PARTE GENERALE E PARTE SPECIALE

DEL MODELLO ORGANIZZATIVO EX D.L.GVO 231/2001

CODICE ETICO E DI CONDOTTA

DI FIOCORSI FORMAZIONE S.R.L.

SOMMARIO

PARTE GENERALE

1.PREMESSA

Il presente Codice Etico riassume identità e valori di riferimento di EOS Formazione S.r.l. (di seguito, per brevità, anche "EOS" o "EOS – European Osteopathic School"), società operante nel settore della formazione volta all'ottenimento dei crediti formativi nel settore medico sanitario, della formazione e della specializzazione professionale e dei corsi di qualificazione, rivolti ai giovani sprovvisti di qualificazione, di aggiornamento e perfezionamento professionale, rivolti ai lavoratori occupati o disoccupati che intendono migliorare la propria preparazione o conseguire una nuova e diversa qualificazione professionale, a qualsiasi livello, nonché a tutti coloro che sono in possesso dei requisiti di legge necessari all'accesso all'offerta formativa di EOS – European Osteopathic School secondo quanto previsto dalla normativa attualmente vigente e in attesa di integrazione.

La Direzione di EOS considera la qualità un elemento fondamentale della strategia aziendale e ne promuove il rispetto a tutti i livelli dell'organizzazione, diffonde e supporta l'impegno a soddisfare i

requisiti del Sistema di Gestione della Formazione per la Qualità e a migliorarne continuamente l'efficacia.

EOS è oggi società certificata UNI EN 16686:2015 – UNI ISO 9001:2015, che, in forza di un'esperienza oramai quasi decennale:

• Lavora al passo con le sfide dell'innovazione tecnologica e organizzativa attraverso la formazione, per lo sviluppo delle competenze personali, per rafforzare il patrimonio professionale, per sostenere i processi di apprendimento, per l'arricchimento del capitale umano, risorsa e valore decisivo per l'impresa e per ogni organizzazione, specie in quella in ambito di prestazione di cure osteopatiche alla luce delle recente inclusione della predetta scienza nell'ambito delle professioni sanitarie.

• Lavora per favorire l'avvicinamento e l'ingresso al lavoro dei giovani, per sostenere i processi di auto orientamento, di transizione e di riconversione verso collocazioni professionali soddisfacenti, fornendo servizi formativi e di inserimento al fianco del sistema scolastico e universitario, per la creazione e formazione di figure professionali sanitarie altamente specializzate.

• Persegue costantemente l'obiettivo "Qualità", attraverso la ricerca di soluzioni innovative in termini di profili professionali, contenuti, docenti e, più in generale, di sistemi di supporto per la crescita delle risorse umane. La cultura organizzativa si fonda su valori fondamentali quali la qualità del servizio al cliente, la flessibilità operativa, l'orientamento al risultato, la creatività e il riconoscimento dell'importanza dell'apprendimento di gruppo.

• Utilizzando una struttura di knowledge management basata su personale interno e consulenti esterni, EOS monitora regolarmente il ciclo delle attività, dalla fase di progettazione a quella di attuazione degli interventi, e organizza la cultura interna ed esterna secondo un modello di faculty, con l'obiettivo di ricercare le soluzioni migliori, in grado di rispondere con efficacia ai cambiamenti del mercato.

• Le risorse, che supportano EOS nella progettazione e realizzazione dei corsi, sono composte da professionisti osteopati, specialisti, manager, imprenditori, legali e docenti che operano in realtà di primo piano nei competenti settori e a livello internazionale.

• La didattica di EOS si fonda su un corretto bilanciamento tra apprendimento teorico, esercitazioni pratiche e analisi dei casi clinici.

Scopo del presente Codice è anche quello di applicare la normativa ex D.lgs. 231/2001 e sue successive mod. e integr., recante la "*Disciplina della responsabilità amministrativa delle persone*

giuridiche, delle società e delle associazioni anche prive di personalità giuridica", che ha introdotto, per la prima volta nel nostro ordinamento, la responsabilità della persona giuridica in sede penale, che si aggiunge a quella della persona fisica che materialmente ha realizzato il fatto illecito. L'ampliamento della responsabilità mira a coinvolgere nella punizione di taluni illeciti penali il patrimonio delle società e, in definitiva, gli interessi economici dei soci, i quali, fino all'entrata in vigore di tale legge, non pativano conseguenze dalla realizzazione dei reati commessi da amministratori e/o dipendenti, con vantaggio della società stessa.

Questa nuova responsabilità sorge soltanto in occasione della realizzazione di determinati tipi di reati, specificatamente indicati dalla legge, da parte di soggetti legati a vario titolo all'azienda. Tra i reati indicati dalla normativa, anche in relazione a quanto previsto dalle Linee Guida elaborate da Confindustria (https://www.aodv231.it/catalogo-reati-aodv.php), si sono ritenute ipotizzabili, per il settore oggetto di attività di riferimento di EOS, soltanto alcune fattispecie, per le quali sono stati individuati gli specifici rischi connessi all'ambito di rispettiva operatività e definite, pertanto, le regole di comportamento da adottare. Per altre fattispecie si è ritenuto che l'ipotesi di reato fosse del tutto astratta, ma si è ritenuto comunque corretto, e in linea con il sistema valoriale di EOS, richiamare nel presente Codice l'attenzione sulla necessità di adottare in ogni caso una condotta adeguata alla loro reputazione. Infine, alcune fattispecie non sono state prese in considerazione in quanto non sussistono gli estremi organizzativi e/o di assetto societario per la commissione di tali reati. Lo stesso Decreto Legislativo 231/2001 prevede, peraltro, l'esclusione della responsabilità della scuola qualora la stessa provi di aver adottato ed efficacemente attuato, prima della commissione del fatto illecito, un "Modello di organizzazione, gestione e controllo" idoneo a prevenire i reati della specie di quello verificatosi e di aver affidato il compito di vigilare sul funzionamento e l'osservanza del Modello.

Pertanto, EOS ha adottato il predetto modello organizzativo, che si ispira ad una serie di principi di deontologia che si riconoscono come propri e sui quali si intende richiamare l'osservanza da parte di tutti coloro che contribuiscono al perseguimento dei fini della scuola, affidandone l'attuazione e il controllo sul suo rispetto alla Direzione, che cura il suo aggiornamento nell'ambito dei principi e delle azioni di prevenzione predisposte dal presente "Codice Etico e di Condotta".

Pertanto, gli operatori, a qualunque titolo e indipendentemente dalla natura contrattuale del rapporto, nonché i partner, sono tenuti a adeguare i propri comportamenti alle disposizioni del presente Modello Organizzativo e Codice Etico e di Condotta.

In nessun modo la convinzione di agire a vantaggio di EOS può o potrà giustificare l'adozione di comportamenti non in sintonia con i contenuti del Codice Etico e chiunque venga a conoscenza di

violazioni di principi fissati dal Codice Etico è tenuto a riferirne alla Direzione, in persona del legale Rappresentante di EOS, mediante segnalazioni motivate in forma scritta, avendo cura di evitare semplici supposizioni o sensazioni.

In coerenza con tali premesse, per mantenere elevata la propria credibilità e reputazione di EOS, quest'ultima ha deciso di dotarsi di un proprio Codice Etico e di renderlo ufficialmente parte del proprio sistema di controllo interno per la prevenzione dei reati, unitamente al Modello di Organizzazione e Gestione contestualmente adottato a norma del D.lgs. 8 giugno 2001, n.231.

2 PRINCIPI GENERALI

2.1 Ambito d'applicazione

Il Codice Etico e di Condotta è l'insieme dei valori, dei principi, delle linee di comportamento cui devono ispirarsi i soci, la Direzione, i dipendenti e i collaboratori a qualsiasi titolo, i fornitori, e, in generale, tutti i terzi che entrano in rapporto con EOS nell'ambito della propria attività lavorativa e tutti coloro che direttamente o indirettamente, stabilmente o temporaneamente, instaurano relazioni o operano nell'interesse della scuola stesso. EOS promuove i principi del presente Codice Etico e di Condotta anche presso i Clienti e i Committenti nella convinzione che i rapporti economici con il proprio mercato di riferimento non possano che essere improntati alla massima serietà e rettitudine. Il Codice Etico e di Condotta, pertanto, si pone come obiettivi la correttezza e l'efficienza economica nei rapporti interni ed esterni all'organizzazione, al fine di favorire indirizzi univoci di comportamento, nonché benefici economici indotti dalla positiva reputazione della scuola. Il Codice Etico e di Condotta costituisce una linea guida nei rapporti economici, finanziari, sociali, relazionali, con particolare attenzione alle tematiche di conflitti d'interesse, rapporti con la concorrenza, rapporti con i clienti, con i fornitori, con la Pubblica Amministrazione e con gli Enti Locali. Il Codice Etico e di Condotta definisce, in ultima analisi, gli standard etici di EOS, indicando le linee di comportamento da tenere da parte di tutti i collaboratori.

2.2 Sistema dei valori di base

Tutte le azioni ed in generale i comportamenti tenuti e seguiti dai collaboratori di EOS in merito alle attività svolte nell'esercizio delle funzioni di propria competenza e responsabilità, devono essere improntati alla massima correttezza, trasparenza, legittimità e chiarezza. Nell'esecuzione dell'attività e nella gestione delle relazioni con i soggetti esterni tutti devono attenersi alla massima diligenza, onestà, lealtà e rigore professionale, nell'osservanza scrupolosa delle leggi, delle procedure, dei regolamenti aziendali e nel rispetto del Codice Etico e di Condotta, evitando in ogni

modo qualunque situazione di conflitto di interessi, nonché evitando di sottomettere le proprie specifiche attività a finalità o logiche differenti da quelle stabilite da EOS.

2.3 Garanti d'attuazione del Codice Etico e di Condotta

Della completa osservanza, interpretazione ed attuazione del Codice Etico e di Condotta è competente la Direzione, in persona dell'Amministratore Unico e legale rappresentante EDEN CORBANESE /OPPURE/ l'Organismo di Vigilanza *ad hoc* nominato, RASCANI NATALIA, in forma monocratica.

Il personale e tutti i collaboratori potranno segnalare alla Direzione/all'Organismo di Vigilanza eventuali richieste di chiarimento o possibili inosservanze al Codice. A tutte le richieste verrà data una tempestiva risposta senza che vi sia, per chi ha effettuato la segnalazione, alcun rischio di subire qualsiasi forma, anche indiretta, di ritorsione.

