

Novembre 2026

flash infopaper

Compliance & Risk Management

compliance normativa | anticorruzione

privacy | giurisprudenza

Compliance normativa

- Prevenzione delle frodi fiscali: l'importanza dell'integrazione tra Tax Control Framework e Modello 231
- Applicazione delle misure straordinarie ex art. 32 del D.L. 90/2014: la rilevanza istruttoria e decisoria del Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001

Anticorruzione

- Riservatezza del segnalante e limiti del sindacato sulla gestione della segnalazione
- Inconferibilità di incarico tecnico ex art. 110 TUEL e periodo di raffreddamento

Privacy

- Dati sanitari pseudonimizzati e finalità di ricerca: il Garante esclude l'anonimizzazione e accerta la titolarità della società fin dalla raccolta dei dati

Giurisprudenza

- Lavoratori esterni: il Datore di lavoro ha obbligo di adottare tutte le misure idonee alla loro tutela (Cass. Pen., Sez. IV, n. 28518/2026)
- Mancanza del Modello e responsabilità dell'ente: la Cassazione esclude l'automatismo e richiede la colpa di organizzazione (Cass. pen., Sez. III, 28/09/2026, n. 34744)

Prevenzione delle frodi fiscali: l'importanza dell'integrazione tra Tax Control Framework e Modello 231

Tra i recenti chiarimenti forniti dall'Agenzia delle Entrate in materia di adempimento collaborativo, assume particolare rilevanza il tema della prevenzione dei rischi di frode fiscale derivanti da condotte poste in essere da soggetti terzi. In dettaglio, con la Circolare n. 6/E del 6 agosto 2026, l'Agenzia delle Entrate ha approfondito il ruolo del Tax Control Framework (TCF), evidenziandone la funzione di presidio non solo per l'individuazione e la gestione dei rischi fiscali, ma anche per il monitoraggio dei rischi connessi ai rapporti con fornitori, clienti e altri partner commerciali.

L'Agenzia ha chiarito che il presidio dei rischi di frode fiscale può ritenersi adeguatamente implementato mediante l'adozione di un Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001, a condizione che quest'ultimo sia efficacemente integrato con il TCF aziendale.
Secondo quanto precisato dall'Amministrazione finanziaria, tale integrazione richiede che i rischi fiscali connessi a potenziali fenomeni fraudolenti siano identificati, valutati e presidiati attraverso specifiche misure di controllo, tra cui:

- l'individuazione dei reati tributari rilevanti ai fini del D.Lgs. 231/2001;
- la mappatura dei rischi fiscali riconducibili a condotte fraudolente;
- l'introduzione di specifici presidi antifrode nell'ambito del sistema di controllo;
- il monitoraggio periodico di secondo livello finalizzato ad accertare l'efficacia dei controlli implementati;
- la definizione di adeguati flussi informativi tra l'Organismo di Vigilanza e la funzione responsabile della compliance fiscale.

A tal proposito, assume particolare rilevanza l'esigenza che i presidi adottati risultino proporzionati e concretamente adeguati alle specificità del business, alla struttura organizzativa e al profilo di rischio della singola impresa.

I chiarimenti forniti dall'Agenzia confermano la crescente convergenza tra i sistemi di controllo fiscale e i modelli di compliance aziendale, evidenziando come l'efficacia del Tax Control Framework presupponga un coordinamento sempre più stretto con gli altri presidi di controllo interno.

Fonte: Circolare n. 6/E/2026 del 6 agosto 2026

Applicazione delle misure straordinarie ex art. 32 del D.L. 90/2014: la rilevanza istruttoria e decisoria del Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001

L'Autorità Nazionale Anticorruzione (ANAC) ha recentemente aggiornato la disciplina relativa al procedimento concernente l'esercizio del potere di proposta del Presidente dell'ANAC per l'applicazione delle misure straordinarie previste dall'articolo 32, commi 1 e 8 del D.L. 90/2014, convertito con modificazioni dalla Legge 114/2014 e s.m.i.. Più dettagliatamente, nei confronti delle imprese aggiudicatarie di appalti pubblici coinvolte in procedimenti penali per reati di corruzione, l'art. 32, al comma 1 disciplina la gestione straordinaria dell'impresa limitatamente alla completa esecuzione del contratto d'appalto, c.d. commissariamento; mentre al comma 8 prevede la misura alternativa di sostegno e monitoraggio dell'impresa, mediante l'affiancamento da parte di soggetti esperti.

