4. Cybersicurezza e Protezione dei Dati (Direttiva NIS 2, GDPR e Legislazione Correlata)

La crescente minaccia degli attacchi informatici ha portato a un rafforzamento della legislazione sulla cybersicurezza, con implicazioni dirette per il D. Lgs. 231/2001, in particolare per quanto riguarda i reati informatici e il trattamento illecito di dati.

Direttiva NIS 2 (UE 2022/2555) e D. Lgs. 138/2024

La Direttiva NIS 2 ha sostituito la precedente Direttiva NIS 1 (recepita in Italia con il D. Lgs. 65/2018). Essa espande l'ambito di applicazione a 18 settori, distinti in altamente critici e critici. La nuova direttiva eleva gli standard di sicurezza e gli obblighi di monitoraggio nell'Unione Europea , introducendo nuovi obblighi di notifica degli incidenti informatici e potenziando il ruolo dell'Agenzia per la Cybersicurezza Nazionale (ACN).

"Legge sulla Cybersicurezza"
La Legge sulla Cybersicurezza mira a rafforzare la cybersicurezza nazionale, aumentando la resilienza delle pubbliche amministrazioni, degli operatori soggetti al Perimetro di Sicurezza Nazionale Cibernetica, dei destinatari del D. Lgs. 65/2018 (NIS 1) e degli operatori che forniscono reti pubbliche di comunicazioni. Prescrive nuovi obblighi di notifica degli incidenti informatici e potenzia il ruolo dell'ACN. La Legge sulla Cybersicurezza apporta significative modifiche al Codice Penale e al D. Lgs. 231/2001. Si segnala un generale inasprimento del trattamento sanzionatorio per i delitti informatici, con un significativo aumento delle pene per la quasi totalità dei reati esistenti, e l'introduzione di nuove fattispecie di reato, con effetti sia per le persone fisiche che per gli enti ai sensi dell'Articolo 24-bis del D. Lgs. 231/2001 ("Delitti informatici e trattamento illecito di dati").

GDPR (Reg. UE 2016/679) e la sua Intersezione con il D. Lgs. 231/2001
Il Regolamento UE 2016/679 (GDPR) impone misure robuste di protezione dei dati personali, prevedendo sanzioni molto elevate (fino al 4% del fatturato consolidato) per la non conformità. Il MOGC e la compliance al GDPR condividono principi comuni: mappatura dei rischi, procedure, regole etiche, chiare deleghe e organi di vigilanza (OdV, DPO). Molti dei reati informatici previsti dall'Articolo 24-bis del D. Lgs. 231/2001 sono, in sostanza, ipotesi di "data breach dolosi" o violazioni informatiche con implicazioni sul trattamento dei dati. Anche se non esplicitamente elencati come reati presupposto 231, il MOGC dovrebbe considerare i rischi di trattamento illecito di dati. Il Responsabile della Protezione dei Dati (DPO) e gli esperti di privacy sono collaboratori cruciali per l'OdV nel monitoraggio della compliance.

Implicazioni per il MOGC di Sage Castelli S.r.l. S.R.L.
Il MOGC di Sage Castelli S.r.l. deve essere aggiornato per riflettere l'aumento delle sanzioni e i nuovi reati presupposto informatici, in particolare quelli previsti dall'Articolo 24-bis del D. Lgs. 231/2001. È necessario rafforzare i protocolli di sicurezza informatica, i piani di risposta agli incidenti e le procedure di notifica delle violazioni dei dati in linea con la Direttiva NIS 2 e la nuova Legge sulla Cybersicurezza. Occorre potenziare l'integrazione tra le misure di prevenzione dei crimini informatici del MOGC e gli sforzi di compliance al GDPR. Deve essere assicurato un flusso chiaro di informazioni e una collaborazione efficace tra l'OdV, la funzione di sicurezza IT e il DPO. È indispensabile condurre una specifica valutazione del rischio per i rischi cyber, inclusi quelli relativi al trattamento dei dati, al fine di identificare le vulnerabilità e implementare controlli preventivi.