Relativamente al Codice Etico e di Condotta, la Direzione/l'Organismo di Vigilanza assicurerà:

• la diffusione del Codice Etico e di Condotta presso i collaboratori e, in generale, presso tutti i terzi che entrano in rapporto con l'organizzazione nell'ambito dello sviluppo delle attività della scuola;

• il supporto nell'interpretazione e attuazione del Codice Etico e di Condotta, nonché il suo aggiornamento;

• la valutazione degli eventuali casi di violazione delle norme, provvedendo, in caso di accertata infrazione, all'adozione delle misure opportune, in collaborazione con le funzioni interne competenti, nel rispetto delle leggi, dei regolamenti e dei contratti di lavoro;

• che nessuno subirà pressioni o ingerenze per aver eventualmente segnalato comportamenti asseritamente non conformi al Codice Etico e di Condotta.

2.4 Obblighi per il personale relativamente al Codice Etico e di Condotta

Ogni collaboratore ha l'obbligo di:

• rappresentare con il proprio comportamento un esempio per i propri colleghi (dipendenti e non, interni ed esterni);

• promuovere l'osservanza delle norme del Codice Etico e di Condotta;

• operare affinché i propri colleghi comprendano che il rispetto delle norme del Codice Etico e di Condotta costituisce parte essenziale del proprio lavoro. EOS promuove un'azione sistematica di informazione e formazione in merito ai reati e ai rischi contemplati dal D. Lgs. 231/2001 e, pertanto, il personale deve responsabilmente conoscere le fattispecie di reato potenzialmente commissibili, rispettare le procedure che ne prevengono l'insorgenza e adottare comportamenti

proattivi in linea con il presente Codice per evitare di incorrere in una qualunque delle fattispecie di reato contemplate.

3 PRINCIPI RELATIVI ALLE OPERAZIONI, ALLE TRANSAZIONI E ALLE REGISTRAZIONI

EOS ha individuato nel proprio sistema di gestione per la qualità lo strumento fondamentale per definire processi, attività e responsabilità afferenti all'operatività della scuola e creare, di conseguenza, attraverso la documentazione messa a punto, una linea guida prescrittiva da utilizzare come riferimento. L'impostazione gestionale data tende a fare in modo che le operazioni e le transazioni rilevanti siano evidenziate nell'ambito della descrizione dei processi produttivi dei servizi di EOS e che ognuna di esse avvenga da parte di personale autorizzato nel rispetto dei requisiti di tracciabilità e trasparenza. Nella gestione delle attività contabili EOS si impegna, attraverso ogni suo collaboratore, ad osservare le regole di corretta, completa e trasparente contabilizzazione, secondo i criteri ed i principi contabili adottati conformemente alle previsioni di legge. Nell'attività di contabilizzazione dei fatti relativi alla gestione, i collaboratori sono tenuti a rispettare le procedure interne in modo che ogni operazione sia, oltre che correttamente registrata, anche autorizzata, verificabile, legittima, coerente e congrua.

La formalizzazione di un sistema sanzionatorio completa il quadro di riferimento, a riprova del fatto che le violazioni alle regole stabilite sono lesive del rapporto di fiducia instaurato.

4 GESTIONE DELLE INFORMAZIONI E DEI DATI

4.1 Norme generali

Le attività di EOS richiedono costantemente l'acquisizione, la conservazione, il trattamento, la comunicazione e la diffusione di dati, documenti ed informazioni attinenti a negoziazioni, procedimenti, operazioni e contratti. Le banche dati di EOS possono contenere, inoltre, dati personali protetti dalla normativa a tutela della privacy, dati che, in assenza di autorizzazione da parte dei legittimi titolari, non possono essere resi noti all'esterno e, infine, dati la cui divulgazione potrebbe produrre danni a EOS. Tutti i collaboratori interni ed esterni sono tenuti a tutelare la riservatezza delle informazioni apprese in ragione della propria funzione lavorativa e, in particolare, ad osservare le clausole di riservatezza richieste dalle controparti, dagli utenti dei siti web di proprietà e/o gestiti da EOS, dai pazienti, dai partecipanti ai corsi di formazione, dagli acquirenti di FAD, libri, prodotti e/o servizi di EOS, etc..

Tutte le informazioni, i dati, le conoscenze acquisite, elaborate e gestite dai collaboratori nell'esercizio della propria attività lavorativa e di consulenza appartengono a EOS e devono

rimanere strettamente riservate e opportunamente protette e non possono essere utilizzate, comunicate o divulgate, né all'interno né all'esterno, se non nel rispetto della normativa vigente, delle procedure aziendali e degli accordi eventualmente presi con ciascuna controparte.
Ciascun collaboratore dovrà pertanto:

- acquisire e trattare solamente i dati necessari e direttamente connessi alle sue funzioni;
- conservare detti dati in modo tale da impedire a terzi estranei di prenderne conoscenza;
- comunicare e divulgare i dati solo nell'ambito delle procedure prefissate ovvero previa autorizzazione della persona a ciò delegata;
- assicurarsi che non sussistano vincoli di confidenzialità in virtù di rapporti di qualsiasi natura con terzi.

I dati e le informazioni raccolti nell'ambito dello svolgimento delle attività sono trattati da EOS nel rispetto delle normative vigenti e in coerenza a quanto stabilito dalla scuola. EOS ha adottato e applica i contenuti della normativa nazionale ed europea ex GDPR 679/2016 in materia di protezione dei dati personali. In particolare, si ricorda l'obbligo di custodia e cambio periodico delle autorizzazioni di accesso al sistema informativo aziendale.

4.2 Utilizzo dei *software* nei rapporti con la Pubblica Amministrazione (Agenzia delle Entrate, Registro delle Imprese, INPS, INAIL etc. etc.)

I programmi *software* destinati all'interazione con istituzioni esterne sono oggetto di particolare attenzione per quanto riguarda le autorizzazioni all'uso. La Direzione definisce i criteri di accesso, i limiti di utilizzo e la regolamentazione delle attività critiche con i fornitori di *service*. Gli utilizzatori per nessun motivo devono comunicare a terzi le loro credenziali di accesso. È in ogni caso vietato un utilizzo non corretto di tali programmi. In particolare, è fatto divieto assoluto di effettuare operazioni non lecite sfruttando particolari abilità personali e/o punti di debolezza dei programmi software ai quali si ha accesso. Nell'ambito nel normale espletamento delle attività formative è essenziale il corretto utilizzo dei *software* e il rispetto dei relativi regolamenti di utilizzo. Nessuno è autorizzato a inserire informazioni o dati difformi da quelli realmente disponibili, anche se ritenuto ininfluente oppure utile/ necessario. I medesimi criteri si applicano nei confronti dei *software* dedicati alla rendicontazione economica delle attività svolte, indipendentemente dalla posizione contrattuale del collaboratore che effettua tali attività.

5 RAPPORTI CON TERZI

5.1 Norme generali

I collaboratori sono tenuti nei rapporti con i terzi a un comportamento etico e rispettoso delle leggi, improntato alla massima trasparenza, chiarezza, correttezza, efficienza, equità. Per questo motivo EOS condanna qualunque pratica illecita possa configurarsi nei confronti delle persone e del patrimonio altrui, vigilando affinché possa essere evitato qualunque tipo di coinvolgimento della scuola, per quanto possibile anche quelli involontari e indiretti, nella commissione di questo tipo di reati. In questo contesto EOS invita tutti i collaboratori a segnalare all'Organismo di Vigilanza o ai propri superiori/referenti interni qualunque situazione nei rapporti con i terzi potenzialmente a rischio sotto il profilo della commissione di reati. Nei rapporti e relazioni commerciali o promozionali, sono proibite pratiche e comportamenti illegali, collusivi, pagamenti illeciti, tentativi di corruzione e favoritismi. Non sono ammesse sollecitazioni dirette o attraverso terzi tese a ottenere vantaggi personali per sé o per altri e devono essere evitati conflitti di interesse tra le attività economiche personali e familiari e le mansioni/funzioni/incarichi/progetti espletati nell'interesse della scuola. L'acquisizione di informazioni relative a terzi che siano di fonte pubblica o privata mediante enti e/o organizzazioni specializzate, deve essere attuata con mezzi leciti nel rispetto delle leggi vigenti. Ai collaboratori non è consentito di ricevere e utilizzare dati e informazioni riservate comunque ricevute da terzi senza che EOS abbia avuto l'autorizzazione dai terzi stessi per l'utilizzo di tali informazioni. In ogni caso, il trattamento dei dati è consentito soltanto nell'ambito dei limiti stabiliti dalle istruzioni ricevute per il proprio ruolo di incaricato. Nell'ambito dell'esecuzione delle attività ogni collaboratore, a qualsiasi livello e per le parti di propria competenza, deve garantire la corretta rendicontazione delle attività svolte sia direttamente, sia attraverso fornitori e/o altri collaboratori da lui coordinati. I relativi documenti informativi/di registrazione (lettere di incarico, registri dei corsi, schede informative) devono essere compilati con attenzione. Per nessun motivo, anche se apparentemente a fin di bene, è ammessa la commissione di falsi. In particolare, non possono essere immessi dati non veritieri, alterati dati preventivamente immessi, compilati e/o firmati documenti di registrazione al posto di altre persone. Eventuali errori nell'imputazione devono essere preventivamente segnalati come non conformità ai propri referenti e successivamente corretti dando evidenza di tale correzione.

5.2 Rapporti con i fornitori di prodotti e servizi

Nei rapporti con i fornitori di prodotti e servizi, con i docenti e con i consulenti (di seguito genericamente indicati come "fornitori") devono essere osservate le procedure interne per la selezione, la qualificazione e la gestione dei rapporti. EOS si ispira nei rapporti con i fornitori ai principi di correttezza e buona fede, nonché al rispetto delle regole sulla concorrenza e sul mercato. In tale contesto i collaboratori, a qualsiasi titolo addetti alle relazioni con i fornitori,

devono operare nell'osservanza di requisiti predefiniti e valutati in termini oggettivi, imparziali e trasparenti, evitando qualunque logica motivata da favoritismi o dettata dalla certezza o dalla speranza di ottenere vantaggi, anche con riferimento a situazioni estranee al rapporto di fornitura, per sé o per EOS. I collaboratori devono evitare qualunque situazione di conflitto di interessi, anche potenziale, con riguardo a fornitori segnalando al proprio referente o all'Organismo di Vigilanza l'esistenza o l'insorgenza di tali situazioni. In modo particolare, la selezione dei fornitori, nonché la formulazione delle condizioni di acquisto di beni e servizi e la definizione delle tariffe professionali sono dettate da valori e parametri di concorrenza, obiettività, correttezza, imparzialità, equità, prezzo, qualità del bene e servizio, garanzie di assistenza e, in generale, un'accurata e precisa valutazione dell'offerta. Non può essere in alcun modo preso in considerazione l'acquisto di beni la cui provenienza non sia nota e non sia garantita la presenza dei relativi documenti fiscali e di garanzia. Non sono ammessi favoritismi nei pagamenti ai fornitori e, più in generale, non possono essere attuate azioni che pregiudichino il loro stato di creditori. Le tipologie contrattuali devono essere coerenti con la tipologia di prodotto e servizio acquistato. Non sono ammesse forme contrattuali che possano in qualche modo rappresentare caratteri elusivi nei confronti delle norme giuslavoristiche.