Le nuove disposizioni, entrate in vigore l'11 settembre 2026, in sostituzione della precedente disciplina del 16 settembre 2022, valorizzano maggiormente l'adozione del Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001 (MOGC) da parte degli enti.

Il Modello si configura quale potenziale ed efficace strumento di tutela per gli enti coinvolti in procedimenti penali per reati di corruzione o di criminalità organizzata collegati ad un contratto di appalto o di concessione ovvero ad un accordo contrattuale con il Servizio Sanitario Nazionale.

In particolare, le nuove disposizioni ANAC richiamano il Modello di Organizzazione, Gestione e Controllo nei seguenti aspetti:

- ai fini della verifica dei presupposti per l'esercizio dei poteri di proposta per l'applicazione delle misure straordinarie, il Presidente dell'ANAC si avvale di una informativa che deve indicare se l'operatore economico abbia adottato il MOGC ovvero sia in possesso di certificazioni ISO per la prevenzione della corruzione;
- viene sancito l'obbligo di disporre l'archiviazione d'ufficio del procedimento nell'ipotesi in cui sia già intervenuto il commissariamento dell'ente disposto dall'Autorità Giudiziaria ai sensi dell'art. 45, comma 3, del D.Lgs. 231/2001;
- ai fini delle determinazioni finali da adottare — alternativamente tra l'archiviazione del procedimento o la formulazione di una proposta al Prefetto competente di applicazione di una o più delle misure previste dall'art. 32 — il Presidente dell'ANAC deve considerare l'adozione di misure cautelari, l'irrogazione di sanzioni amministrative, la contestazione di illeciti amministrativi dipendenti da reato nei confronti dell'operatore economico ai sensi del Decreto Legislativo n. 231/2001 nonché il comportamento assunto dall'operatore economico affidatario a seguito della contestazione o notizia della vicenda corruttiva/illecita e, in particolare il c.d. self-cleaning, ovvero l'adozione di misure, condotte o atti realmente dissociativi rispetto ai soggetti cui sono riferibili le condotte illecite (tra cui l'adozione di MOGC) e la presentazione di impegni idonei a ripristinare spontaneamente il rispetto della legalità all'interno dell'operatore economico.

Fonte: Disposizioni per la disciplina del procedimento preordinato alla proposta del presidente dell'anac di adozione delle misure straordinarie ai sensi dell'articolo 32, del d.l. 90/2014, convertito con modificazioni dalla legge 114/2014, e s.m.i..

Riservatezza del segnalante e limiti del sindacato sulla gestione della segnalazione

Con la delibera n. 344 del 9 settembre 2026, l'Autorità Nazionale Anticorruzione (ANAC) ha irrogato una sanzione di € 15.000 a ciascun componente dell'organo cui una società privata aveva affidato la gestione del canale interno di segnalazione, a seguito dell'accertamento della violazione dell'obbligo di riservatezza dell'identità del segnalante (art. 12 D.Lgs. n. 24/2023, sanzionabile ai sensi dell'art. art. 21, comma 1, lett. a) D.Lgs. n. 24/2023).

La vicenda trae origine da una segnalazione anonima, presentata da un dipendente il 9 dicembre 2024, relativa a presunte modifiche fittizie di un contratto con un cliente, finalizzate a consentirne la fatturazione entro la chiusura dell'esercizio, su sollecitazione della controparte. Il 19 dicembre era seguita una contestazione disciplinare e il 27 gennaio 2025 il licenziamento, poi dichiarato ritorsivo e nullo con sentenza non ancora definitiva.

In via preliminare, ANAC ha riconosciuto la sussistenza dei presupposti soggettivi e oggettivi per l'applicazione della tutela prevista dal D.Lgs. n. 24/2023 in favore del segnalante. In particolare, ANAC ha sottolineato che l'art. 12, comma 2, estende la protezione non soltanto all'identità in senso stretto ma a «qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente» tale identità. La violazione può pertanto configurarsi anche in assenza di un'esplicita rivelazione del nominativo, qualora le informazioni disponibili siano sufficienti a consentire l'identificazione, anche indiretta, della persona che ha effettuato la segnalazione. L'Autorità ha evidenziato che la gestione di una segnalazione whistleblowing presenta caratteristiche peculiari rispetto a quelle ordinarie, richiedendo al gestore un costante bilanciamento tra l'accertamento della fondatezza dei fatti segnalati e la tutela della riservatezza dell'identità del whistleblower, del segnalato, del contenuto della segnalazione e delle persone menzionate.