La convergenza della legislazione sulla cybersicurezza (NIS 2, Legge sulla Cybersicurezza) e sulla protezione dei dati (GDPR) con il D. Lgs. 231/2001 segna

un cambiamento critico: i rischi cyber non sono più solo preoccupazioni IT, ma rischi diretti di responsabilità legale e penale per l'ente. L'aumento delle sanzioni per i reati informatici e la loro inclusione come reati presupposto 231 (Art. 24-bis) elevano l'importanza della sicurezza IT da costo operativo a imperativo di compliance fondamentale. Un singolo incidente informatico (ad esempio, una violazione dei dati causata da negligenza o atto doloso) potrebbe innescare più livelli di responsabilità: sanzioni GDPR, sanzioni amministrative D. Lgs. 231/2001 (se viene commesso un reato presupposto) e danni reputazionali. Ciò richiede un approccio di gestione del rischio veramente integrato, in cui i team di sicurezza IT, privacy e compliance 231 lavorino in modo sinergico. Il ruolo dell'OdV nella supervisione dei protocolli di cybersicurezza diventa di primaria importanza. La "Legge sulla Cybersicurezza" mira esplicitamente ad aumentare la resilienza della cybersicurezza nazionale. Per le aziende, ciò significa che la cybersicurezza non è più solo una misura difensiva contro minacce esterne, ma anche una componente attiva della sicurezza nazionale. Questo eleva l'importanza strategica degli investimenti in cybersicurezza e dei controlli interni. Il MOGC di Sage Castelli S.r.l. dovrebbe riflettere questo contesto sociale e di sicurezza nazionale più ampio, enfatizzando che una robusta cybersicurezza non riguarda solo l'evitare sanzioni, ma anche il contribuire a un ecosistema digitale sicuro, che a sua volta protegge la vitalità e la reputazione a lungo termine dell'azienda. Il MOGC dovrebbe delineare chiare responsabilità per la cybersicurezza a tutti i livelli, dal personale IT alla direzione.

Di seguito una tabella riassuntiva dei principali aggiornamenti legislativi e del loro impatto sul MOGC:

Tabella 3: Panoramica degli Aggiornamenti Legislativi Chiave e Impatto sul MOGC

Atto Legislativo	Disposizioni/Modifiche Chiave	Impatto Diretto sul MOGC D. Lgs. 231/2001	Riferimenti
Legge 190/2012 (Legge Severino)	Istituzione RPCT, PTPC, modifiche Codice Penale (es. concussione, traffico di influenze illecite).	Nuovi reati presupposto, revisione aree di rischio corruzione, necessità di protocolli specifici per interazioni con PA.	
D.L. 124/2019 conv. L. 157/2019 & Direttiva PIF (UE 2017/1371)	Introduzione reati tributari (Art. 25-quinquiesdecies) come	Espansione significativa dei reati presupposto, necessità di mappatura	

Atto Legislativo	Disposizioni/Modifiche Chiave	Impatto Diretto sul MOGC D. Lgs. 231/2001	Riferimenti
	reati presupposto, con condizioni specifiche per alcuni.	dei rischi finanziari/contabili, rafforzamento controlli interni su fiscalità.	
D. Lgs. 24/2023 (Whistleblowing)	Obbligo di canali di segnalazione interni ed esterni, protezione estesa dei segnalanti e "facilitatori", sanzioni ANAC.	Integrazione del sistema whistleblowing nel MOGC, definizione di protocolli per la gestione delle segnalazioni e la protezione dalle ritorsioni.	
Direttiva NIS 2 (UE 2022/2555) & Legge sulla Cybersicurezza (D. Lgs. 138/2024)	Ampliamento settori critici, obblighi di notifica incidenti, potenziamento ACN, inasprimento pene per reati informatici (Art. 24-bis D. Lgs. 231/2001).	Aumento delle sanzioni e nuovi reati presupposto informatici, necessità di rafforzare i protocolli di cybersicurezza, gestione incidenti e protezione dati.	
Regolamento UE 2016/679 (GDPR)	Obblighi di protezione dei dati personali, sanzioni elevate per violazioni, intersezioni con reati informatici 231.	Necessità di integrazione tra compliance privacy e MOGC, rafforzamento dei protocolli di gestione dei dati e collaborazione tra OdV e DPO.	