Nei rapporti con i fornitori non è ammesso dare o ricevere sotto alcuna forma, diretta o indiretta, offerte di denaro o regalie tendenti ad ottenere vantaggi reali o apparenti di varia natura (es. economici, favori, raccomandazioni). Tale divieto ha validità generale, nel senso che deve considerarsi esteso anche a iniziative individuali, utilizzando denaro e beni propri o del nucleo familiare. In ogni caso atti di cortesia commerciale non devono mai essere compiuti in circostanze tali da poter dare origine a sospetti di illiceità e compromettere l'immagine aziendale.

Eventuali operazioni di sconto da parte di fornitori o verso i clienti rientrano nel regolare svolgimento dell'attività d'impresa della scuola e sono improntate al rispetto rigoroso e tassativo delle normative vigente in materia, nonché condizionate al rispetto di particolari requisiti soggettivi e/o oggettivi.

Anche per i fornitori che non sono oggetto di qualificazione (ad esempio commercialisti, avvocati e simili) si deve comunque applicare il normale iter di controllo previsto per il ciclo passivo, con il riscontro formale (firma di benestare al pagamento, fatturazione elettronica etc.) da parte del collaboratore che è stato interfaccia della prestazione eseguita e della congruità della parcella.

5.3 Rapporti con i destinatari dei servizi

EOS persegue l'obiettivo di soddisfare pienamente le aspettative dei propri stakeholders. Pertanto, esige dai collaboratori e, in generale, dai destinatari del Codice Etico e di Condotta che ogni

rapporto e contatto con e tra tali soggetti sia improntato a onestà, correttezza professionale e trasparenza. In generale nei rapporti con i destinatari dei servizi coloro che operano a diverso titolo in nome e per conto di EOS devono astenersi da qualunque comportamento che consenta, direttamente o indirettamente, anche in via meramente potenziale, di trarre o attribuire vantaggi economici indebiti. Nei rapporti con i destinatari, non è ammesso dare o ricevere sotto alcuna forma, diretta o indiretta, offerte di denaro o regalie tendenti ad ottenere vantaggi reali o apparenti di varia natura (es. economici, favori, raccomandazioni). Tale divieto ha validità generale, nel senso che deve considerarsi esteso anche a iniziative individuali, utilizzando denaro e beni propri o del nucleo familiare. EOS si impegna a garantire adeguati standard di qualità dei prodotti/ servizi offerti sulla base di livelli predefiniti e a monitorare periodicamente la qualità percepita.

5.4 Rapporto con le Istituzioni: rapporti con la Pubblica Amministrazione e con gli Enti Locali

EOS adotta nelle relazioni con la Pubblica Amministrazione e con gli Enti Locali la più rigorosa osservanza delle normative comunitarie, nazionali, locali e dei regolamenti interni applicabili. Nei rapporti con tali soggetti, è severamente vietato cercare di influenzare impropriamente le decisioni dell'istituzione interessata, al fine di ottenere il compimento di atti non conformi o contrari ai doveri di ufficio, in particolare offrendo o promettendo, direttamente o indirettamente, doni, favori, denaro o utilità di qualunque genere. Tale divieto ha validità generale, nel senso che deve considerarsi esteso anche a iniziative individuali, utilizzando denaro e beni propri o del nucleo familiare. In ogni caso atti di cortesia commerciale non devono mai essere compiuti in circostanze tali da poter dare origine a sospetti di illiceità e compromettere l'immagine aziendale. Il collaboratore che dovesse ricevere indicazioni da chiunque di operare in tal senso è tenuto a darne immediata comunicazione al proprio referente o all'Organismo di Vigilanza. I rapporti con le Istituzioni, la gestione di trattative, l'assunzione di impegni e l'esecuzione di rapporti, di qualsiasi genere con la Pubblica Amministrazione e gli Enti Locali necessari per lo sviluppo delle attività di EOS, sono riservati esclusivamente alle funzioni della scuola a ciò delegate. Pertanto, qualunque rapporto si attivi tra un collaboratore e persone facenti parte della Pubblica Amministrazione o di Enti Locali, riconducibile a ambiti di interesse di EOS, deve essere segnalato dall'interessato alla Direzione che, valutata la correttezza di tale rapporto nel contesto delle specifiche mansioni/ progetto, ne mantiene evidenza. I rapporti devono essere improntati alla massima trasparenza, chiarezza, correttezza e tali da non indurre a interpretazioni parziali, falsate, ambigue o fuorvianti da parte dei soggetti istituzionali con i quali s'intrattengono relazioni a vario titolo.

5.5 Rapporti con gli allievi e destinatari nell'ambito dei progetti di formazione

Nel rapporto con gli allievi e destinatari dei progetti di formazione i collaboratori sono tenuti alla massima correttezza, nella consapevolezza che, nei progetti di formazione, proprio gli allievi sono i primi, fondamentali stakeholders di EOS. I docenti devono mantenere in ogni occasione un atteggiamento professionale ineccepibile, evitando di instaurare rapporti che possano nuocere al risultato formativo. Non sono ritenuti accettabili, qualunque siano le circostanze, episodi di intolleranza, discriminazione e razzismo.

Analogamente, non saranno ritenuti accettabili atteggiamenti, comportamenti e condotte confidenziali con corsisti, utenti e colleghi, soprattutto per quanto riguarda l'attività della categoria dei docenti incaricati di tenere i corsi. Anche e soprattutto relativamente alle pratiche osteopatiche dimostrative, che solitamente vengono messe in atto durante i percorsi formativi e a cui i corsisti si prestano "direttamente" e personalmente come possibili fruitori del trattamento, i docenti/ formatori dovranno attenersi alle più scrupolose regole di buon senso, oltre che tecniche e scientifiche, al fine di evitare qualsiasi situazione di dubbia interpretazione circa l'opportunità del trattamento dimostrato o delle modalità del suo svolgimento.

È fatto divieto a chiunque di ricevere denaro o altri beni, per sé, per altri o per EOS, in cambio di informazioni di qualsiasi natura. Analogamente tali informazioni non possono essere fornite anche solo a titolo gratuito.

5.6 Rapporti con organizzazioni politiche e sindacali

EOS non eroga contributi diretti o indiretti sotto qualsiasi forma a partiti politici, movimenti, organizzazioni politiche e sindacali, a loro rappresentanti e candidati, se non previa decisione del legale rappresentante.

5.7 Rapporti con le Autorità di Vigilanza e di Controllo

EOS impronta i propri rapporti con le Autorità di Vigilanza e di Controllo alla massima collaborazione nel pieno rispetto del loro ruolo istituzionale, impegnandosi a dare sollecita esecuzione alle loro prescrizioni.

5.8 Comunicazioni e informazioni della scuola

EOS riconosce il ruolo primario di una comunicazione chiara ed efficace nelle relazioni esterne ed interne. In particolare, si ricorda che è fatto divieto di divulgare qualunque informazione che possa in qualche modo avvantaggiare soggetti a discapito di altri. Analogamente non devono essere

divulgate informazioni che possano in qualche modo incidere sulla reputazione di soggetti esterni e sull'affidabilità che il mercato in essi ripone. Le informazioni divulgate all'esterno devono essere, in ogni caso, tempestive e coordinate. Le persone incaricate di divulgare al pubblico informazioni sotto forma di discorsi, partecipazioni a convegni, pubblicazioni o qualsiasi altra forma di presentazione, devono attenersi alle disposizioni della Direzione, ottenendone la preventiva autorizzazione. Le comunicazioni devono essere veritiere, chiare, trasparenti, non ambigue o strumentali: esse devono, infatti, essere coerenti, omogenee e accurate, complete e trasparenti, nonché conformi alle politiche ed ai programmi della scuola. I collaboratori sono tenuti a non fornire informazioni a organi di comunicazione di massa senza esserne stati specificamente e previamente autorizzati.

5.9 Regali

Fatto salvo quanto già specificato relativamente ai rapporti con clienti e fornitori, si precisa ulteriormente che i collaboratori di EOS non possono in generale, direttamente o indirettamente, dare o ricevere regali di natura materiale o immateriale, offrire o accettare denaro, ad eccezione di casi specificatamente concordati con la Direzione. Sono consentiti atti di cortesia commerciale come omaggi o doni di modico valore, di carattere puramente simbolico o personalizzati e comunque tali da non compromettere l'integrità o la reputazione di una delle parti. In ogni caso la decisione in merito all'opportunità e all'entità di omaggi, doni, ecc. spetta esclusivamente alla Direzione.

6 RAPPORTI INTERNI

6.1 Dignità e rispetto

EOS intende rispettare le disposizioni nazionali e internazionali in materia di occupazione ed è contraria ad ogni forma di lavoro irregolare. EOS contrasta e respinge, tanto in fase di selezione e assunzione del personale o contrattualizzazione degli esterni, quanto nella gestione del rapporto di lavoro, qualunque forma di discriminazione fondata sul sesso, sulla religione, sull'età, sulla razza, sulla condizione sociale, sulla nazionalità dei candidati o dei dipendenti/collaboratori, garantendo pari opportunità e attivandosi al fine della rimozione di eventuali ostacoli alla effettiva realizzazione di tale situazione. EOS si impegna a tutelare l'integrità psico-fisica di dipendenti e collaboratori, nel rispetto della loro personalità. Per questo motivo EOS esige che nelle relazioni di lavoro non venga dato luogo a molestie, intendendo come tali anche la creazione di un ambiente di lavoro intimidatorio, ostile o di isolamento nei confronti dei singoli o di gruppi di persone. A tal

fine EOS previene, per quanto possibile, e comunque persegue il mobbing e le molestie personali di ogni tipo. È politica di EOS promuovere un clima interno in cui ognuno interagisca con gli altri colleghi onestamente, con dignità e rispetto reciproco. Pertanto, i collaboratori sono tenuti ad avere una condotta costantemente rispettosa dei diritti e della personalità dei colleghi e dei terzi in generale. I responsabili sono tenuti a esercitare il proprio ruolo con correttezza e imparzialità e sono tenuti a adottare un comportamento di esemplare osservanza delle normative aziendali e del presente Codice Etico e di Condotta anche al fine di stimolare lo spirito di emulazione nei propri collaboratori diretti. I collaboratori devono conoscere e osservare, per quanto di loro competenza, le prescrizioni del Codice Etico e di Condotta e devono, compatibilmente con le possibilità individuali, promuoverne la conoscenza presso i neoassunti e i nuovi collaboratori, nonché presso i terzi con i quali vengano in contatto per ragioni inerenti ai loro compiti. I collaboratori sono tenuti a segnalare all'Organismo di Vigilanza ogni violazione del Codice Etico e di Condotta da parte di colleghi, collaboratori, consulenti, clienti e fornitori. EOS considererà sanzionabile qualunque segnalazione infondata effettuata in malafede.