In tale quadro di opposte esigenze, il comportamento dei membri dell'organo di gestione è risultato privo della dovuta "diligenza", in quanto la gestione "circoscritta" della segnalazione ha pregiudicato, in concreto, la riservatezza. Infatti:

- il perimetro dell'indagine è risultato eccessivamente ristretto ovvero riferito esclusivamente al singolo e specifico contratto e al relativo team di lavoro;
- ai soggetti intervistati veniva comunicato che venivano sentiti in quanto coinvolti nel contratto o comunque citati nella documentazione trasmessa dal segnalante;
- durante le audizioni sono state fornite informazioni "identificanti" (contratto e cliente citati nella segnalazione);
- erano presenti dati di contesto noti a tutti i soggetti intervistati (caratteristiche del segnalante riferibili alla sua seniority e al suo ruolo, precedenti azioni di escalation);
- sebbene per ANAC non utile all'accertamento dei fatti, è stato ascoltato il superiore gerarchico del soggetto segnalato, a cui erano note le problematiche professionali esistenti tra segnalante e segnalato, con conseguente imprudente circolazione di informazioni;
- nonostante la segnalazione fosse stata presentata in forma anonima, prima ancora dell'inizio formale dell'audizione il Presidente dell'Organo di gestione si è rivolto al segnalante facendo intendere che la sua identità fosse già nota;
- dopo le audizioni il segnalante è stato escluso da tutte le attività e comunicazioni riguardanti il contratto.

ANAC ha quindi qualificato la condotta dei gestori come colposa per la mancata adozione delle necessarie cautele. A tal fine, ANAC ha richiamato l'opportunità di ampliare apparentemente il perimetro delle verifiche, ad esempio, riconducendole ad attività di compliance auditing, così da ridurre il rischio di identificazione del segnalante.

Fonte: Delibera n. 344 del 9 settembre 2026

Inconferibilità di incarico tecnico ex art. 110 TUEL e periodo di raffreddamento

L'Autorità Nazionale Anticorruzione, con Delibera n. 371 del 23 settembre 2026, ha concluso un procedimento di vigilanza relativo all'ipotesi di inconferibilità dell'incarico di Responsabile dell'Ufficio Tecnico nei confronti di un'amministrazione comunale. L'attività istruttoria è stata avviata d'ufficio per verificare la legittimità del conferimento disposto, in data 26 febbraio 2025, a favore di un professionista esterno quale funzionario tecnico a tempo determinato ex art. 110, comma 1, del TUEL (Area dei Funzionari e dell'Elevata Qualificazione) e della successiva nomina, in data 6 marzo 2025 (rinnovata l'8 gennaio 2026), a Responsabile del 3° Settore "Area Tecnico Manutentiva".

L'attribuzione dell'incarico è avvenuta a fronte di molteplici e pregressi rapporti tra l'ente e il professionista, già "Esperto del Sindaco" nonché socio e amministratore unico di una società privata proponente un progetto tecnologico per il depuratore comunale.

L'Autorità ha rilevato le seguenti violazioni di carattere normativo e operativo:

- mancato rispetto del "periodo di raffreddamento": il professionista incaricato della responsabilità del 3° Settore aveva svolto per conto del medesimo ufficio un'attività professionale continuativa e remunerata per l'aggiornamento del Piano Comunale di Protezione Civile, affidata nel maggio 2019 e conclusa con la consegna della Relazione Generale il 24 gennaio 2025, ossia a distanza di un mese dall'assunzione delle funzioni gestionali e direttive. Tale circostanza ha integrato la violazione dell'art. 4, comma 1, lett. c), del d.lgs. 39/2013 («Inconferibilità di incarichi nelle amministrazioni statali, regionali e locali a soggetti provenienti da enti di diritto privato regolati o finanziati») in combinato disposto con l'art. 1, comma 2, lett. k), del d.lgs. 39/2013 («Definizioni»);
- inottemperanza agli obblighi in materia di dichiarazioni e trasparenza: la dichiarazione di insussistenza di cause di inconferibilità è stata sottoscritta dall'interessato in data 27 febbraio 2025 ma non è mai stata acquisita formalmente agli atti dell'ente né pubblicata nella sezione "Amministrazione Trasparente", ed è stata del tutto omessa in occasione dei successivi decreti sindacali di assegnazione dell'incarico di Responsabile di Settore, in contrasto con l'art. 20 del d.lgs. 39/2013 («Dichiarazione sulla insussistenza di cause di inconferibilità o incompatibilità»).