3. Migliori Prassi per il Potenziamento e l'Integrazione del MOGC

Questa sezione esplora approcci strategici per ottimizzare il MOGC, andando oltre i semplici mandati legislativi.

3.1. Sfruttare le Linee Guida di Confindustria (2021)

Le Linee Guida di Confindustria sono un riferimento cruciale per la costruzione e l'efficacia dei MOGC, essendo state approvate dal Ministero della Giustizia. L'ultima versione è stata pubblicata nel 2021. Sage Castelli S.r.l. dovrebbe assicurarsi che il proprio MOGC sia allineato a queste linee guida aggiornate, che riflettono le attuali migliori prassi e tendenze interpretative. Le linee guida forniscono metodologie dettagliate per la valutazione del rischio, la progettazione dei protocolli, i sistemi disciplinari e le funzioni dell'OdV. Ciò implica che il MOGC deve identificare le aree di rischio, definire protocolli specifici per la formazione e l'attuazione delle decisioni e stabilire sanzioni disciplinari per la non conformità.
Le Linee Guida di Confindustria (2021) non sono un documento statico, ma un'interpretazione dinamica del D. Lgs. 231/2001, che riflette l'evoluzione della comprensione legale e delle migliori prassi. La loro approvazione da parte del

Ministero della Giustizia conferisce loro un peso autorevole significativo, rendendo l'adesione un forte indicatore dell'idoneità del MOGC. Sebbene non siano legalmente vincolanti come una legge, gli organi giudiziari spesso si riferiscono a queste linee guida per valutare l'idoneità e l'efficacia di un MOGC. L'adesione a esse fornisce una solida difesa, dimostrando la dovuta diligenza e l'allineamento con gli standard riconosciuti del settore. Questo è un'applicazione pratica del principio di "attuazione effettiva". Adottando le Linee Guida di Confindustria, Sage Castelli S.r.l. può ottimizzare il proprio MOGC, evitando insidie comuni e sfruttando metodologie consolidate per la mappatura dei rischi, la progettazione dei controlli e la supervisione dell'OdV. Ciò riduce il rischio di avere un modello formalmente corretto ma sostanzialmente inadeguato, migliorandone così il potenziale esimente. Le linee guida forniscono anche un quadro per i sistemi disciplinari , che sono cruciali per l'applicabilità del MOGC.

3.2. Sistemi di Compliance Integrati

La ricerca evidenzia una forte tendenza all'integrazione di vari quadri di compliance (D. Lgs. 231/2001, GDPR, D. Lgs. 81/2008 per la Salute e Sicurezza sul Lavoro) in un unico sistema di gestione coeso. I benefici di tale approccio includono l'ottimizzazione degli sforzi, l'evitare duplicazioni, lo sfruttamento delle sinergie e un miglioramento dell'efficacia complessiva. Tutti questi quadri normativi condividono requisiti comuni: mappatura dei rischi, procedure, regole etiche, chiare deleghe e organismi di supervisione (OdV, DPO, dirigenti delegati). Per Sage Castelli S.r.l., ciò implica la necessità di perseguire un approccio integrato, riconoscendo le esigenze "gemelle" di questi diversi pacchetti normativi. Questo significa progettare controlli che affrontino simultaneamente i rischi in più domini legali.