6.2 Formazione

EOS pone la massima attenzione nella valorizzazione delle competenze professionali dei collaboratori attraverso la realizzazione di iniziative formative finalizzate all'apprendimento degli elementi essenziali della professionalità e dell'aggiornamento delle competenze acquisite.

6.3 Assunzioni

Ai collaboratori viene fatto divieto di accettare o sollecitare promesse o versamenti di denaro o beni o benefici, pressioni o prestazioni di qualsiasi tipo che possano essere finalizzati a promuovere l'associazione o l'assunzione come dipendente di un qualsiasi soggetto (o anche la semplice stipula di un incarico) o il suo trasferimento o la sua promozione. La presente disposizione è applicata anche nei confronti dei contratti di collaborazione o di contratti di consulenza. Ogni assunzione / proposta di collaborazione è decisa sulla base delle risultanze di valutazioni il più possibili oggettive che riguardano le competenze possedute in rapporto ai profili necessari. Ogni assunzione/ collaborazione segue scrupolosamente la procedura specificatamente dedicata. Non sono ammesse assunzioni che, per la loro collocazione di tempo e luogo e/o collegamenti diretti/ indiretti con il Committente, possano configurarsi come scambio per progetti / commesse acquisiti.

6.4 Condotta etica

I collaboratori sono tenuti a svolgere le proprie mansioni in modo responsabile, onesto, diligente, in conformità con le politiche della scuola, le procedure e le direttive stabilite. I valori etici descritti nel presente Codice devono costituire un dovere costante e sistematico della condotta operativa di ogni collaboratore di EOS.

6.5 Salute, sicurezza dei lavoratori e tutela ambientale

EOS offre i principali percorsi formativi professionali avvalendosi di strutture ospitanti autonomamente gestite e organizzate rispetto all'adeguamento alla normativa in oggetto. In Ogni caso EOS si impegna a gestire le proprie attività nel pieno rispetto della normativa vigente in materia di prevenzione e sicurezza sul lavoro. EOS non accetta alcun compromesso nel campo della tutela della salute e della sicurezza dei propri collaboratori sul posto di lavoro. Ciascun collaboratore non deve esporre gli altri (interni o esterni) a rischi inutili che possano provocare danni alla loro salute o incolumità fisica.

6.6 Tutela del patrimonio della scuola

in considerazione del fatto che EOS offre i principali percorsi formativi professionali avvalendosi di strutture ospitanti autonomamente gestite e organizzate, il suo patrimonio di EOS è costituito da limitati beni fisici materiali, quali ad esempio: computer, stampanti, attrezzature, testi/libri e immobili, nonché da beni immateriali quali, ad esempio, informazioni riservate, *software* e *know-how* specifico di settore. La protezione e conservazione di questi beni costituisce un valore fondamentale per la salvaguardia degli interessi della scuola. Ognuno deve sentirsi responsabile dei beni che gli sono stati affidati in quanto strumentali all'attività svolta. È cura di ogni collaboratore, nell'espletamento delle proprie attività non solo proteggere tali beni, ma impedirne l'uso fraudolento o improprio da parte di terzi. L'utilizzo di questi beni da parte dei collaboratori deve essere pertanto funzionale ed esclusivo allo svolgimento delle attività della scuola.

7 CONFLITTO DI INTERESSI

7.1 Principi generali

EOS intende improntare i rapporti con i propri *stakeholders* alla massima fiducia e lealtà. EOS intende aderire ai più elevati standard etici nella conduzione delle sue attività. È quindi doveroso che ciascuno eviti situazioni di conflitti di interesse o altre situazioni che possano essere dannose o inadatte per EOS.

7.2 Rapporti di parentela

Chiunque tra i collaboratori abbia rapporti di parentela anche solo potenzialmente in conflitto con il proprio ruolo è tenuto a segnalarlo tempestivamente all'Organismo di Vigilanza e/o alla Direzione.

7.3 Attività lavorativa esterna

I collaboratori devono evitare tutte quelle attività che siano in conflitto di interesse con EOS, con particolare riferimento a interessi personali o familiari che potrebbero influenzare l'indipendenza nell'espletare le attività loro assegnate. È pertanto fatto obbligo a tali soggetti di segnalare situazioni di conflitto di interesse, anche solo potenziale, informando l'Organismo di Vigilanza e la Direzione. A titolo esemplificativo, ma non esaustivo, sono considerate situazioni di conflitto di interesse: la strumentalizzazione della propria posizione per la realizzazione di interessi propri o di terzi contrastanti con quelli di EOS; l'utilizzazione di informazioni acquisite nello svolgimento di attività lavorative a vantaggio proprio o di terzi; il possesso di partecipazioni finanziarie, di cointeressenze o di interessi con fornitori o concorrenti; ricoprire cariche o incarichi di qualunque genere presso fornitori o concorrenti, salvo il caso di società partecipate dalla stessa scuola e su incarico di quest'ultimo.

7.4 Uso del tempo e dei beni della scuola

II collaboratori non potranno svolgere, durante il proprio orario lavorativo, altre attività non congruenti con le proprie mansioni e responsabilità organizzative. L'utilizzo dei beni della scuola, quali ad esempio locali, attrezzature, informazioni riservate di EOS, non è consentito per l'uso e interesse personale di qualunque genere, salva l'autorizzazione di EOS.

8 VIOLAZIONI E SANZIONI

I collaboratori devono riferire prontamente all'Organismo di Vigilanza o alla Direzione ogni circostanza che comporti, o che sembri comportare, una deviazione dalle norme di comportamento riportate nel presente Codice e/o una violazione alle procedure/istruzioni operative interne in essere. Omettere o non riferire tali circostanze costituisce una violazione del presente Codice Etico e di Condotta. Le segnalazioni sono trattate con la massima riservatezza e tutte le violazioni riferite diventano immediatamente oggetto di indagine. I collaboratori sono tenuti a cooperare senza riserve alle fasi istruttorie e a fornire tutte le informazioni in loro possesso riguardanti tali violazioni, indipendentemente dal fatto che le stesse siano considerate rilevanti. La

mancata cooperazione, o la cooperazione solo parziale con le attività di istruttoria, costituisce una violazione del presente Codice Etico e di Condotta. EOS nei casi accertati e verificati di dolo, furto, omissioni, falsificazioni, alterazioni, utilizzo improprio di informazioni riservate, appropriazione indebita di beni fisici e immateriali del patrimonio della scuola, provvederà ad applicare le sanzioni disciplinari necessarie ed eventualmente, secondo la gravità delle infrazioni commesse, a dare corso ad azioni legali nei confronti delle persone coinvolte. Qualsiasi violazione delle disposizioni del Codice Etico e di Condotta e delle procedure interne verrà trattata con fermezza con la conseguente adozione di adeguate misure sanzionatorie coerentemente con quanto previsto dai contratti nazionali di lavoro e dal presente Modello di organizzazione, gestione e controllo elaborato ai sensi del D.Lgs.231/2001.

Quanto ai reati che nello specifico si intende prevenire e per i quali si è ritenuto fondamentale la creazione e promulgazione delle presenti linee guida, EOS riserva particolare attenzione alle condotte e dinamiche strettamente connesse alle modalità dei erogazione da parte di EOS dei contributi/contenuti formativi ed informativi (sia nei corsi residenziali, sia nelle FAD, che prevedono l'applicazione di tecniche/pratiche osteopatiche), alle fasi di registrazione e memorizzazione dei contenuti formativi (riprese audio-video, utilizzo e/o pubblicazione di immagini da parte dei collaboratori/ fornitori di EOS per la prestazione dei relativi servizi).

Il personale docente incaricato di rappresentare EOS nei percorsi formativi offerti dalla scuola deve tenere nel rapporto con l'utenza un rigore professionale idoneo al ruolo ed alla natura delle pratiche e dei trattamenti tipici dell'osteopatia.

In particolare, nei trattamenti pratici, il formatore deve tenere una condotta ispirata al rigoroso rispetto del diritto alla salute, al corretto trattamento dei dati personali e/o clinici conosciuti in forza dell'incarico ricevuto, alla inequivocabile attuazione di tutte le misure necessarie ad escludere contestazioni, reclami e/o eccezioni riguardanti le modalità e/o tecniche di trattamento osteopatico o di attuazione del sistema informativo obbligatorio.

Ad escludere qualsiasi dubbio interpretativo in merito ai possibili reati configurabili nel settore di operatività in termini strettamente formativi di EOS, si rimanda integralmente alla Parte Speciale del presente documento.

---

9 ENTRATA IN VIGORE E DIFFUSIONE

Il presente Codice Etico e di Condotta entra in vigore a partire dalla sua approvazione da parte del Direzione e viene attuato insieme al Modello di organizzazione, gestione e controllo predisposto ai

sensi del D.Lgs. 231/2001. Ogni variazione o integrazione successiva è approvata dalla Direzione e diffusa secondo quanto previsto del Modello.

PARTE SPECIALE

10 ANALISI DEL RISCHIO NELLA SCUOLA EOS - OSTEOPATHIC SCHOOL E CLASSIFICAZIONE DEI REATI

Il Decreto legislativo 231/2001 individua alcune fattispecie di reato che, se commesse da soggetti che rivestono una posizione apicale all'interno dell'azienda o da persone sottoposte alla Direzione o vigilanza degli stessi (cfr. artt. 6-7 D. Lgs. 231/2001), costituiscono fonte di responsabilità per gli enti, qualora risultino compiuti nell'interesse o a vantaggio degli stessi. In via del tutto esemplificativa e non esaustiva, l'analisi è stata condotta, fra l'altro, attraverso l'esame:

• dell'attività svolta dalla scuola;

• della struttura organizzativa;

• dei contratti che la scuola, in ragione della sua attività, stipula con fornitori esterni.