Alla luce di tali criticità, l'ANAC ha accertato l'inconferibilità dell'incarico, dichiarando la nullità di diritto dell'atto di conferimento e del relativo contratto ai sensi dell'art. 17 del d.lgs. 39/2013 («Nullità degli incarichi conferiti in violazione delle disposizioni del presente decreto»).

Contestualmente, l'Autorità ha demandato al Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) il compito di:

- comunicare formalmente all'interessato la sussistenza della causa di inconferibilità e la relativa nullità, assistendo l'ente nell'adozione dei provvedimenti conseguenti;
- verificare il rispetto della disciplina sulle dichiarazioni sostitutive e la veridicità di quanto dichiarato, la cui eventuale falsità comporta l'inconferibilità di qualsivoglia incarico per la durata di cinque anni ai sensi dell'art. 20, comma 5, del d.lgs. 39/2013 («Dichiarazione sulla insussistenza di cause di inconferibilità o incompatibilità»);
- avviare la procedura sanzionatoria ex art. 18 del d.lgs. 39/2013 («Sanzioni») nei confronti dei componenti dell'organo che hanno disposto la nomina, con conseguente inibizione trimestrale della facoltà di conferire ulteriori incarichi amministrativi.

Fonte: Delibera n. 371 del 23 settembre 2026

Dati sanitari pseudonimizzati e finalità di ricerca: il Garante esclude l'anonimizzazione e accerta la titolarità della società fin dalla raccolta dei dati

Con il provvedimento n. 710 del 23 settembre 2026, il Garante per la protezione dei dati personali ha dichiarato illecito il trattamento effettuato da una società attiva nell'analisi dei dati sanitari e nella ricerca clinica, accertando la violazione degli artt. 5, 9, 13, 25, 28, 32 e 35 del GDPR. L'Autorità ha inoltre disposto una sanzione amministrativa pecuniaria di 7 milioni di euro – con massimo edittale calcolato sul fatturato della capogruppo statunitense –, ordinando alla società, qualora intenda proseguire l'attività, di conformare il trattamento entro 120 giorni. L'istruttoria, nata da accertamenti ispettivi, ha riunito il procedimento sul *data breach* notificato dalla società. Oggetto delle verifiche è stata una banca dati contenente informazioni sulla salute di circa un milione di pazienti di 800 medici di medicina generale, alimentata tramite un modulo aggiuntivo installato nel *software* gestionale dei medici e utilizzata per studi commissionati da aziende farmaceutiche.

Il nodo centrale riguarda la natura dei dati. La società sosteneva che le informazioni fossero anonime, richiamando la recente giurisprudenza della Corte di Giustizia UE (causa C-413/23). Secondo il Garante, invece, i dati erano soltanto pseudonimizzati e restavano quindi dati personali: il codice identificativo stabile associato a ciascun paziente consentiva di seguirlo nel tempo e, unito a un patrimonio informativo dettagliato (anno di nascita, sesso, diagnosi, prescrizioni, esami, vaccinazioni e dati di localizzazione), rendeva possibile isolare i singoli individui e, con mezzi ragionevoli, reidentificarli. Né erano sufficienti le misure adottate dalla società: la codifica del codice identificativo ne nascondeva il collegamento diretto con il paziente, ma non impediva di seguirlo nel tempo, mentre la generalizzazione dei soli dati anagrafici lasciava intatto un patrimonio informativo così dettagliato da consentire, da solo, di isolare i singoli individui. L'Autorità ha inoltre escluso che il precedente europeo potesse applicarsi a un soggetto che, come nel caso di specie, aveva un ruolo attivo nella definizione delle misure di pseudonimizzazione e non quello di mero destinatario dei dati.

