



13 PARTE SPECIALE - REATI RILEVANTI PER L'ATTIVITÀ DELLO STUDIO

13.1 PREMESSA GENERALE

La presente Parte Speciale integra la Parte Generale del Modello di Organizzazione, Gestione e Controllo adottato dallo Studio ai sensi del **D. Lgs. 231/2001**, ed è finalizzata a individuare e descrivere i reati potenzialmente rilevanti in relazione alle attività svolte, nonché a definire i presidi e i principi di comportamento volti a prevenire la loro commissione.

Lo Studio svolge principalmente attività di **consulenza, formazione, audit e assistenza tecnica** in materia di:

- salute e sicurezza sul lavoro (D. Lgs. 81/2008);
- qualità (ISO 9001);
- ambiente (ISO 14001);
- privacy e protezione dei dati (Reg. UE 2016/679 e D. Lgs. 196/2003);
- modelli di organizzazione e gestione ex D. Lgs. 231/2001;
- compliance e responsabilità amministrativa d'impresa.

La natura consulenziale e formativa dell'attività comporta un'esposizione al rischio-reato **non diretta**, ma **mediata** attraverso:

- i rapporti con la Pubblica Amministrazione e con enti di accreditamento;
- la gestione di dati e documenti sensibili di clienti;
- la sicurezza dei luoghi di lavoro interni e durante le attività presso clienti;
- la correttezza nella gestione economico-amministrativa e nelle relazioni contrattuali;
- la tutela ambientale e informatica.

Le sezioni seguenti analizzano le categorie di reati ritenute potenzialmente rilevanti per lo Studio Samele S.r.l.

13.2 REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

13.2.1 Riferimenti normativi

- Artt. 24 e 25 del D. Lgs. 231/2001
- Artt. 316-bis, 316-ter, 317, 318, 319, 319-ter, 319-quater, 320, 321, 322, 322-bis, 323, 640 co.2 n.1, 640-bis, 640-ter c.p.

13.2.2 Descrizione

Si tratta di reati che coinvolgono rapporti diretti o indiretti con pubblici ufficiali o incaricati di pubblico servizio, anche mediante l'indebita percezione o gestione di fondi pubblici, erogazioni, contributi o accreditamenti.

13.2.3 Aree di rischio per lo Studio Samele S.r.l.

- **Partecipazione a bandi e gare pubbliche** per l'erogazione di corsi di formazione finanziati o progetti cofinanziati da enti pubblici (es. Regioni, INAIL, Fondi Interprofessionali);
- **rendicontazione di contributi pubblici** o utilizzo di fondi destinati a specifiche iniziative formative;



- **rapporti con enti di accreditamento** (Regioni, ASL, INAIL, Ispettorato Nazionale del Lavoro) per pratiche autorizzative o di certificazione;
- **attività ispettive o di verifica** da parte di enti pubblici o organismi di controllo;
- **gestione di relazioni con funzionari pubblici** in fase di audit o sopralluogo presso clienti pubblici.

13.2.4 Principi e regole di comportamento

- È **assolutamente vietato** offrire, promettere o dare denaro, beni o altre utilità a pubblici ufficiali o incaricati di pubblico servizio per influenzare decisioni o ottenere vantaggi indebiti;
- i rapporti con la P.A. devono essere **gestiti unicamente da soggetti autorizzati**, nel rispetto delle deleghe interne e delle procedure operative;
- ogni spesa od omaggio deve essere **preventivamente autorizzata, giustificato e documentato**;
- le **comunicazioni e i documenti** inviati a enti pubblici devono essere veritieri, tracciabili e conservati secondo le procedure;
- in caso di dubbio, il personale è tenuto a **consultare l'Organismo di Vigilanza** prima di intraprendere qualsiasi iniziativa verso la P.A.

13.2.5 Presidi organizzativi

- Mappatura dei rapporti con la Pubblica Amministrazione;
- procedure interne di autorizzazione per spese e rapporti istituzionali;
- registrazione e conservazione delle comunicazioni e rendicontazioni pubbliche;
- formazione periodica del personale sui rischi di corruzione e sulle condotte etiche;
- controlli dell'OdV sulle pratiche di rendicontazione e accreditamento.

13.3 REATI IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO

13.3.1 Riferimento normativo

- Art. 25-septies D. Lgs. 231/2001 (Derivanti da violazioni degli artt. 589 e 590 c.p. in relazione al D. Lgs. 81/2008)

13.3.2 Descrizione

Tali reati si concretizzano nella **commissione di delitti colposi di omicidio o lesioni personali gravi o gravissime**, commessi con violazione delle norme antinfortunistiche o di tutela della salute e sicurezza dei lavoratori.

13.3.3 Aree di rischio per lo Studio Samele S.r.l.

- Sicurezza dei **locali aziendali** (uffici, aule di formazione, archivi, depositi);
- attività **esterne presso clienti**, in ambienti produttivi o a rischio specifico;
- sicurezza di **collaboratori, consulenti e docenti** che operano per conto dello Studio;
- **organizzazione dei corsi di formazione** (logistica, emergenze, attrezzature didattiche);
- gestione di **attrezzature informatiche e audiovisive**.

13.3.4 Principi di comportamento

- Tutti i soggetti che operano per conto dello Studio devono rispettare **rigorosamente le norme di sicurezza** previste dal D. Lgs. 81/2008 e dal DVR interno;
- i consulenti e docenti devono attenersi alle **misure di sicurezza del cliente** quando operano presso le sue sedi;



- ogni **infortunio o quasi incidente** deve essere immediatamente segnalato e registrato;
- lo Studio promuove una **cultura della prevenzione**, della segnalazione dei rischi e del miglioramento continuo.