Proprio in considerazione della natura dell'attività svolta da EOS, sono stati valutati come rilevanti (ossia come potenzialmente a rischio di essere commessi nell'interesse o a vantaggio della società o di chi commette il reato), ai fini della predisposizione del presente Modello, i reati, o alcuni dei reati richiamati dagli articoli:

- 24 e 25 del D. Lgs. 231/2001 (delitti contro la Pubblica Amministrazione);
- 25-ter e 25-sexies del D. Lgs. 231/2001 (reati societari);
- 25-quinquies D. Lgs. 231/2001 (delitti contro la personalità individuale);
- 24-bis D.Lgs. 231/2001 (delitti informatici e trattamento illecito di dati);
- 25-nonies (reati in materia di violazione del diritto d'autore);

Alla luce delle considerazioni di cui sopra, è stata di contro esclusa la rilevanza, ossia ragionevolmente non vi è il rischio di verificazione, dei reati richiamati dall'art. 25-quater (delitti in materia di terrorismo e di eversione dell'ordine democratico) e dall'art. 25-quater punto 1 del D. Lgs. 231/2001, art 10 della legge 16 marzo 2006 n. 146 (reati transazionali), art 25 bis (falsità in monete in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento), art 25 bis. 1 (delitti contro l'industria e il commercio), art. 25-octies, D.Lgs. 231/2001, reati di ricettazione, riciclaggio, impiego di denaro beni o utilità di provenienza illecita, nonché art. 25-septies D. Lgs. 231/2001 (reati di omicidio colposo e lesioni colpose gravi e gravissime commesse con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, in quanto l'attività di formazione della scuola si svolge quasi prevalentemente all'interno di strutture ospitanti di proprietà di terzi, dotate di autonoma responsabilità in materia.

Si è ritenuto, infatti, che il rischio di compimento di tali reati da parte di un soggetto che opera nella scuola, nello svolgimento di una delle attività della stessa, rappresenti anche astrattamente un'ipotesi difficilmente configurabile. Per le suddette ipotesi di reato, non riconducibili ad eventuali attività sensibili della scuola, si ritiene sufficiente il richiamo ai principi contenuti nel Codice Etico della scuola facente parte integrante del presente Modello.

La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo, che integra a sua volta il Codice Etico e di Condotta, integrato dalle informazioni contenute nella documentazione prodotta agli enti certificatori per ottenere le omonime attestazioni, risulta suddivisa in sezioni, tenendo conto delle diverse tipologie di reati individuate e delle relative misure di controllo. Pertanto, vengono di seguito regolamentate le aree "sensibili" che sono emerse dall'analisi dell'attività della scuola e che hanno consentito di identificare i reati di cui sopra.

11 Le Fattispecie di reato nei rapporti con la Pubblica Amministrazione richiamate dal D.LGS. 231/2001

La conoscenza delle fattispecie di reato e delle modalità di configurazione degli stessi, alla cui commissione da parte dei "soggetti qualificati", ai sensi dell'art. 5 del D. Lgs. 231/2001, è collegata la responsabilità a carico dell'ente, è funzionale alla prevenzione dei reati e, di conseguenza, all'intero sistema di controlli previsto dal decreto.

Agli effetti della legge penale rientra nell'ambito della Pubblica Amministrazione qualsiasi soggetto che svolga attività legislativa, giurisdizionale o amministrativa disciplinata da norme di diritto pubblico o persegua, realizzi o gestisca interessi pubblici. A titolo meramente esemplificativo ed avendo riguardo all'ambito di operatività di EOS si possono individuare quali soggetti appartenenti alla Pubblica Amministrazione, lo Stato, le Regioni, le Province, i Comuni; i Ministeri, i Dipartimenti, le Commissioni, nonché gli Enti Pubblici non economici (INPS, ENASARCO, INAIL, ISTAT, INPDAP) e l'Autorità Giudiziaria. Tra le fattispecie penali qui considerate, il reato di concussione, nonché il reato di corruzione, nelle sue varie tipologie, presuppongono il coinvolgimento di una persona fisica che assuma, ai fini della legge penale, la qualifica di "Pubblico Ufficiale" e/o di "Incaricato di Pubblico Servizio", nell'accezione rispettivamente attribuita dagli artt. 357 e 358 c.p.

Le fattispecie delittuose previste dal decreto si riferiscono alle condotte di cui:

- all'articolo 316 bis c.p. (Malversazione a danno dello Stato, reato si configura nel caso in cui, dopo avere ricevuto finanziamenti o contributi da parte dello Stato o da altro Ente Pubblico o dalla Unione Europea, non si utilizzino le somme ottenute conformemente agli scopi cui erano destinate;

- articolo 316 ter c.p. (Indebita percezione di erogazioni a danno dello Stato), ipotesi di reato che si configura nei casi in cui - mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute - si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dalla Unione Europea.;
- articolo 640, comma 2, n. 1 c.p. (Truffa), che si consuma nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato (oppure ad altro Ente Pubblico o all'Unione Europea);
- articolo 640 bis c.p. (Truffa aggravata per il conseguimento di erogazioni pubbliche), che norma l'indebito conseguimento di erogazioni pubbliche, come nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici;
- articolo 640 ter c.p. (Frode informatica), ipotesi di reato che si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno allo Stato, all'Unione Europea o ad altro Ente Pubblico;
- articolo 317 c.p. (Concussione), ipotesi di reato che si configura nel caso in cui un pubblico ufficiale o un incaricato di un pubblico servizio, abusando della sua posizione, costringa o induca taluno a procurare a sé o ad altri denaro o altre utilità non dovutegli;
- articoli 318-319 c.p. (Corruzione per un atto d'ufficio o per un atto contrario ai doveri d'ufficio), che si configurano nel caso in cui il pubblico ufficiale o l'incaricato di pubblico servizio ricevano, per sé o per altri, denaro o altri vantaggi per compiere atti contrari al proprio ufficio, ovvero per compiere, omettere o ritardare atti del proprio ufficio (determinando un vantaggio in favore del corruttore);
- articolo 319 ter c.p. (Corruzione in atti giudiziari), ipotesi di reato che può venire in rilievo in quei casi in cui la scuola sia parte di un procedimento giudiziario e, al fine di ottenere un vantaggio nel procedimento stesso, tramite un proprio esponente o rappresentante, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro funzionario);
- articolo 322 c.p. (Istigazione alla corruzione) che si configura nel caso in cui, in presenza di un comportamento finalizzato alla corruzione, il pubblico ufficiale o l'incaricato di pubblico servizio rifiuti l'offerta illecitamente avanzatagli;

- articolo 322 bis c.p. (Peculato, concussione, corruzione e istigazione alla corruzione di membri degli organi della Unione Europea e di funzionari della Unione Europea e di Stati esteri).

11.1 Attività sensibili in relazione ai reati contro la Pubblica Amministrazione

Le attività potenzialmente "sensibili" riferite ai rapporti con la Pubblica Amministrazione sono qui di seguito elencate:

- negoziazione, stipulazione ed esecuzione di contratti con soggetti pubblici: si tratta dell'attività dell'Ente che decide di partecipare, o negoziare/stipulare/eseguire contratti/ convenzioni di concessione con la Pubblica Amministrazione mediante procedure negoziate (affidamento o trattativa privata);
- gestione dei rapporti con enti previdenziali e assistenziali (in particolare INPS, INPDAP e INAIL) con adempimento di quanto previsto dalla relativa disciplina e/o gestione dei relativi accertamenti/ispezioni;
- gestione dei rapporti con i soggetti pubblici, relativi all'assunzione di personale anche appartenente a categorie protette o la cui assunzione sia agevolata;
- gestione dei rapporti con soggetti pubblici per gli aspetti che riguardano la sicurezza sul lavoro e il rispetto delle cautele previste da leggi e regolamenti per l'impiego di dipendenti adibiti a particolari mansioni: si tratta dell'attività connessa agli adempimenti previsti dalla normativa in materia di sicurezza e igiene sul lavoro e ai relativi rapporti con le Autorità preposte al controllo, anche in caso di ispezioni. (D. Lgs. N. 81/2008);
- gestione dei contenziosi giudiziali e stragiudiziali: si fa riferimento ai contenziosi sorti in seguito a cause avviate da e contro la scuola nei confronti di diversi soggetti (es. soggetti pubblici, dipendenti, clienti e fornitori);
- gestione dei rapporti con organismi di vigilanza relativi all'adempimento degli obblighi legislativi in materia di privacy: si tratta degli adempimenti e delle prescrizioni previste dalla legge in materia di trattamento della privacy e tutela dei dati personali e della relativa disciplina sanzionatoria (compresa l'applicazione della normativa all'infrastruttura dei sistemi informativi);
- gestione dei rapporti con soggetti pubblici per l'acquisizione di finanziamenti/contributi: si tratta dell'attività di richiesta e gestione di contributi/finanziamenti concessi da soggetti pubblici per la realizzazione di attività/servizi, dalla ricerca e individuazione del progetto alla gestione dell'iniziativa e rendicontazione finale delle spese sostenute;

- gestione dei rapporti/ispezioni con l'Amministrazione Finanziaria (in particolare: Agenzia delle Entrate o Guardia di Finanza): si tratta dell'attività relativa alla gestione delle visite ispettive in materia fiscale;
- gestione dei flussi finanziari: l'attività si riferisce alla gestione ed alla movimentazione delle risorse finanziarie relative all'attività della scuola, in particolare agli incassi e pagamenti.

11.2 Identificazione delle potenziali Aree di Rischio e dei Protocolli di Controllo Specifici per la prevenzione di tali reati

Esempi di possibile realizzazione di reato sono:

· l'utilizzo di un finanziamento ottenuto da parte della PA per un altro scopo dallo svolgimento di attività di pubblico interesse;

· nel corso di una richiesta di contributi, finanziamenti, o altre erogazioni comunque denominate, a un ente della P.A. per una determinata attività o acquisizione di un bene, si potrebbe verificare l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, oppure omissione di informazioni dovute all'ente pubblico.

· nel corso della realizzazione di attività sostenute da finanziamento della P.A., si potrebbe verificare la falsa attestazione e successiva dichiarazione di informazioni riguardanti le condizioni in cui si realizza l'attività (ad esempio, la rilevazione delle presenze / assenze dei fruitori).

· in occasione di una gara d'appalto per l'assegnazione di servizi o lavori, o per l'acquisizione di forniture, o in occasione di altre procedure di acquisto, un pubblico ufficiale o l'incaricato di un pubblico servizio, potrebbe costringere o indurre un appaltatore o un fornitore a dare o promettere denaro o altre utilità di cui si avvantaggia anche EOS.