Il concetto di un "modello integrato" rappresenta una risposta strategica alla crescente complessità e sovrapposizione dei requisiti di compliance. Riflette una comprensione sempre più diffusa che i rischi (ad esempio, cyber, sicurezza, finanziari) sono interconnessi e non possono essere gestiti efficacemente in silos. Un approccio a compartimenti stagni porta a "duplicazioni di sforzi, regole e procedure" e "perde la convenienza delle sinergie". Un sistema integrato, al contrario, è più efficiente nell'allocazione delle risorse e più efficace nella mitigazione del rischio perché affronta le cause profonde della non conformità in modo olistico. Ad esempio, robusti controlli di sicurezza IT (cybersicurezza) prevengono sia le violazioni dei dati (GDPR) che i crimini informatici (D. Lgs. 231/2001). L'integrazione favorisce una cultura di compliance più coerente e consistente in tutta l'organizzazione. Quando i dipendenti percepiscono un approccio unificato alla gestione del rischio, piuttosto che regole disparate e talvolta contrastanti, si rafforza la comprensione e l'adesione. Questo trasforma la compliance da un onere burocratico a un asset strategico, rafforzando la natura

"preventiva" del MOGC e la sua capacità di superare il vaglio giudiziario.

3.3. Rafforzamento dell'Organismo di Vigilanza (OdV)

L'Organismo di Vigilanza (OdV) è centrale per l'efficacia del MOGC, essendo incaricato di supervisionare la sua osservanza e il suo funzionamento. Le sue funzioni includono la vigilanza sull'effettività del Modello (verificando la coerenza tra comportamenti concreti e modello istituito), il monitoraggio degli aggiornamenti, la gestione dei flussi informativi e la promozione della formazione. L'indipendenza e l'autonomia dell'OdV sono critiche per la sua credibilità ed efficacia. In considerazione della nuova legislazione, il ruolo dell'OdV si è ampliato: deve supervisionare i canali e le procedure di whistleblowing , monitorare i protocolli di cybersicurezza e collaborare con il Responsabile della Cybersicurezza , e assicurare un corretto flusso di informazioni con le funzioni finanza/controllo e il DPO. Ciò implica che Sage Castelli S.r.l. deve assicurare che il proprio OdV disponga di risorse adeguate, competenze (anche in nuove aree come la fiscalità e la cybersicurezza) e poteri chiaramente definiti per adempiere al suo mandato ampliato. La composizione dell'OdV e le sue linee di riporto interne devono garantirne l'indipendenza.
La continua espansione dei reati presupposto e degli obblighi di compliance (fiscali, whistleblowing, cyber) aumenta direttamente la complessità e il carico di lavoro dell'OdV. Ciò rende necessaria una rivalutazione della composizione, delle risorse e delle competenze dell'OdV. Un OdV con risorse insufficienti o competenze inadeguate farà fatica a monitorare efficacemente il MOGC ampliato, rendendo potenzialmente il modello inefficace in tribunale. Pertanto, investire nelle capacità dell'OdV non è solo un costo, ma un investimento strategico nella difesa legale e nella mitigazione del rischio dell'azienda. Questo include la formazione continua per i membri dell'OdV. Il ruolo dell'OdV si estende oltre la mera supervisione alla "vigilanza sull'effettività del Modello" e al "monitoraggio dell'aggiornamento del Modello". Ciò implica una funzione proattiva nell'identificazione dei rischi emergenti e nel raccomandare gli adeguamenti necessari al MOGC, piuttosto che reagire passivamente agli incidenti. Questa postura proattiva è cruciale per soddisfare lo standard di "attuazione effettiva" richiesto dalla giurisprudenza.

3.4. Formazione e Comunicazione Continua

Per promuovere una cultura di compliance robusta, sono essenziali una formazione e una comunicazione continue. La formazione dovrebbe coprire il MOGC, i principi etici, i protocolli specifici e le implicazioni della nuova legislazione (ad esempio, whistleblowing, reati tributari, rischi cyber). Il pubblico di riferimento include tutto il personale, dalla direzione al personale operativo, che deve comprendere i propri ruoli e responsabilità nella prevenzione dei reati. Sage Castelli S.r.l. necessita di un programma di formazione strutturato e continuativo, adattato ai diversi livelli

organizzativi e alle esposizioni al rischio. Le campagne di comunicazione dovrebbero rafforzare i principi del MOGC e l'importanza della condotta etica.