Una seconda questione ha riguardato la titolarità del trattamento. La società si qualificava come mero supporto tecnologico e finanziario di un progetto promosso da una società scientifica di medicina generale. Il Garante l'ha invece ritenuta titolare dell'intero trattamento fin dalla raccolta presso i medici, avendone determinato finalità e mezzi, gestito i rapporti con i professionisti e commissionato lo sviluppo del modulo di estrazione. Il Garante ha invece ritenuto giustificata la fiducia riposta dai medici e dalla società scientifica nel modulo di estrazione, che la società aveva presentato come idoneo a rendere anonimi i dati. La mancata designazione dei medici quali responsabili del trattamento ha comportato anche la violazione dell'art. 28 GDPR.

Il trattamento di dati sanitari – inclusa la stessa anonimizzazione -,richiedeva una delle condizioni di liceità previste dall'art. 9 GDPR, che nel caso di specie non sussisteva: il contratto stipulato con i medici non poteva, infatti, costituire una base giuridica, non essendone parte i pazienti, né era stato acquisito il loro consenso esplicito. Anche le informazioni rese agli interessati sono state ritenute inadeguate. Ulteriori rilievi hanno riguardato la mancata definizione dei tempi di conservazione, oltre che l'omessa valutazione d'impatto, mai completata nonostante il trattamento riguardasse dati sanitari di interessati vulnerabili. Irrilevante, per il Garante, che il trattamento fosse iniziato prima dell'applicazione del GDPR: anche i sistemi preesistenti devono essere verificati e aggiornati.

Sotto il profilo della sicurezza, è emerso che il modulo estraeva anche i campi di testo libero - compilati dai medici -, nei quali erano presenti dati identificativi diretti: nella banca dati sono così confluiti nomi, codici fiscali e recapiti di circa 3.370 pazienti, di cui oltre 3.000 insieme a dati sulla salute, poi comunicati anche alla società scientifica, in violazione degli artt. 5, 12 e 13 GDPR. Il Garante ha escluso che i medici avessero commesso un errore, poiché l'inserimento di tali informazioni nel gestionale rispondeva a finalità di cura: la responsabilità ricade sulla società, che non aveva verificato che il modulo escludesse dall'estrazione i campi di testo libero, peraltro non necessari al progetto. L'Autorità ha inoltre rilevato che la società si era basata esclusivamente sulle valutazioni di anonimato svolte da una società del gruppo, senza ulteriori analisi sul rischio di reidentificazione né controlli sui dati effettivamente raccolti, in violazione dei principi di responsabilizzazione e di protezione dei dati fin dalla progettazione.

Se intende proseguire, la società dovrà individuare una base giuridica, informare i pazienti, completare la valutazione d'impatto e nominare i medici responsabili del trattamento. In alternativa, il Garante ha indicato le condizioni alle quali l'anonimizzazione potrà essere svolta dai medici prima dell'invio dei dati. Anzitutto, saranno i medici a decidere, senza alcun intervento della società, come sostituire i dati identificativi dei pazienti con codici privi di significato. Inoltre, le informazioni che combinate tra loro possono rendere riconoscibile una persona, come età, sesso o comune di residenza, dovranno essere generalizzate in modo che ciascun profilo corrisponda ad almeno 10 pazienti. Lo stesso vale per ogni altro dato, ad esempio diagnosi o terapie, che la società potrebbe conoscere per altre vie e usare per riconoscere qualcuno. Questi dati andranno generalizzati allo stesso modo, eliminati, oppure elaborati con tecniche crittografiche che consentono di svolgere analisi statistiche senza mai vedere il dato completo (c.d. secure *multiparty computation*). Le stesse regole varranno nell'ipotesi in cui sarà la società a voler, a sua volta, comunicherà i dati a terzi.

La decisione conferma dunque he la qualificazione dei dati come anonimi deve essere supportata da un'analisi concreta del rischio di reidentificazione e che la pseudonimizzazione, pur costituendo una misura di sicurezza, non sottrae il trattamento all'applicazione del GDPR. Soprattutto, chiarisce che chi definisce o governa le misure di pseudonimizzazione non può invocare la sentenza C-413/23 per considerarsi destinatario di dati anonimi.