· i referenti di EOS potrebbero dare o promettere a pubblici ufficiali o a incaricati di un pubblico servizio il denaro od altra utilità (ad esempio posti o contratti di lavoro, disponibilità di strutture, servizi che oltrepassano il regolare dovere d'ufficio) al fine di acquisire servizi o attività, di ottenere finanziamenti, acquisire o mantenere certificazioni ed autorizzazioni oppure conseguire il superamento di una verifica o di una valutazione.

· in attività svolte da responsabili di EOS è possibile che i referenti stessi vengano meno ai doveri connessi con la propria funzione, ricevendo o accettando la promessa di denaro o altra utilità di cui si avvantaggia anche la scuola.

· per conseguire un profitto con danno dello Stato, di un Ente pubblico o della Comunità Europea, o in relazione alla possibilità di percepire contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, da parte dello Stato, di un Ente pubblico o della

Comunità Europea, potrebbe accadere che si rappresentino in maniera artificiosa fatti, situazioni, condizioni, che non corrispondono alla realtà.

· nel corso di una richiesta di contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, ad un ente della PA per una determinata attività o acquisizione di un bene, si potrebbe verificare da parte del personale e/o collaboratori l'alterazione di dati contenuti in registri informatici e/o la trasmissione di documenti attestanti fatti e circostanze inesistenti, o la modificazione di dati fiscali/previdenziali della scuola;

11.3 Attività/Processi organizzativi sensibili

Sono sensibili le attività collegate all'ottenimento di finanziamenti, attività collegate all'acquisizione o il mantenimento di certificazioni ed autorizzazioni, rendicontazione alla PA dell'esecuzione del progetto e delle attività erogate, attività collegate alle verifiche di regolarità contabili e fiscale, attività collegate alla acquisizione di servizi o attività, attività finalizzata alla realizzazione operativa di servizi affidati alla Società.

11.4 Funzioni e posizioni organizzative sensibili

- Legale Rappresentante.

· Responsabili, coordinatori e referenti di progetto o di servizio.

· Responsabili e operatori incaricati della richiesta dei finanziamenti.

· Responsabile della Qualità.

Hanno tutti obblighi di vigilanza e di informazione al fine di consentire controlli tempestivi sulla correttezza delle procedure adottate.

12 FATTISPECIE IN TEMA DI REATI SOCIETARI

L'art. 25-ter del D. Lgs. n. 231/2001 introduce la responsabilità amministrativa della persona giuridica con riferimento alla maggior parte dei reati societari. Nel novero di detti reati, è ravvisabile l'interesse del legislatore finalizzato ad assicurare la trasparenza nella gestione societaria, la corretta tenuta dei documenti contabili, la corretta informazione ai terzi e al mercato in generale, a tutelare il capitale sociale, il patrimonio sociale, il regolare funzionamento dell'Ente, le funzioni di controllo. Si elencano qui di seguito le fattispecie contemplate dall'art. 25-ter del Decreto che possono assumere rilevanza in relazione a EOS:

- False comunicazioni sociali (art. 2621 c.c.) e false comunicazioni sociali in danno della Società, dei soci o dei creditori (art. 2622 c.c.). La consumazione di questi reati avviene con

l'esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette alle competenti autorità o al pubblico, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni ovvero omettendo informazioni imposte dalla legge, in modo idoneo ad indurre in errore i destinatari sulla situazione economica, patrimoniale o finanziaria della scuola, con l'intenzione di ingannare i soggetti destinatari di cui sopra. La condotta deve essere finalizzata a conseguire per sé o per altri un ingiusto profitto. La responsabilità si ravvisa anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla scuola per conto di terzi.

Ai fini della punibilità, le informazioni false o omesse devono alterare "in modo sensibile la rappresentazione della situazione economica patrimoniale o finanziaria della scuola e la condotta deve comunque determinare una variazione superiore al 5% del risultato economico di esercizio, al lordo delle imposte, o una variazione superiore all'1% del patrimonio netto". Qualora le alterazioni siano inferiori alle soglie sopra indicate, sono comunque previste sanzioni amministrative pecuniarie e sanzioni interdittive nei confronti delle persone fisiche che hanno posto in essere la condotta. il reato di cui all'art. 2622 c.c. richiede l'ulteriore circostanza che le informazioni, false od omesse, abbiano cagionato un danno patrimoniale alla scuola e ai creditori;

- Impedito controllo (art. 2625 c.c.) L'illecito si verifica nell'ipotesi in cui gli amministratori impediscano o comunque ostacolino, occultando documenti o con altri idonei artifici, lo svolgimento delle attività di controllo o di revisione legalmente attribuite ad altri organi sociali o alle Società di revisione. Per la responsabilità amministrativa della persona giuridica occorre che la condotta di cui sopra abbia indirettamente portato un vantaggio all'Ente.

12.1 Identificazione delle potenziali Aree/attività sensibili di Rischio e dei Protocolli di Controllo per la prevenzione di tali reati

Esiste la possibilità che in documenti contabili della scuola o in altri documenti contenenti comunicazioni sociali dirette ai portatori di interesse vengano determinate poste valutative di bilancio non conformi alla reale situazione della scuola oppure vengano esposti fatti non veri o vengano omesse informazioni dovute riguardo all'Azienda.

L' Amministratore – anche avvalendosi di propri diretti collaboratori – potrebbe non assolvere alla richiesta di informazioni utili al controllo sugli atti di indirizzo e governo della scuola da parte di soci, di altri organi sociali o mediante l'occultamento, anche accompagnato da artifici, della

documentazione necessaria al controllo stesso (ad esempio, esibizione parziale o alterata di detta documentazione).

12.2 Attività/Processi organizzativi sensibili

Nella scuola le attività potenzialmente "sensibili" in relazione ai reati societari sono connesse ai vari adempimenti cui lo stesso deve ottemperare. In particolare, assumono rilevanza le seguenti attività: tenuta della contabilità, formazione e redazione del bilancio e di ogni altra comunicazione sociale, formazione e redazione delle relazioni e delle altre comunicazioni previste dalle singole disposizioni di legge e relative alla situazione economica, patrimoniale o finanziaria della scuola, attività di revisione contabile, ove prevista, disposizione dei beni sociali (in particolare: investimenti con il patrimonio libero), conservazione della documentazione inerente l'attività della scuola al fine di consentire l'attività di controllo o di revisione previste dalla legge, preparazione delle riunioni assembleari, formazione della volontà assembleare, svolgimento e verbalizzazione delle assemblee, rapporti con gli organi (interni ed esterni) deputati al controllo e alla vigilanza del Codice Etico e di Condotta.

In sintesi, le predette attività o processi organizzativi sensibili posso essere commessi in fase di costruzione e redazione dei seguenti documenti o nello svolgimento delle seguenti attività:

· bilancio d'esercizio;

· relazioni o altre comunicazioni concernenti la situazione economica, patrimoniale o finanziaria della società;

· attività di informazione sugli atti di governo ed indirizzo della scuola;

· attività di gestione del capitale sociale.

12.3 Funzioni e posizioni organizzative sensibili

- Legale Rappresentante/ Amministratore e soci.

· Responsabili, coordinatori e referenti di progetto o di servizio.

· Responsabili e operatori incaricati della richiesta dei finanziamenti.

· Responsabile della Qualità.

· Dottore Commercialista e consulenti in materia di bilancio e fiscalità.

---

13. LE FATTISPECIE DI REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI RICHIAMATE DALL'ART. 24-BIS DEL D.LGS. 231/2001

La presente parte speciale si riferisce ai delitti informatici, introdotti nel corpus del D.Lgs. 231 del 2001, all'art. 24- bis, attraverso la Legge 18 marzo 2008 n. 48. Si tratta delle seguenti fattispecie di reato:

- Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.). Documenti informatici: "Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli". L'art. 491-bis c.p. fornisce una definizione di documento informatico basata sull'elemento materiale del supporto di memoria e non sui dati in esso contenuti: può definirsi supporto informatico qualsiasi supporto di memoria – sia esso interno sia esso esterno all'elaboratore elettronico – sul quale possono essere registrati e conservati per un certo periodo di tempo dei dati destinati ad essere letti ed eventualmente elaborati da un sistema informatico. Non costituisce supporto informatico ai sensi dell'art. 491-bis c.p. il tabulato emesso dal computer al termine del processo di elaborazione: il tabulato – così come ogni output stampato – è infatti normalmente costituito da un foglio di carta sul quale il contenuto dei dati è riprodotto in caratteri alfanumerici per consentirne la lettura da parte dell'uomo; rientrano invece nella nozione di documento informatico le carte di pagamento a banda magnetica e le carte a microprocessore (ad es. carte prepagate, carta Viacard a scalare e alcune carte telefoniche). È inoltre documento informatico il supporto informatico che contenga il programma specificamente destinato ad elaborare i dati, ossia il programma memorizzato all'interno del sistema informatico o su un supporto esterno che svolga la funzione di elaborare dati.
- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.): "Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con

abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio". Tale disposizione è rivolta a tutelare la riservatezza dei dati e dei programmi contenuti in un sistema informatico. In particolare, per sistema informatico, ai fini della configurabilità del delitto di cui all'art. 615-ter c.p., deve intendersi una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione, anche in parte, di tecnologie informatiche. Il sistema è dunque tale se gestisce ed elabora dati, mentre tutto ciò che in un sito web o nel mondo dell'informatica non è capace di gestire o elaborare dati in vista dello svolgimento di una funzione non è sistema informatico. L'accesso abusivo si concretizza non appena vengono superate le misure di sicurezza del sistema, ossia tutte quelle misure di protezione al cui superamento è possibile subordinare l'accesso ai dati e ai programmi contenuti nel sistema, quali a titolo esemplificativo codici di accesso, alfabetici o numerici da digitare su una tastiera o memorizzati su una banda magnetica di una tessera da introdurre in apposito lettore. Oltre a queste misure logiche possono rilevare anche misure fisiche quali l'uso di chiavi metalliche per l'accensione dell'elaboratore. La condotta rilevante consiste nell'introdursi abusivamente in un sistema protetto o nel permanervi contro la volontà espressa o tacita del titolare del diritto di escludere gli altri dall'uso del sistema. Si ha introduzione quando si oltrepassano le barriere logiche e/o fisiche che presidiano l'accesso alla memoria interna del sistema e si è quindi in condizione di richiamare i dati ed i programmi che vi sono contenuti. L'introduzione può avvenire sia da lontano ossia per via elettronica sia da vicino da parte di chi si trovi a diretto contatto con l'elaboratore. Oltre all'introduzione rileva anche l'ipotesi del mantenersi in un sistema protetto contro la volontà espressa o tacita del titolare dello *ius excludendi*: tale caso ricorre quando, in seguito ad un'introduzione involontaria o causale o solo inizialmente autorizzata, l'agente permanga nel sistema informatico altrui nonostante il dissenso del soggetto che ha interesse alla riservatezza dei dati e dei programmi in esso contenuti. È bene precisare che per operatore di sistema deve

intendersi solo quella particolare figura di tecnico dell'informatica (c.d. *system administrator*) che all'interno di un'azienda ha il controllo delle diverse fasi del processo di elaborazione dati nonché la possibilità di accedere a tutti i settori della memoria del sistema informatico su cui opera, oppure di altri sistemi, qualora vi sia un collegamento in rete.

- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.) "Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a 5.164 euro. La pena è della reclusione da uno a due anni e della multa da 5.164 euro a 10.329 euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater". L'art. 615-quater è rivolto a punire la condotta di detenzione e di diffusione abusiva di codici di accesso che può portare alla commissione di altri reati informatici: infatti chi entra in possesso abusivamente di codici d'accesso, può commettere un accesso abusivo ad un sistema o può diffondere tali codici ad altre persone che a loro volta potrebbero accedere abusivamente al sistema. L'oggetto del reato viene identificato in qualsiasi mezzo che permetta di superare la protezione di un sistema informatico indipendentemente dalla natura del mezzo: può infatti trattarsi di una password, di un codice d'accesso o semplicemente di informazioni che consentano di eludere le misure di protezione. La disposizione in esame incrimina due tipi di condotte volte rispettivamente ad acquisire i mezzi necessari per accedere al sistema informatico altrui oppure a procurare ad altri tali mezzi o comunque le informazioni sul modo di eludere le barriere di protezione; non è invece punita la semplice detenzione di codici di accesso o di strumenti similari da parte di chi non sia autorizzato a farne uso.
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.) "Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a 10.329 euro". L'art. 615-quinques c.p. è rivolto a tutelare il patrimonio informatico, inteso come hardware, software e dati da attacchi con virus informatici. La

condotta punita è la diffusione (divulgazione), la comunicazione (portare a conoscenza) o la consegna (dare in senso materiale) di un programma informatico che ha lo scopo o l'effetto di danneggiare il sistema informatico o telematico altrui, o di danneggiare dati o programmi in esso contenuti o ad esso pertinenti, oppure l'interruzione parziale o totale del suo funzionamento o la sua alterazione. La legge non fa distinzione tra virus creati da chi commette il reato o da terzi, né tanto meno tra programma informatico che reca concretamente un danno al sistema informatico e quello che non lo provoca.

Un programma può essere definito infetto ai sensi della disposizione in esame se è in grado non solo di danneggiare le componenti logiche di un sistema informatico, ma anche di interrompere o alterare il funzionamento di quest'ultimo.

- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.) "Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso: 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; 3) da chi esercita anche abusivamente la professione di investigatore privato". Ai sensi della disposizione in esame la condotta può consistere alternativamente nell'intercettare fraudolentemente una comunicazione informatica o telematica oppure nell'impedirla o interromperla; il secondo comma prevede poi l'ipotesi della rivelazione in tutto o in parte mediante qualsiasi mezzo di informazione al pubblico del contenuto di una conversazione intercettata. Intercettare una comunicazione informatica o telematica significa prendere cognizione del suo contenuto, intromettendosi nella fase della sua trasmissione; l'intercettazione deve essere realizzata fraudolentemente, ossia eludendo eventuali sistemi di protezione della trasmissione in corso (ad es. decodificando dei dati trasmessi in forma cifrata o superando delle barriere logiche poste a difesa del sistema che invia o riceve la comunicazione) o comunque in modo tale da rendere non percepibile o riconoscibile a terzi l'intromissione

abusiva. La comunicazione è invece impedita quando se ne renda impossibile la trasmissione, intervenendo sul sistema informatico che deve inviare o ricevere i dati; una comunicazione può invece essere interrotta sia agendo sul sistema che invia e che deve ricevere la comunicazione, sia ad esempio deviando il flusso dei dati in corso di trasmissione da un elaboratore ad un altro. - Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.) "Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater. Tale disposizione mira a reprimere una condotta antecedente e preparatoria rispetto a quella prevista dall'art. 617- quater c.p., vietando l'installazione abusiva di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche. Il reato previsto dall'art. 617-quinquies c.p. è stato ravvisato nel caso di utilizzazione di apparecchiature capaci di copiare i codici di accesso degli utenti di un sistema informatico dal momento che la copiatura abusiva dei codici di accesso per la prima comunicazione, con il sistema rientra nella nozione di "intercettare" di cui alla norma incriminatrice.

- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.) "Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni. Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni". Oggetto del danneggiamento può essere innanzitutto un sistema informatico di qualsiasi tipo e dimensione, eventualmente collegato a distanza con altri elaboratori come nel caso dei sistemi telematici. L'aggressione può rivolgersi tanto al sistema nel suo complesso, quanto a una o più delle sue componenti materiali, quali a titolo esemplificativo le periferiche. Non possono invece essere considerati componenti di un sistema informatico i supporti magnetici o ottici sui quali non siano memorizzati dati o programmi, in quanto il loro danneggiamento non arreca nessun pregiudizio alla funzionalità del sistema informatico nel quale dovrebbero essere utilizzati. Oltre al sistema informatico il danneggiamento può avere ad oggetto dati e programmi informatici; per dati si intendono quelle rappresentazioni di informazioni o di concetti che, essendo destinate alla

elaborazione da parte di un computer, sono codificate in una forma (elettronica, magnetica ottica o similare) non percettibile visivamente. Suscettibili di danneggiamento possono essere anche dati o programmi immagazzinati nella memoria interna dell'elaboratore, oppure su un supporto esterno come un disco magnetico o ottico. Tra i beni suscettibili di danneggiamento l'art. 635-bis c.p. indica anche le informazioni: poiché l'informazione è un'entità di per sé astratta, questa espressione assume significato solo in quanto la si riferisca alle informazioni incorporate su un supporto materiale, cartaceo o di altro tipo. Le condotte rilevanti per l'illecito in esame sono la distruzione, il deterioramento e la inservibilità totale o parziale. L'ipotesi di distruzione di dati e programmi più frequente e significativa è rappresentata dalla loro cancellazione: sia attraverso la smagnetizzazione del supporto, sia sostituendo i dati originari con nuovi dati diversi, sia impartendo all'elaboratore, in cui si trovano i dati o i programmi, uno dei comandi in grado di provocarne la scomparsa. Poiché la distruzione deve essere totale, non ricorre questa ipotesi quando i dati o i programmi cancellati siano ancora recuperabili in una zona remota dell'elaboratore, utilizzando un determinato tipo di programma oppure ne sia stata solo impedita la visualizzazione sullo schermo del computer. - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.) "Salvo che il fatto costituisca un più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata". Vd. precedenti fattispecie.

- Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.) "Salvo che il fatto costituisca più grave reato, chiunque mediante le condotte di cui all'art. 635 bis c.p. ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende in tutto o in parte inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore di sistema, la pena è aumentata. - Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies

c.p.) “Se il fatto di cui all’art. 635-quater c.p. è diretto a distruggere, danneggiare, rendere in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso in tutto o in parte inservibile la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell’articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata”. Cfr. precedenti fattispecie.

- Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.) “Il soggetto che presta servizi di certificazione di firma elettronica, il quale al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro”.

13.1 Attività/Processi organizzativi sensibili

Si tratta di ogni attività aziendale che utilizza sistemi informatici (computer, e server interno) e telematici (internet).

13.2 Funzioni e posizioni organizzative sensibili

Le funzioni e posizioni organizzative sensibili in questo settore possono essere rivestite da tutti i collaboratori e consulenti esterni che hanno la possibilità di utilizzare sistemi informatici (computer e server interno) e telematici (internet).

13.3 Protocolli di controllo specifici e Protocolli già in essere

Procedure di sicurezza informatica dei dati prevedono in particolare che la sicurezza sia determinata attraverso l’assegnazione di una password per l’accesso ai sistemi informatici e telematici della scuola da parte dei collaboratori ad esso autorizzati.

13.4 Le "ATTIVITÀ SENSIBILI" ai fini del D. LGS. 231/2001 in relazione ai delitti informatici e di violazione della Privacy (CYBERCRIME)

L'art. 6, comma 2, lett. a) del D. Lgs. 231/2001 indica, come uno degli elementi essenziali dei Modelli di Organizzazione, Gestione e Controllo previsti dal Decreto, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D. Lgs. 231/2001. L'analisi svolta nel corso del Progetto per l'adozione del Modello e, successivamente, durante la sua applicazione ed implementazione nel tempo, ha permesso di individuare le attività di EOS che potrebbero essere considerate "sensibili" con riferimento al rischio di commissione dei reati richiamati dall'art. 24-bis per cui è applicabile il D. Lgs. 231/2001. Per una corretta individuazione delle aree di rischio è stata fatta una mappatura dei sistemi informatici utilizzati da EOS, e, di conseguenza, ai fine 231, una regolamentazione anche in ordine all'accesso agli stessi. L'attività svolta dalla scuola richiede infatti l'utilizzazione da parte di alcuni collaboratori (dipendenti, webmaster, social-media manager, responsabile della qualità, responsabile privacy) di programmi, piattaforme, credenziali, profili ed accounts di proprietà o comunque utilizzati da EOS.

Per comodità di consultazione, anche in ragione della particolare realtà professionale della scuola, qui di seguito viene trattato specificamente quanto viene regolamentato in materia di privacy, attraverso l'individuazione delle relative "aree sensibili".

Le caratteristiche della realtà formativa della scuola, nella quale operano docenti, corsisti, web-designer, e altri collaboratori a vario titolo richiede di mostrare una particolare attenzione al "corretto trattamento dei dati personali", condizione essenziale per il rispetto della dignità delle persone, della loro identità, del loro diritto alla riservatezza ed al corretto trattamento delle informazioni che le riguardano.

A tal fine, EOS ha preordinato una dettagliata documentazione (informative sul trattamento dei dati, liberatorie/autorizzazioni al trattamento, su qualsiasi formato, di particolari dati, di foto, di riprese audio-video, di testimonianze…), per ciascuna area sensibile "tangibile" dall'attività della scuola.

13.5 Protocolli di controllo specifici Protocolli già in essere

L'organizzazione di EOS, per la prevenzione di questa tipologia di reati, si è in particolare concentrata nella predisposizione di tutta la documentazione necessaria all'autorizzazione, al rilascio e al trattamento dei dati personali nel rispetto della normativa vigente, quali le informative sul trattamento dei dati appartenenti a:

- navigatori del sito web di proprietà di EOS o da questa comunque gestito;

- utenti iscritti alla newsletter della scuola;
- utenti dei corsi FAD e/o residenziali;
- collaboratori, fornitori, docenti;
- acquirenti di libri di testo editi da EOS.