4. Recenti Tendenze Giurisprudenziali (2024-2025) e Implicazioni Pratiche

Questa sezione sottolinea la prospettiva giudiziaria sull'efficacia del MOGC, che è di primaria importanza per la difesa di Sage Castelli S.r.l..

4.1. Enfasi sull'Attuazione Effettiva

Un principio chiave emerso dalle recenti pronunce della Cassazione è che, affinché un MOGC sia esimente, deve essere *effettivamente attuato* e non meramente formalmente corretto. La sentenza della Cassazione n. 31665/2024, ad esempio, ha annullato una condanna, sottolineando che l'efficacia del MOGC è cruciale per escludere la responsabilità. Questo rafforza il concetto che la mera esistenza formale del modello non è sufficiente. Il concetto di "colpa di organizzazione" si configura quando l'ente non adotta un sistema adeguato di valutazione dei rischi e non implementa procedure operative specifiche. Può essere desunta da una "vera e propria politica aziendale di incuria" finalizzata al risparmio sui costi. Per Sage Castelli S.r.l., ciò implica la necessità di dimostrare che il proprio MOGC è genuinamente applicato, monitorato e aggiornato. Questo richiede prove documentate di formazione, implementazione dei controlli, azioni disciplinari e attività dell'OdV.

L'enfasi costante della Cassazione sull'"attuazione effettiva" rappresenta un indurimento definitivo del controllo giudiziario sui MOGC. Sposta l'onere della prova per il modello esimente dalla semplice adozione alla funzionalità dimostrabile e all'adattamento continuo. Il focus giudiziario sull'"attuazione effettiva" sposta il paradigma della compliance da un approccio incentrato sul documento a uno incentrato sul processo e basato sull'evidenza. Sage Castelli S.r.l. deve stabilire chiari processi interni per documentare le attività di compliance e l'efficacia dei controlli. Ciò significa che la progettazione del MOGC deve includere meccanismi di auto-valutazione e miglioramento continuo, che vengono poi documentati per una potenziale revisione giudiziaria. Questa tendenza giurisprudenziale rafforza la necessità di una "cultura della compliance" profondamente radicata all'interno dell'organizzazione, dove l'adesione al MOGC è compresa e praticata a tutti i livelli. Una "politica aziendale di incuria" può essere dedotta da fallimenti isolati se riflettono una negligenza sistemica. Pertanto, l'efficacia del MOGC è in definitiva legata all'impegno etico e alla diligenza di ogni individuo all'interno di Sage Castelli S.r.l..

4.2. "Vantaggio dell'Ente" e "Colpa di Organizzazione"

Il "vantaggio dell'ente" è un elemento essenziale per configurare la responsabilità amministrativa (Art. 5 D. Lgs. 231/01). La Cassazione ha implicitamente escluso il vantaggio se l'evento è stato tragico e non intenzionale. Tuttavia, anche un "esiguo