13.3.5 Presidi organizzativi

- DVR aggiornato, con nomine formali di RSPP, addetti emergenze, medico competente (se previsto);
- procedure per la gestione delle emergenze e degli infortuni;
- sorveglianza sanitaria e formazione periodica dei lavoratori;
- audit periodici sull'applicazione delle norme di sicurezza;
- riunione periodica di sicurezza e tracciabilità delle azioni correttive.

13.4 REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

13.4.1 Riferimento normativo

- Art. 24-bis D. Lgs. 231/2001 – artt. 615-ter, 615-quater, 615-quinquies, 617-quater, 635-bis e ss. c.p.
- In correlazione con il Reg. UE 2016/679 (GDPR).

13.4.2 Descrizione

Riguardano condotte di accesso abusivo, manipolazione, danneggiamento o diffusione illecita di dati e sistemi informatici.

13.4.3 Aree di rischio per lo Studio Samele S.r.l.

- Gestione di **dati personali e sensibili** dei clienti (es. DVR, cartelle sanitarie, relazioni di audit);
- **accesso a portali pubblici** o sistemi informativi aziendali dei clienti (INAIL, CIVA, SUAP, Portali regionali);
- utilizzo di **strumenti informatici aziendali** e servizi cloud;
- gestione delle **credenziali di accesso** e della sicurezza logica.

13.4.4 Principi di comportamento

- È vietato accedere a sistemi informatici o database di terzi senza autorizzazione;
- le credenziali aziendali sono personali e non cedibili;
- i dati trattati devono essere utilizzati esclusivamente per finalità professionali e secondo le procedure GDPR;
- qualsiasi violazione o anomalia informatica deve essere segnalata tempestivamente.

13.4.5 Presidi organizzativi

- Adozione di **policy di sicurezza informatica e Data Protection Policy**;
- procedure di **backup e disaster recovery**;
- formazione periodica su sicurezza informatica e phishing;
- nomina del **Responsabile della Protezione dei Dati (DPO)** se previsto;
- audit periodici ISO 27001 o equivalenti.

13.5 REATI SOCIETARI

13.5.1 Riferimento normativo

- Art. 25-ter D. Lgs. 231/2001

13.5.2 Descrizione

Riguardano reati commessi nell'ambito della gestione societaria e contabile, con particolare riferimento alla redazione di bilanci, amministrazione e controllo.

13.5.3 Aree di rischio

- Redazione del bilancio e delle scritture contabili;
- gestione delle spese e delle note professionali;
- comunicazioni verso soci, revisori o enti terzi;
- gestione dei conflitti di interesse.

13.5.4 Presidi e principi

- Contabilità chiara, trasparente e verificabile;
- separazione tra chi effettua e chi controlla le operazioni contabili;
- tracciabilità di ogni operazione economica;
- audit e controlli periodici da parte dell'OdV o revisore contabile;
- formazione continua su etica e responsabilità d'impresa.

13.6 REATI AMBIENTALI

13.6.1 Riferimento normativo

- Art. 25-undecies D. Lgs. 231/2001 e D. Lgs. 152/2006

13.6.2 Aree di rischio

- Gestione e smaltimento di **rifiuti speciali** (es. toner, apparecchiature elettroniche);
- uso di **prodotti chimici o materiali di consumo** in ufficio e aule;
- emissioni e consumi energetici degli uffici.

13.6.3 Presidi

- Raccolta differenziata e smaltimento tramite fornitori autorizzati;
- contratti con operatori ambientali certificati;
- monitoraggio periodico dei consumi e sensibilizzazione alla sostenibilità.

13.7 WHISTLEBLOWING E MISURE DI TUTELA

13.7.1 Riferimento normativo

- D. Lgs. 24/2023 – art. 6, comma 2-bis D. Lgs. 231/2001

13.7.2 Descrizione

Lo Studio ha adottato un sistema di segnalazione interna (Whistleblowing) volto a consentire a dipendenti, collaboratori, consulenti e terzi di segnalare condotte illecite, violazioni del Modello 231 o del Codice Etico. Le segnalazioni devono essere:

- veritiere, circostanziate e in buona fede;
- gestite in modo riservato e protetto;
- analizzate dall'Organismo di Vigilanza.



13.7.3 Misure di tutela

- Divieto assoluto di ritorsione o discriminazione nei confronti del segnalante;
- canali di segnalazione dedicati (piattaforma digitale o indirizzo e-mail riservato dell'OdV);
- possibilità di segnalazione anche in forma anonima;
- tracciabilità e conservazione delle segnalazioni secondo la normativa vigente.

13.8 RUOLO DELL'OdV

L'OdV garantisce:

- la ricezione, gestione e archiviazione delle segnalazioni;
- la verifica della fondatezza dei fatti;
- la proposta di eventuali azioni correttive o sanzionatorie;
- la redazione di report periodici all'organo dirigente.

13.9 CONCLUSIONI

L'effettiva attuazione della presente Parte Speciale è elemento fondamentale per l'efficacia complessiva del Modello 231 dello Studio Samele S.r.l.

Tutti i destinatari del Modello sono tenuti a:

- conoscere e rispettare le disposizioni contenute nella presente Parte Speciale;
- partecipare ai programmi di formazione e aggiornamento;
- collaborare con l'OdV nelle attività di vigilanza e verifica.

Il mancato rispetto delle regole e dei principi contenuti nel Modello potrà comportare l'applicazione delle **sanzioni disciplinari** previste dal sistema sanzionatorio aziendale.