Fonte: Garante per la protezione dei dati personali, Provvedimento n. 710 del 23 settembre 2026.

Lavoratori esterni: il Datore di lavoro ha obbligo di adottare tutte le misure idonee alla loro tutela (Cass. Pen., Sez. IV, n. 28518/2026)

La sentenza della Corte di Cassazione del 28518/2026 del 28 luglio 2026 si esprime sul riscorso avverso la sentenza della Corte di Appello di Ancona del 25/03/2026 nell'ambito del reato di lesioni personali colpose gravi aggravate derivanti dalla violazione della normativa antinfortunistica, commesso in danno di un lavoratore di una società esterna, confermando la responsabilità del datore di lavoro della macroarea e delegato in materia di sicurezza.

Secondo l'imputazione, il datore di lavoro ha cagionato per colpa le lesioni personali gravi, derivanti da un investimento da parte di un'autobetoniera in retromarcia, omettendo la predisposizione di una postazione sicura e separata dall'area di circolazione e manovra delle autobetoniere.

Il ricorso per Cassazione aveva evidenziato i seguenti aspetti:

- la Corte di Appello non ha verificato che l'adozione della misura omessa avrebbe effettivamente impedito l'evento infortunistico;
- l'impossibilità di predisporre una postazione sicura e segregata per via dell'estensione dell'area di manovra delle betoniere;
- l'organo di vigilanza aveva considerato impossibile o non necessaria l'individuazione di una specifica area dedicata reputando, invece, sufficiente la delimitazione e segnalazione delle aree di transito dei mezzi.

Gli Ermellini hanno rigettato il ricorso e confermato la responsabilità del Datore di lavoro in quanto:

- la Corte di Appello di Ancona ha accertato in maniera adeguata, esposta coerentemente agli elementi probatori, che la misura di sicurezza da adottare era la creazione di una postazione protetta e ha logicamente ritenuto che tale misura organizzativa avrebbe evitato l'esposizione del lavoratore al rischio concretizzatosi nell'investimento da parte dell'autobetoniera in manovra;
- il Datore, ai sensi dell'art. 2, comma 1, lett. b), d.lgs. n.81 del 2008, aveva l'obbligo giuridico di provvedere in tal senso, riconducendo l'infortunio non alla mancata previsione delle misure di sicurezza idonee a prevenirlo ma alla mancata adozione delle stesse;
- l'adempimento degli obblighi di prevenzione riguarda anche la presenza nel luogo di lavoro di un lavoratore dipendente di altra impresa ovvero qualsiasi persona presente nel luogo di lavoro, a prescindere dalla sussistenza delle fattispecie contrattuali previste dall'art. 26 d.lgs. n. 81 del 2008.

La Corte di Cassazione, infine, sottolinea che deve essere posta maggior tutela proprio per i soggetti esterni in quanto sono più distanti dalle informazioni e dalle prassi aziendali e il lavoratore esterno, in coerenza con l'art. 18, lett. e), d.lgs n. 81 del 2008 che obbliga il datore di lavoro a «prendere le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio grave e specifico, va tutelato mediante la sua collocazione in aree meno rischiose».

Fonte: Corte di Cassazione - IV Sez. Penale - sentenza 28 luglio 2026 n. 28518/2026 (udienza 16/01/2026)

Mancanza del Modello e responsabilità dell'ente: la Cassazione esclude l'automatismo e richiede la colpa di organizzazione (Cass. pen., Sez. III, 28/09/2026, n. 34744)

Con la sentenza n. 34744 del 28 settembre 2026, la Corte di Cassazione, Sezione III Penale, ha riaffermato un principio centrale in tema di responsabilità dell'ente *ex* D. Lgs. 231/2001: la mancata adozione, l'inidoneità o l'inefficace attuazione del Modello non determinano automaticamente la responsabilità della società. Occorre, invece, accertare una specifica "colpa di organizzazione" e il nesso causale tra la carenza organizzativa e il reato presupposto.