risparmio di spesa" può costituire un vantaggio, specialmente se inserito in un contesto di generale "incuria". La "colpa di organizzazione" si configura quando l'ente non adotta un sistema adeguato di valutazione dei rischi e non implementa procedure operative specifiche. Può essere inferita da una "vera e propria politica aziendale di incuria in materia antinfortunistica" finalizzata al risparmio sui costi. Il MOGC di Sage Castelli S.r.l. deve dimostrare chiaramente che qualsiasi condotta illecita non è stata intrapresa nell'interesse o a vantaggio dell'ente. Ciò richiede controlli interni robusti che impediscano ai dipendenti di perseguire "vantaggi" illeciti (ad esempio, risparmi sui costi a scapito della sicurezza o della compliance). Il MOGC dovrebbe anche affrontare esplicitamente come previene e gestisce la "colpa di organizzazione".
L'interpretazione sfumata di "vantaggio dell'ente" e "colpa di organizzazione" da parte della Cassazione rivela una sofisticata comprensione giudiziaria della motivazione aziendale e dei fallimenti sistemici. Anche risparmi sui costi apparentemente minori possono essere considerati un "vantaggio" se riflettono una più ampia "politica di incuria", collegando gli incentivi finanziari direttamente alla colpa organizzativa. L'enfasi sulla "colpa di organizzazione" come "politica aziendale di incuria" significa che i fallimenti sistemici, anche se non esplicitamente pianificati per commettere un crimine, possono essere interpretati come un difetto organizzativo colpevole. Questo costringe Sage Castelli S.r.l. a dare priorità alla compliance rispetto a guadagni finanziari a breve termine o scorciatoie operative, riconoscendo che tali "risparmi" comportano significativi rischi legali. Ciò implica che il quadro etico del MOGC deve affrontare esplicitamente la tensione tra la ricerca del profitto e la compliance. Se la "colpa di organizzazione" è collegata a una "politica aziendale", essa punta implicitamente alla responsabilità dell'"Organo di indirizzo" e della direzione senior nel definire il tono e la cultura. La "Parte Generale" del MOGC dovrebbe articolare chiaramente l'impegno della direzione alla compliance e i meccanismi per ritenere la leadership responsabile di promuovere una cultura che prevenga la colpa organizzativa.

4.3. Proporzionalità nei Sequestri Preventivi

La Cassazione sottolinea che i sequestri preventivi (ad esempio, per equivalente) devono rispettare il principio di proporzionalità, essere adeguatamente motivati e giustificare la necessità di anticipare l'effetto ablativo rispetto alla definizione del giudizio. Il sequestro per equivalente richiede un "nesso di strumentalità" tra l'attività illecita e l'ente. Sebbene questo sia un aspetto procedurale, esso evidenzia l'importanza di un MOGC ben progettato ed efficacemente implementato come meccanismo di difesa. Un MOGC robusto può aiutare a dimostrare l'assenza di un "nesso di strumentalità" o a mitigare la necessità percepita di misure così severe.

Evoluzioni del quadro normativo intercorse tra la fine del 2025 e il primo semestre del 2026.

A. Introduzione dell'Art. 25-octies.2 – Violazione delle Misure Restrittive UE (D.Lgs. n. 211/2025)
A seguito dell'entrata in vigore del D.Lgs. 30 dicembre 2025, n. 211 (attuativo della Direttiva UE 2024/1226), è stata introdotta nel paniere dei reati presupposto 231 la fattispecie di cui al nuovissimo Articolo 25-octies.2.
• Ambito di applicazione: La norma sanziona gli enti nel cui interesse o vantaggio sia posta in essere la violazione di blocchi commerciali, embarghi economici o l'omesso congelamento di risorse finanziarie e patrimoniali nei confronti di Stati o entità sottoposte a misure restrittive dall'Unione Europea.
• Implicazioni per Sage Castelli S.r.l.: Il rischio potenziale si concentra nell'area Approvvigionamenti e Logistica. L'ufficio acquisti ha l'obbligo di adottare protocolli di Due Diligence sui fornitori e importatori terzi di macchinari sanitari complessi, reattivi di laboratorio e dispositivi medici, verificando che la filiera distributiva non sia collegata direttamente o indirettamente a soggetti iscritti nelle blacklist dell'Unione Europea.