Si tratta, come è evidente, dei professionisti con i quali EOS collabora a vario titolo (consulente del lavoro, commercialista, legale), dei corsisti, anche in relazione ad eventuali utilizzi successivi di materiale contenente immagini, riprese e qualsiasi informazione li riguardino, memorizzabili su qualsiasi supporto e riproducibili in qualsiasi formato.

EOS ha, infatti, predisposto accurata modulistica anche in relazione al rilascio delle autorizzazioni all'utilizzo di immagini, di riprese audio video e di altro materiale prodotto in occasione dei corsi organizzati da EOS attraverso attività trasversali, di natura commerciale o di marketing.

I dati idonei a rivelare lo stato di salute dei corsisti possono essere trattati durante l'attività formativa di EOS limitatamente ed esclusivamente per l'eventuale e contestuale dimostrazione di trattamento pratico/osteopatico dell'area interessata dalla asserita patologia, previa autorizzazione della persona titolare dei predetti dati.

Il trattamento di dati sensibili e giudiziari è previsto per tutte le attività connesse ai contenziosi con corsisti o collaboratori a vario titolo, ivi compresi i docenti.

---

14 REATI CONTRO LA PERSONALITÀ INDIVIDUALE I reati di cui agli art. 25 - quinquies del D.Lgs. 231/01

Tra i reati contenuti nell'art. 25 - quinquies del D.Lgs. 231/2001,In considerazione della specificità e abitudinarietà della organizzazione, gestione e controllo di EOS, impegnata nella erogazione dei servizi formativi principalmente presso struttura terze, esterne e ospitanti, di volta in volta, i singoli eventi/corsi (HOTEL, strutture ospedaliere private, poliambulatori, aree di coworking etc. etc.), nonché il requisito indispensabile della maggiore età, le uniche condotte ipotizzabili in relazione alla struttura fisica ed organizzativa di EOS sono:

I. art. 600-quater c.p. detenzione di materiale pornografico;
II. art. 600-quater 1 c.p. – Pornografia virtuale;
III. art. 600 quinquies c.p. iniziative turistiche volte allo sfruttamento della prostituzione minorile;
IV. art. 609-undecies c.p. - Adescamento di minorenni;
V. art. 603-bis c.p. - Intermediazione illecita e sfruttamento del lavoro.

Quanto al reato di cui al punto I. la sua commissione si rende ipotizzabile in virtù del fatto che alcuni collaboratori possono accedere o comunque utilizzare dispositivi appartenenti o in uso ad EOS in essi memorizzare eventuale materiale pornografico.
Quanto al reato di cui al punto II. lo stesso è ipotizzabile in virtù dello scambio di informazioni e di dati, a volte personali, tra utenti/corsisti e docenti incaricati da EOS, informazioni e dati potenzialmente utilizzabili anche per la commissione del predetto reato e astrattamente riconducibile alla scuola.
Quanto ai reati di cui ai punti III. e IV. gli stessi sono ipotizzabili rispetto ai soggetti incaricati da EOS di pianificare e calendarizzare eventi o corsi. Sarebbero tali soggetti, infatti, ad avere la possibilità di rivolgersi eventualmente ad un'utenza di età inferiore ai 18 anni (esclusa dai corsi EOS), agendo illegittimamente il nome della scuola.
Quanto al reato di cui al punto V. eventuali collaboratori delegati al reperimento/selezione di risorse umane (docenti, formatori, professionisti) potrebbero rendersi autori di condotte illecite ricadenti in possibili reati ex art. 603 bis c.p..
In ogni caso, EOS, per quanto non esplicitamente indicato, ipotizzato e regolamentato, fa espresso riferimento ai principi del Codice Etico circa il rispetto della dignità della persona e ai richiami al ripudio di violenze e molestie anche dal punto di vista sessuale in esso contenuti.

14.1 Attività/Processi organizzativi sensibili

Si tratta di ogni attività aziendale che utilizza sistemi informatici (computer e server interno) e telematici (internet), o di attività svolte da collaboratori incaricati della raccolta dati e gestione dei calendari per l'organizzazione di corsi ed eventi.

Le funzioni e posizioni organizzative sensibili in questo settore possono essere rivestite da tutti i collaboratori e consulenti esterni che hanno la possibilità di utilizzare sistemi informatici (computer e server interno) e telematici(internet) o che sono stati incaricati della raccolta dati e gestione dei calendari per organizzazione di corsi ed eventi.

14.2 Protocolli di controllo specifici e Protocolli già in essere

Le procedure di sicurezza già in essere a livello gestionale, assunte indipendentemente dall'insorta esigenza di prevenire la commissione dei reati di cui al D.Lgs. 231/2001, consentono un efficace e attento monitoraggio delle procedure, dirette o svolte tramite scambio/invio di informazioni e dati, finalizzate al reclutamento di capitale umano (dipendenti, docenti, social media manager…),

nonché dello svolgimento degli incarichi ad esso affidati, che prevedono il contatto con gli utenti/ clienti e/o i fornitori dei servizi indispensabili agli eventi/corsi organizzati da EOS (Hotel, strutture ricettive, strutture ospedaliere etc.).

Tali controlli hanno già permesso l'individuazione e la risoluzione di alcune significative problematiche (non ricadenti in nessuna delle ipotesi delittuose previste dalla normativa 231) legate alla condotta di alcuni collaboratori e di operare scelte esclusivamente volte alla tutela ed all'immagine di EOS, idonee a garantire la reputazione, l'immagine ed i principi espressi nel Codice Etico e di Condotta.

---

15 Delitti commessi in materia di violazione del diritto d'autore (art. 25 novies del D. Lgs. 231/2001)

I reati di delitti in materia di violazione del diritto d'autore sono richiamati dall'articolo 25 novies del d.lgs. 231/2001 Art. 171, comma 1 lett. a) bis e comma 3 L. n. 633/1941. Il reato si configura mediante la messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta o di parte di essa; il medesimo comportamento è punito anche quando riguardi opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione.

L'art. 171-bis, comma 1 e comma 2 L. n. 633/1941 prevede che l'illecito si realizza mediante l'abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori; riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico del contenuto di una banca dati; estrazione e reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche dati.

L'art. 171-ter L. n. 633/1941 precisa che il reato si perfeziona mediante l'abusiva duplicazione, riproduzione trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e

dai diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o di parte di essa.

L'art. 171-septies L. n. 633/1941 concerne la mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione. Il reato si concretizza con la fraudolenta produzione, vendita, importazione, promozione installazione, modifica, o con l'utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo in forma sia analogica che digitale.

L'articolo 171-octies della legge 22 aprile 1941, n. 633 contiene una norma che reprime – qualora il fatto non costituisca più grave reato - la condotta di chi, a fini fraudolenti, produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.

15.1. Le attività individuate come potenzialmente sensibili ai fini del d.lgs. 231/2001 con riferimento ai reati riferiti ai delitti in materia di violazione del diritto d'autore

L'analisi dei processi aziendali ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 25-novies del d.lgs. 231/01. Di seguito sono elencate le cosiddette attività sensibili o a rischio identificate con riferimento ai delitti in materia di violazione del diritto d'autore:

- Duplicazione, per trarne profitto, di programmi per elaboratori e software applicativi in assenza del pagamento dei relativi diritti e/o licenze di terzi, da parte di chi, a qualsiasi titolo, si occupa della gestione sistemi informativi e di telecomunicazione, anche tramite siti web di proprietà e/ o comunque gestiti da EOS.
- Utilizzo di contenuti audiovisivi, immagini, foto, disegni, opere letterarie (opuscoli libri, testi in genere) protetti dal diritto d'autore, in assenza di accordi formalizzati per iscritto con il soggetto titolare dei relativi diritti di sfruttamento e utilizzazione economica e/o in violazione di quanto previsto da eventuali specifici accordi.

15.2 Funzioni e posizioni organizzative sensibili

Le funzioni e posizioni organizzative sensibili in questo settore sono rivestite dalla Direzione (Amministratore Unico o suo delegato)/oppure/dall'ODV nominato per le funzioni di controllo del rispetto del Modello organizzativo e del Codice Etico e di Condotta, dal responsabile della Qualità e da chi, in ragione del proprio ruolo (ad es. social media manager), gestisce lo scambio di materiale protetto dal diritto d'autore.

Per ognuna delle attività sensibili identificate sono stati individuati i sistemi dei controlli e i presidi in essere a mitigazione dei rischi reato in riferimento ai reati di delitti in materia di violazione del diritto di autore:

- Adozione di regole comportamentali all'interno del Codice Etico che prevedono il divieto a tutti gli esponenti aziendali, nell'ambito delle proprie attività lavorative e/o mediante utilizzo delle risorse della scuola, comportamenti di qualsivoglia natura atti a ledere diritti di proprietà di EOS, assicurando il rispetto delle leggi e delle disposizioni regolamentari nazionali, comunitarie e internazionali poste a tutela della proprietà industriale, della proprietà intellettuale e del diritto d'autore.
- è stata prevista la regola comportamentale che richiede ai dipendenti di curare diligentemente gli adempimenti di carattere amministrativo connessi all'utilizzo di opere protette dal diritto d'autore (software, banche dati, libri di testo osteopatici etc.) nell'ambito dell'utilizzo di applicazioni software di terzi.
- Per quanto attiene all'ideazione e/o gestione di iniziative promo-pubblicitarie o alla redazione e pubblicazione di testi, viene preventivamente verificata l'eventuale altrui titolarità di diritti d'autore, diritti di edizione, diritti di utilizzazione economica e / o altri diritti di proprietà intellettuale relativamente alle opere di qualsiasi natura e a qualsiasi titolo utilizzate, ivi compresi i disegni o i modelli eventualmente protetti ai sensi della normativa sul diritto d'autore. Tali verifiche vengono effettuate attraverso l'utilizzo delle apposite banche dati e/o deferendo a professionisti tecnico-legali lo svolgimento delle relative indagini. In caso le prescritte verifiche individuino la sussistenza di diritti altrui inerenti alle opere oggetto di indagine, sarà necessario astenersi da qualunque forma di utilizzo e/o riferimento alle stesse.
- La parte generale del presente Modello contiene già direttive, procedure e modulistica relative al corretto delle modalità di utilizzo di contenuti audiovisivi, immagini, foto, disegni, testi, opere/testi protetti dal diritto d'autore, da chiunque trattati conosciuti, elaborati o riprodotti.