Il caso riguardava una società condannata, in primo grado e in appello, a una sanzione pecuniaria per l'illecito dipendente dal reato di truffa aggravata per il conseguimento di erogazioni pubbliche (*ex* artt. 24 D. Lgs. 231/2001 e 640-*bis* c.p.). In particolare, il legale rappresentante aveva predisposto e presentato documentazione non veritiera sullo stato di avanzamento di un progetto, per ottenere dall'Assessorato regionale competente una quota e il saldo del finanziamento. La società ricorrente, per quanto qui di interesse, lamentava che la colpa di organizzazione fosse stata fondata sulla sola assenza del Modello all'epoca dei fatti, con una motivazione apparente, difettando una verifica concreta delle specifiche cautele organizzative e gestionali che sarebbero state necessarie per prevenire il reato.

La Corte, in risposta alla censura, ha richiamato i precedenti arresti giurisprudenziali sul tema, ricordando che l'ente risponde per un fatto proprio e non per un fatto altrui. Per escludere forme di responsabilità oggettiva si richiede, invero, l'accertamento della colpa di organizzazione, cioè della mancata predisposizione di accorgimenti preventivi idonei a evitare reati del tipo di quello realizzato.

L'assenza, l'inidoneità o l'inefficace attuazione dei Modelli di organizzazione previsti dagli artt. 6 e 7 del D. Lgs. 231/2001 non sono elementi costitutivi dell'illecito dell'ente. Lo sono invece la cosiddetta immedesimazione organica "rafforzata" tra autore del reato ed ente, la colpa di organizzazione, il reato presupposto e il nesso causale che li lega.

Nel caso concreto, la Corte ha ritenuto provata la colpa di organizzazione, confermando la valutazione dei giudici di merito. Sono stati considerati il reato commesso da una figura apicale con condotta fraudolenta, organizzata e reiterata nel tempo allo scopo di conseguire un'utilità (c.d. interesse o vantaggio) per l'ente, la mancata predisposizione e attuazione dei Modelli di organizzazione, gestione e controllo previsti dal Legislatore, nonché un deficit organizzativo complessivo, consistente soprattutto nell'omessa predisposizione di un organismo di controllo contabile e di verifica delle attività del progetto finanziato. Tali elementi sono stati ritenuti dimostrativi della condotta colpevole della società e dotati di incidenza causale rispetto al reato. Pertanto, la Corte, escludendo un addebito di responsabilità oggettiva, ha dichiarato inammissibile il ricorso della società.

Fonte: Cass. pen., Sez. III, Sent., 28/09/2026, n. 34744

CONTATTI

BDO Advisory Services S.r.l.
Via San Raffaele, 5
20121 Milano
Tel. 02 58 20 10
ras@bdo.it

BDO è tra le principali organizzazioni internazionali di servizi professionali alle imprese.

Audit | Advisory | Digital | Tax | Law

Il Flash Info Paper viene pubblicato con l'intento di tenere aggiornati i clienti sugli sviluppi in ambito Risk & Compliance. Nonostante l'attenzione con cui è stata preparata, la presente pubblicazione deve essere considerata soltanto come un'indicazione di massima e non può, in nessuna circostanza, essere associata, in parte o in toto, ad un'opinione espressa da BDO. Non si deve fare affidamento sulla pubblicazione per trattare situazioni specifiche e non si deve agire, o astenersi dall'agire, sulla base delle informazioni ivi contenute senza un parere professionale specifico. Si prega di rivolgersi alla società membro di BDO della propria area geografica per discutere di queste questioni tenendo conto delle proprie particolari circostanze. La redazione di questo numero è stata completata il 4 novembre 2026.

BDO Advisory Services S.r.l., società a responsabilità limitata, è membro di BDO International Limited, società di diritto inglese (company limited by guarantee), e fa parte della rete internazionale BDO, network di società indipendenti. BDO è il marchio utilizzato dal network BDO e dalle singole società indipendenti che ne fanno parte.

BDO Advisory Services S.r.l. si riserva ogni diritto di utilizzo e riproduzione di tutti i contenuti qui riportati. Precisando che è fatto anche divieto di utilizzo degli stessi per addestrare sistemi di intelligenza artificiale.

© 2026 BDO Advisory Services S.r.l.- Flash Info Paper - Tutti i diritti riservati.

www.bdo.it

NEWSLETTER

Vuoi ricevere aggiornamenti e notizie da BDO direttamente via email?
Iscriviti alle nostre mailing list.