B. Aggravanti connesse all'uso di Sistemi di Intelligenza Artificiale (Legge n. 132/2025)
La Legge n. 132/2025 in materia di Intelligenza Artificiale ha introdotto un severo inasprimento sanzionatorio modificando l'applicazione di reati presupposto già esistenti nel catalogo 231.
• Profili impattati: Vengono inserite specifiche aggravanti per i Reati Societari (Art. 25-ter) e per i Delitti contro il Diritto d'Autore (Art. 25-novies) laddove la condotta illecita sia perpetrata mediante l'ausilio di sistemi di IA o algoritmi automatizzati.
• Protocolli di controllo: Viene introdotto il divieto assoluto per i dipendenti e i consulenti di Sage Castelli S.r.l. di ricorrere a sistemi di IA generativa non preventivamente autorizzati dal reparto IT e dall'OdV per l'elaborazione di dati contabili, report di bilancio o comunicazioni aziendali esterne, nonché il divieto di praticare attività di estrazione dati (data scraping) su banche dati protette da privativa intellettuale.

3. Migliori Prassi per il Potenziamento e l'Integrazione del MOGC

Rafforzamento dell'Organismo di Vigilanza (OdV) e Flussi Informativi
In linea con il consolidato orientamento espresso dalla Corte di Cassazione (sent. n. 30039/2025), l'efficacia esimente del Modello Organizzativo è subordinata alla sua attuazione "concreta e dinamica" e non a una conformità meramente documentale o cartacea. Per garantire l'effettività delle verifiche, Sage Castelli S.r.l.

istituzionalizza un flusso informativo semestrale e vincolante da parte del Responsabile del Servizio di Prevenzione e Protezione (RSPP) verso l'OdV, avente ad oggetto il registro dei quasi-incidenti, l'aggiornamento dinamico del DVR e lo stato di completamento della formazione obbligatoria del personale medico e infermieristico.

4. Recenti Tendenze Giurisprudenziali (Aggiornamento 2026)

Autonomia della Tutela Legale dell'Ente e Conflitto di Interessi Processuale
Un principio cardine di matrice giurisprudenziale affermatosi nel corso del primo semestre del 2026 impone la revisione delle procedure della "Parte Generale" relative alla gestione del contenzioso penale e alla rappresentanza in giudizio della società.

- Il Principio: Sussiste una netta incompatibilità oggettiva qualora la procura speciale al difensore di fiducia dell'ente (chiamato a rispondere dell'illecito amministrativo 231) venga conferita dal Legale Rappresentante (Amministratore Unico) che risulti contemporaneamente indagato o imputato, come persona fisica, per il medesimo reato presupposto. Il potenziale conflitto di interessi inficia la validità degli atti costitutivi dell'ente in giudizio.
- Procedura di Salvaguardia per Sage Castelli S.r.l.: Qualora la Società sia attinta da un procedimento ex D.Lgs. 231/2001 e l'azione penale coinvolga l'Organo Amministrativo, la facoltà di nomina e il conferimento della procura al difensore dell'ente dovranno essere sottratti all'Amministratore in conflitto e demandati tassativamente all'Assemblea dei Soci o a un Procuratore Speciale appositamente nominato su formale input dell'Organismo di Vigilanza.

5. Tabella Riassuntiva dei Nuovi Reati e Presidi (Integrazione 2026)

Articolo MOGC	Fattispecie di Reato / Riforma	Fonte Normativa	Presidio Operativo Richiesto
Art. 25-octies.2	Violazione delle misure restrittive e degli embarghi commerciali UE.	D.Lgs. n. 211/2025 (Direttiva UE 2024/1226)	Due Diligence obbligatoria sui fornitori di apparecchiature elettromedicali complesse. Verifiche sulle blacklist dell'Unione Europea.

Art. 25-ter / Art. 25-novies	Aggravanti per reati societari e diritto d'autore tramite sistemi algoritmici.	Legge n. 132/2025 (Disciplina dell'Intelligenza Artificiale)	Adozione di una Policy Aziendale sull'uso dell'IA. Divieto di utilizzo di applicativi non autorizzati per bilanci, report e data scraping.
Parte Generale (Tutela Legale)	Incompatibilità nella nomina del difensore dell'ente in caso di co-indagato.	Giurisprudenza di Legittimità (Primo Semestre 2026)	Sottrazione del potere di nomina all'Amministratore in conflitto; delega esclusiva all'Assemblea dei Soci o a un Procuratore Speciale.